Ghid GDPR pentru medici

DE CE UN GHID PRACTIC PENTRU MEDICI IN CEEA CE PRIVESTE PROTECTIA DATELOR CU CARACTER PERSONAL?

Regulamentul General privind Protectia Datelor cu Caracter Personal (GDPR) se aplica din data de 25 mai 2018. In Romania, pana la aplicarea acestui Regulament, exista Legea nr. 677/2001[1], care incepand cu 25 mai 2018 a fost abrogata.[2]

Scopul prezentului ghid este a orienta medicii in practica lor liberala, in punerea in aplicare a obligatiilor prevazute de noul regulament privind protectia datelor personale.

In plus, daca esti practicant intr-o unitate sanitara sau intr-un centru de sanatate de orice tip, te poti duca la personalul din conducere sau la orice alta persoana care ar putea gestiona problema datelor cu caracter personal. In masura in care compania sau organizatia in cauza a desemnat un ofiter privind protectia datelor cu caracter personal (DPO), acesta este interlocutorul privilegiat: va poate oferi orice informatie privind statutul de conformitate al organizatie cu GDPR sau va poate raspunde la orice intrebare legata de protectia datelor.

1. De ce esti afectat de GDPR?

In calitate de medic practicant, esti implicat in primirea sau in difuzarea de informatii despre pacientii tai pentru a asigura urmarirea acestora. In plus, colectezi informatii in egala masura pentru a-ti administra cabinetul (*de exemplu, gestionarea furnizorilor, a personalului angajat etc.*). Aceste informatii pe care le primesti sau le emiti cu ocazia activitatii derulate sunt considerate date cu caracter personal.

GDPR defineste datele cu caracter personal ca fiind "***orice informatie referitoare la o persoana fizica indentificata sau identificabila***", adica o persoana fizica care poate fi identificata, direct sau indirect.

In practica, poate fi vorba de date de indentificare, precum numele, prenumele, adresa sau numarul de telefon, informatii despre viata personala a pacientului (de exemplu, numarul copiilor), despre asigurarea sociala si, in special, informatii cu privire la sanatatea sa (de exemplu, diagnostic, prescriptii, ingrijire etc.) sau in legatura cu potentialii specialist implicati in ingrijirea sa.

In toate aceste situatii in care utilizezi aceste date personale ale pacientului, esti afectat de GDPR.

---

[1] Legea nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, publicata in Monitorul Oficial nr. 790 din data de 12 decembrie 2001.

[2] Legea nr. 677/2001 a fost abrogata prin Legea nr. 129 din 15 iunie 2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, publicata in Monitorul Oficial nr. 503 din data de 19 iunie 2018.

2. Ce cadru trebuie aplicat inregistrarilor pacientilor?

2.1. Check-list-ul practicilor bune de urmat:

- Limitez informatiile colectate la cele strict necesare si folosesc fisele pacientului in conformitate cu scopurile definite (monitorizarea pacientului)
- Pastrez un registru actualizat al “tratamentelor” mele
- Sterg inregistrarile pacientului si, in general, orice informatie ce a depasit termenul de valabilitate recomandat
- Pun in aplicare masuri de securitate adecvate pentru dosarele pacientilor mei
- Imi informez pacientii si ii asigur de respectarea drepturilor lor
- Utilizez, in activitatea profesionala, un software furnizat de o companie acredidata pentru pastrarea fisierelor pacientilor sau pastrez dosarele acestora in format fizic. Aceste fisiere contin, in mod obligatoriu, date cu caracter personal ale pacientilor sau ale altor profesionisti din domeniul sanatatii, implicati in ingrijirea lor.

Prin urmare, esti considerat un “*operator de date*” in sensul reglementarilor privind protectia datelor cu caracter personal. In acest sens, trebuie sa te asiguri de conformitatea dosarelor cu acest regulament.

3. Care sunt obligatiile tale?

Trebuie sa te asiguri ca utilizarea fisierelor, dosarelor pacientilor respecta principiile fundamentale in ceea ce priveste protectia datelor cu caracter personal.

Dosarele in format fizic sau inregistrarile medico-administrative trebuie sa raspunda unor obiective sau finalitati specifice, explicite si legitime.

Astfel, informatiile pe care le colectati in fisierele pacientilor sunt utilizate pentru a va exersa activitatea de prevenire, diagnosticare si ingrijire, servind la gestionare cabinetului. Aceste informatii raspund cerintelor referitoare la ingrijirea pacientilor si includ:

- Gestionarea intalnirilor, programarilor
- Gestionarea dosarelor medicale
- Editarea prescriptiilor
- Trimiterea de scrisori
- Stabilirea si (tele)transmisia foilor de ingrijire

Orice alta utilizare a informatiilor pe care le colectati trebuie facuta cu atentie. In particular, orice utilizare personala sau comerciala a dosarelor pacientilor este prin natura sa interzisa.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

Datele pe care le colectati si pe care le transferati in dosarele pacientilor trebuie sa fie adecvate, relevante si limitate la ceea ce este necesar pentru ingrijirea pacientului prin activitati de prevenire, de diagnostic si ingrijire.

Toate informatiile pe care pacientul le-a dezvaluit, ca parte a schimburilor de comunicari dintre dumneavoastra, nu trebuie neaparat sa se integreze in dosar. Doar cele care sunt cu adevarat utile pentru urmarirea acestuia pot fi salvate si pastrate.

In acest context, se considera legitima colectarea anumitor categorii de date cu caracter personal:

- ***Datele de identificare***: nume, prenume, data nasterii, adresa, numar de telefon
- ***Numarul de Securitate sociala***: numai pentru publicarea fisei de ingrijire si in caz de teletransmitere catre fondurile de asigurari de sanatate
- In functie de context, ***situatia familiala***: starea civila, numarul copiilor
- In functie de context, ***viata profesionala***: profesie, conditii de munca
- ***Sanatatea***: istoricul medical, istoricul de ingrijire, diagnostic medical, tratamente prescrise, natura actelor efectuate, rezultatele testelor de laborator, precum si orice alte dovezi care pot caracteriza starea de sanatate a pacientului si sunt considerate relevante de catre medic
- ***Informatii privind stilul de viata***: daca sunt colectate cu acordul pacientului si in masura strict necesara diagnosticarii si ingrijirii

Daca alte informatii par relevante si necesare in practica profesionala, le puteti colecta (de exemplu, originea etnica, obiceiurile alimentare).

Pe de alta parte, **trebuie exclusa orice informatie care nu are legatura cu obiectul consultarii pacientului sau care nu este esentiala pentru diagnosticarea sau ingrijirea acestuia**. De exemplu, nu trebuie introduse informatii cu privire la viata privata a pacientului care nu sunt relevante din punct de vedere medical (de exemplu, religia pacientului, orientarea sexuala).

Datele pe care le colectati cu privire la pacienti trebuie sa fie pastrate pentru o durata care nu depaseste timpul necesar utilizarii dvs.

Este important sa se tina seama de termenele de prescriptie pentru orice actiuni in raspundere si/sau orice dispozitii particulare.

Trebuie sa informati pacientii despre existenta inregistrarilor si a drepturilor lor in aceastra privinta.

Aceasta informare se poate face prin postarea informatiilor in sala de asteptare sau prin furnizarea unui document specific (de exemplu, pliante adresate pacientului sau puse la dispozitia acestuia in sala de asteptare).

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

Informarea pacientului trebuie sa includa urmatoarele elemente:

- Numele dvs si informatiile de contact;
- Scopurile si temeiul juridic al prelucrarii, inclusiv scopurile ulterioare;
- Destinatarii datelor;
- Termenul de stocare;
- Drepurile persoanei: acces, rectificare, in anumite conditii stergerea, limitarea, opozitia, depunerea unei plangeri la ANSPDCP;
- Caracterul obligatoriu al datelor furnizate si posibilele consecinte ale lipsei de raspuns;
- Daca este cazul, utilizarea in continuare a datelor pentru alt scop decat cel pentru care au fost colectate (de exemplu, daca medicul doreste sa le utilizeze pentru o cercetare ulterioara).

Pacientii dumneavoastra au drepturi. Ei pot:

- Accesa datele care ii privesc
- Rectifica datele in caz de eroare
- Se pot opune tratamentului din motive legate de situatia lor particulara
- Sterge datele, in anumite situatii speciale (dosarul pacientului a fost pastrat prea mult timp, date nepotrivite etc.)

Fiecare solicitare privind aceste drepturi trebuie examinata intr-un termen rezonabil. In cazul unei cereri de acces la dosarul unui pacient, termenul trebuie sa fie de o luna, majorat la 2 luni, cand informatiile solicitate sunt mai greu/complex de obtinut.

Trebuie sa luati toate masurile de precautie necesare pentru a impedica accesul tertilor neautorizati la datele privind sanatatea!

Intr-adevar, numai anumite persoane sunt autorizate, avand in vedere misiunile lor sau dispozitiile legale ce le permit accesul la datele de sanatate ale pacientului (o echipa de ingrijire a unei institutii medicale implicate in ingrijirea pacientului).

In practica, este important sa se asigure respectarea normelor privind schimbul de date intre profesionisti. Astfel, orice profesionist din domeniul sanatatii, implicat in ingrijirea pacientului, poate avea acces specific la informatiile necesare acestei ingrijiri sau, daca acest lucru nu este posibil, medicul poate trimite informatiile necesare acestor profesionisti. In ceea ce priveste personalul administrativ, acesta nu dispune de un acces global la dosarele pacientilor. Unele date (numele, prenumele, data consultatiei) sunt transmise organizatiilor de asigurari de sanatate prin fisele de transmitere la distanta.

In cazul in care utilizati un furnizor de servicii pentru a mentine software-ul care gestioneaza inregistrarile pacientilor, acesta nu trebuie sa acceseze datele personale de sanatate. Are un

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

rol pur tehnic. In principiu, datele trebuie sa fie criptate pentru a permite tehnicianului sa-si indeplineasca sarcinile, fara a putea citi aceste date.

Daca incredintati stocarea fisierelor pacientilor unui furnizor responsabil de pastrarea acestora in servere la distanta, acesta trebuie sa fie licentiat sau certificat in pastrarea, stocarea, gazduirea datelor de sanatate.

In orice caz, imediat ce solicitati serviciile unui furnizor, acesta actioneaza in numele dvs. Trebuie sa formalizati relatia pe care o aveti cu acesta printr-un contract care prevede ca furnizorul:

- nu va folosi datele personale decat sub indrumarea dvs.;
- asigura semnarea angajamentelor de confidentialitate de catre personal;
- ia toate masurile de securitate ce se impun;
- nu apeleaza la un subcontractant fara consimtamantul dvs prealabil si exprimat in scris;
- colaboreaza cu dvs. in indeplinirea obligatiilor pe care le aveti fata de pacienti;
- sterge sau revizuieste datele personale la sfarsitul serviciilor prestate;
- colaboreaza in cadrul auditurilor.

Trebuie sa luati toate masurile necesare pentru a asigura si proteja datele personale pe care le procesati.

Trebuie sa respectati masurile prevazute de standardele privind securitatea datelor si de interoperabilitate.

In ceea ce priveste securitatea sistemului informatic, ar trebui sa respectati urmatoarele mari principii:

- Utilizarea unei parole in conformitate cu recomandarile grupurilor de lucru - 12 caractere (numere, litere mici si majuscule, caractere speciale), reinnoite in mod regulat;
- Blocarea automata a computerelor dupa maxim 30 de minute de inactivitate;
- Antivirus actualizat, firewall;
- Backup-uri regulate (cel putin saptamanal, pastrarea acestora peste 12 luni intr-un loc diferit de firma dvs.);
- Criptarea datelor cu un software adecvat;
- Absenta sau minimizarea conexiunilor dispozitivelor neprofesioniste la retea;
- Autentificarea prin intermediul cardului dvs profesional pentru sanatate sau prin orice alt mijloc de autentificare puternica.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

In niciun caz nu comunicati codurile dvs. secrete personalului (secretar medical, de exemplu). Puteri seta o parola unica pentru restul personalului sau prin intermediul unor cartele personale.

Daca va pastrati inregistrarile in format fizic (pe suport hartie), trebuie sa va asigurati de siguranta acestora (spatii securizate, dulapuri blocate etc.).

In cazul incalcarii, violarii datelor (distrugerea, pierderea, modificarea, divulgarea neautorizata, accesul neautorizat la astfel de date), trebuie sa urmati directiile de mai jos:

- Analizati, pe cat posibil, amploarea problemei pentru a identifica pasii ce trebuie urmati pentru a impiedica reaparitia unui astfel de incident: cine a avut acces la date?
- Care este originea problemei?
- Au fost datele trimise unei terte persoane? Sunt datele de sanatate vizate?
- Ce masuri ar fi putut impiedica evenimentul sau ce masuri ar putea atenua consecintele?

Daca exista un risc pentru drepturile si libertatile persoanelor, notificati ANSPDCP. Aceasta notificare trebuie sa contina:

- natura incalcarii,
- categoriile si numarul aproximativ al persoanelor vizate,
- numele si datele de contact ale firmei dvs.,
- consecintele posibile ale incalcarii datelor,
- actiunile intreprinse sau care urmeaza sa fie luate pentru a remedia incalcarea, inclusiv, daca este cazul, masuri de atenuare a eventualelor consecinte negative.

In cazul in care **incalcarea de date creeaza un risc ridicat pentru drepturile si libertatile persoanelo**r, la cererea ANSPDCP sau la initiativa dvs., comunicati persoanei in cauza, in cel mai scurt timp, aceasta incalcare, cu exceptia cazului in care datele au fost criptate, iar citirea lor este imposibila. Aceasta comunicare trebuie sa aiba loc in mod individual sau, daca necesita eforturi disproportionate, prin comunicare publica. Notificarea contine urmatoarele elemente:

- numele si datele de contact ale firmei dvs.,
- consecintele probabile,
- masurile luate sau care urmeaza a fi intreprinse,
- masuri de atenuare a consecintelor.

Inregistrati aceastra incalcare intr-un registru specific, intr-un tabel rezumat al incidentelor sau chiar in registrul activitatilor de prelucrare (*regasiti in KIT-ul nostru toate modele de registre de care aveti nevoie in activitatea curenta*).

Contactati cat mai curand posibil asiguratorul.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

4. Trebuie sa urmati o anumita formalitate in ceea ce priveste ANSDPC?

Incepand cu data de 25 mai 2018, nu mai este necesar sa va inscrieti ca operator de date cu caracter personal la ANSPDCP, asa cum se practica inainte.

Cu toate acestea, trebuie tinut un registru al operatiunilor de prelucrare, care enumera toate tratamentele pe care le puneti in aplicare: cel pe care il utilizati pentru monitorizarea pacientilor, cat si pe cel ce rezulta din utilizarea postei electronice sau a unui dispozitiv de telemedicina etc.

Registrul activitatilor de prelucrare trebuie sa includa numele si informatiile de contact, precum si caracteristicile esentiale ale tratamentului (scop, persoane vizate, destinatari) - (*regasiti in KIT-ul nostru toate modele de registre de care aveti nevoie in activitatea curenta*).

Cu toate acestea, avand in vedere natura datelor prelucrate, fiind catalogate date sensibile, ar trebui informata si ANSPDCP.

5. Trebuie sa desemnati un responsabil cu protectia datelor DPO?

Atata timp cat nu prelucrati date pe scara larga, nu este necesara numirea unui DPO (vezi aici ce inseamna prelucrare pe scara larga si cand avem nevoie de un DPO). Cu toate acestea, in cazul in care, din cauza activitatii dvs. aveti de-a face cu date personale pe scara larga, trebuie sa fie desemnat un astfel de responsabil la nivel intern sau se pot solicita serviciile unui DPO din mediul extern (consultant, firme de avocatura).

6. Puteti fi sanctionat?

Daca nu va indepliniti obligatiile, se poate aplica o sanctiune de catre ANSPDCP (mustrare sau avertisment – am scris mai multe despre amenzile pe GDPR aici). Prin urmare, este imperativ sa respectati noua reglementare, iar documentele dvs sa fie in conformitate cu noul regulament. In cazul in care ANSPDCP constata lipsa conformitatii unei anumite actiuni, va va impune sa va conformati sis a adoptati masurile necesare pentru a evita o penalizare.

Esential este sa puteti demonstra ca sunteti in cursul unui proces de conformare.

7. Ce cadru trebuie aplicat efectuarii programarilor?

7.1. Check-list-ul practicilor bune de urmat:

- Limitez informatiile colectate de prestatorul de servicii si verific conformitatea acestuia cu reglementarile si, in special, prezenta informatiilor obligatorii din contractual pe care l-am incheiat cu acesta;
- Pastrez un registru actualizat al tratamentelor mele;
- Imi informez pacientii si ii asigur de respectarea drepturilor lor.

Ca parte a practicii dvs. profesionale, puteti utiliza o platforma de programare online sau un furnizor de astfel de servicii. Aceasta parte terta este obligata sa colecteze informatii despre pacientii ce efectueaza o programare, inclusive motivele consultarii.

7.2. Care sunt obligatiile dumneavoastra?

Cand se efectueaza programari, se colecteaza, se pastreaza si se utilizeaza date personale despre pacientii dvs., in special identitatea si datele personale. Motivele consultarii pot fi uneori solicitate cu un grad de precizie ce variaza in functie de specialitati sau de necesitatile pregatirii pentru o anumita examinare. Aceste informatii pot furniza detalii privind starea de sanatate. Daca programarile sunt facute chiar de dvs. sau de o linie telefonica terta sau de o platforma online, ramaneti responsabil pentru procesarea datelor personale ale pacientului.

In calitate de responsabil cu protecția datelor personale, obligatiile dvs. sunt identice cu cele aplicabile dosarelor, fisierelor pacientilor: inregistrarea datelor strict necesare, utilizarea legitima a informatiilor obtinute, limitarea accestului, notificarea ANSPDCP in cazul incalarii obligatiilor etc.

Atenție!

- Dacă consultările nu necesită pregătirea prealabilă sau rezervarea instrumentelor specifice, motivele consultării nu trebuie completate.
- Spre deosebire de înregistrările "pacient" care au o durată de depozitare suficientă, datele legate de programare pot fi șterse atunci când nu mai sunt necesare. Această durată trebuie gândită în funcție de activitatea dvs., știind că datele examenelor și consultărilor medicale sunt, în orice caz, înregistrate în dosarele pacienților dumneavoastră.
- Furnizorul este, de asemenea, responsabil pentru prelucrarea datelor referitoare la conturile create de pacienți și de profesioniștii din domeniul sănătății. Drepturile pacienților sunt identice cu cele menționate anterior pentru fișierele "pacient". In ceea ce priveste drepturile pacientilor, trebuie să li se furnizeze informații specifice.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

7.3. Care sunt obligațiile furnizorului terț care gestionează programarile?

Furnizorul terț, fie că este o platformă de rezervări online sau un furnizor de linii de asistență telefonică, acționează în numele dvs. El este considerat un subcontractant (*persoana* imputernicita) în conformitate cu reglementările in vigoare. Acesta trebuie să fie ghidat de dorința de a proteja mai bine informațiile despre pacienții dumneavoastră și de a respecta reglementările aplicabile. El poate folosi doar informațiile despre pacienții dumneavoastră pentru îndeplinirea strictă a misiunilor sale. În special, prestatorul de servicii trebuie să pună în aplicare măsurile tehnice și organizatorice necesare pentru a asigura securitatea și confidențialitatea datelor încredințate. Aceasta sarcina implică stabilirea accesului securizat, a unei politici de autorizare (acces acordat numai persoanelor autorizate), criptarea datelor (făcând imposibilă citirea unei terțe părți fără cheia de decriptare), protecția împotriva atacurilor pe calculator (antivirus etc.).

Relația cu furnizorul dvs. de servicii trebuie să fie formalizată printr-un contract de subcontractare (*acord de prelucrare a datelor personale pe care il gasiti in KIT-ul nostru*). Trebuie să citiți cu atenție prevederile înainte de semnarea acestui contract pentru a verifica dacă furnizorul de servicii:

- proceseaza datele personale doar dupa instrucțiunile dvs.;
- asigură semnarea angajamentelor de confidențialitate de către personal;
- ia toate măsurile de securitate necesare;
- nu recrutează un subcontractant fără consimțământul scris prealabil al dvs;
- colaborează cu dvs. în îndeplinirea obligațiilor dumneavoastră de operator de date, în special atunci când pacienții au solicitări de date;
- șterge toate datele personale la sfârșitul serviciilor;
- colaborează în contextul auditurilor.

Prestatorul tert, daca ia parte la incidente legate de datele pe care le gestionează pentru contul dvs. (hackeri, pierdere etc), trebuie să va informeze cât mai curând, astfel încât să îndeplinească propriile obligații în acest sens.

Dacă furnizorul dvs. găzduiește în mod electronic informații de la programarile pacientului dvs., inclusiv date de sănătate, acesta trebuie să utilizeze un furnizor de date de sănătate acreditat sau certificat. Furnizorul terț trebuie să țină o evidență a activităților de procesare care menționează utilizările, înregistrările sau orice tranzacții pe care le efectuează asupra datelor personale pentru contul dvs.

7.4. Puteți fi pedepsit?

Pentru nerespectarea obligatiilor ce revin programarilor online, se aplica aceleasi sanctiuni ca în cazul managementului fisierelor „pacienți“.

8. Ce cadru trebuie aplicat utilizării poștei electronice?

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

8.1. Check-list-ul practicilor bune de urmat:

- folosesc un serviciu de mesagerie securizat pentru transferurile cu alți profesioniști din domeniul sănătății;
- dacă folosesc e-mail standard sau o mesagerie instantanee, mă asigur că aceste e-mailuri sunt sigure și potrivite pentru utilizarea mea in scop de afaceri;
- folosesc criptarea atașamentelor atunci când folosesc e-mailul standard care nu garantează confidențialitatea mesajelor.

Ca parte a practicii dvs. profesionale, vi se cere să faceți schimb de informații cu alți profesioniști din domeniul sănătății sau cu pacienții dumneavoastră. S-ar putea să utilizați mesajele de mesagerie securizată sau un serviciu de e-mail standard.

În calitate de operator de date și de o persoană supusă secretului profesional, trebuie să vă asigurați de protecția datelor pe care le schimbați. Această protecție necesită respectarea anumitor reguli.

8.2. Ce reprezinta sistemul securizat de mesagerie din domeniul sănătății?

- Sistemul securizat de mesagerie din domeniul sănătății este un spațiu dematerializat, care permite schimbul de date din domeniul sănătății, cu încredere, între profesioniștii din domeniu și, în general, între profesioniștii din sectoarele sănătății, social și medico-social. De asemenea, integrează un sistem comun și certificat al tuturor profesioniștilor autorizați sau al structurilor în care aceștia practică.

După intrarea în vigoare a GDPR, utilizarea mesageriei securizate este posibilă fără a fi nevoie de îndeplinirea unei formalități pe lângă ANSPDCP. Ca atare, prelucrarea ce decurge din utilizarea mesageriei securizate va trebui să fie înscrisă în registrul dumneavoastră de activități de prelucrare.

8.3. Puteți să utilizați serviciile de mesagerie electronică de tip standard ?

Obligația dumneavoastră de a securiza schimburile de date pe care le realizați, în mod particular în ceea ce privește datele de sănătate, impune să treceți printr-o mesagerie electronică securizată. Cu toate acestea, utilizarea unei asemenea mesagerii nu este posibilă decât între profesioniștii din domeniul sănătății.

Pentru a schimba date cu alți profesioniști, cu non-profesioniști din domeniul sănătății, care intervin în îngrijirea pacientului (ex : psihologi etc) sau cu privire la pacienți, transmiterea datelor de sănătate printr-o mesagerie electronică standard implică următoarele :

- Criptarea datelor sensibile de transmis.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

- Utilizarea unui protocol care garantează confidențialitatea și autentificarea serverului destinatar pentru transferurile de fișiere, de exemplu SFTP sau HTTPS, utilizând versiunile cele mai recente ale protocoalelor.
- Garantarea secretului necesar pentru citirea fișierului (ex: parolă) prin utilizarea unui canal de natură diferită (ex : telefon, SMS etc)

Astfel, utilizarea oricărei mesagerii care nu criptează datele și care le găzduiește într-o țară sau la un prestator care nu garantează protecția acestora conform cu reglementările europene este interzisă.

Totodată, mesageriile instantanee sau de tip chat trebuie să fie utilizate cu cea mai mare precauție. Utilizarea unei asemenea mesagerii trebuie să fie securizată.

Atenție !

Nu toate mesageriile standard pe internet garantează confidențialitatea datelor. Ca atare, criptarea documentelor anexate se va impune.

9. Ce aplicăm în cazul telefoanelor mobile și tabletelor ?

9.1. Check-list al bunelor practici ce trebuie respectate:

- Îmi securizez accesul pe telefon sau pe tabletă, dar și conținutul acestuia/acesteia (parolă, cod etc);
- Nu stochez informații medicale cu privire la pacienții mei pe telefon sau pe tabletă;
- Mă asigur că accesul la programul meu de dosare-pacient de pe telefon/tabletă este securizat;
- Îmi consult programul de dosare-pacient cu precauție.

În exercițiul dumneavoastră profesional, vă utilizați telefonul mobil/tableta pentru a consulta informațiile referitoare la pacienții dumneavoastră sau pentru a comunica cu alți profesioniști din domeniul sănătății sau cu alți pacienți.

9.2. Puteți să vă utilizați telefonul mobil sau tableta pentru a accede la dosarele pacienților ?

Tableta, telefonul mobil pot fi utilizate într-un context profesional, cu condiția respectării regulilor privind securitatea.

Este nerecomandată păstrarea informațiilor de ordin medical în memoria internă a tabletei sau a telefonului dumneavoastră mobil (acest lucru permite evitarea consecințelor grave pentru pacienți în ipoteza unui furt sau a unei pierderi de materiale). Cu toate acestea, în practică, dacă nu puteți ține cont de acest sfat, conservarea datelor trebuie să se efectueze cel puțin cu respectarea următoarelor reguli de securitate : utilizarea de parole conforme

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

recomandărilor GDPR (12 caractere care să cuprindă litere mari, litere mici, cifre, caractere speciale), blocarea automată după un termen scurt, criptarea datelor sensibile. Într-o notă generală, trebuie să evitați să dați cu împrumut telefonul sau tableta dumneavoastră și să evitați să le lăsați nesupravegheate.

Pentru a garanta calitatea și confidențialitatea datelor de sănătate cu caracter personal, dar și protecția acestora, accesul de la distanță la dosarele pacienților trebuie să se facă în conformitate cu standarde rezonabile de siguranță și, pe cât posibil, prin folosirea unor infrastructuri aprobate.

În cursul deplasărilor dumneavoastră, trebuie să verificați întotdeauna, indiferent că veți consulta informațiile referitoare la pacienți pe tabletă sau pe telefonul mobil, ca ecranul dumneavoastră să fie ferit de privirile indiscrete.

Atenție !

Utilizarea suporturilor mobile (USB, CD) este în mod cert nerecomandată. Dacă totuși se întâmplă acest lucru, este recomandat să criptați datele sensibile care sunt stocate pe acestea.

9.3. Cum puteți utiliza telefonul mobil sau tableta ca mod de comunicare ?

Puteți să utilizați telefonul mobil ca mijloc de comunicare cu pacienții dumneavoastră, cu alți profesioniști din domeniul sănătății sau cu personalul dumneavoastră. Asigurați-vă, în cursul deplasărilor efectuate, ca discuțiile de natură profesională să nu fie auzite de persoane din apropiere.

Utilizarea căilor orale de comunicare, a mesageriilor instantanee sau de tip chat, prin aplicații pe internet și nesecurizate este interzisă. De fapt, doar o aplicație care prezintă garanții suficiente de protecție a datelor poate fi utilizată în cadrul exercițiului dumneavoastră profesional. În lipsa acesteia, nicio informație referitoare la un pacient sau la un profesionist din domeniul sănătății care intervine în îngrijirea acestuia nu poate fi transmisă.

Puteți să consultați mesageria dumneavoastră electronică securizată pe tableta sau pe telefonul mobil cu respectarea regulilor de securitate descrise mai sus.

10. Ce cadru se aplică cercetărilor?

10.1. Check-list al bunelor practici ce trebuie respectate:

- Realizez o analiză de impact înainte de efectuarea studiilor interne asupra datelor pacienților mei dacă prelucrarea datelor este susceptibilă să dea naștere unui risc ridicat cu privire la drepturile și libertățile persoanelor fizice;

- În cadrul cercetărilor în parteneriat cu un terț, mă asigur că acestea sunt conforme cu reglementarea;
- Țin la zi registrul activităților de prelucrare (*a se vedea anexa 2: Registrul activităților de prelucrare*);
- Îmi informez pacienții și mă asigur că drepturile lor sunt respectate (*a se vedea anexa 1: Notă de informare*).

Conduceți voi înșivă studii asupra pacienților de care vă ocupați (studii interne) sau interveniți în cadrul cercetărilor medicale în parteneriat cu institute de cercetare etc.

Conduceți dumneavoastră înșivă studii asupra pacienților de îngrijirea cărora vă ocupați (*studii interne*) sau interveniți în cadrul cercetărilor medicale în parteneriat cu institute de cercetare etc.

10.2. Care sunt obligațiile pe care le aveți în cadrul studiilor interne?

Vă doriți să conduceți studii cu privire la datele referitoare la pacienții dumneavoastră, plecând de la datele despre sănătate pe care le-ați obținut cu ocazia urmăririi acestora.

În măsura în care aceste studii sunt realizate de către dumneavoastră și sunt destinate utilizării dumneavoastră exclusive, nu este necesară nicio autorizație din partea ANSPDCP.

În schimb, dumneavoastră va trebui:

- **Să realizați o analiză de impact (DPIA) referitoare la fiecare cercetare sau ansamblu de cercetări similare dacă prelucrarea datelor este susceptibilă să angajeze un risc ridicat pentru drepturile și libertățile persoanei fizice**. O atenție sporită trebuie îndreptată asupra utilizării care va fi făcută asupra datelor cu caracter personal în cadrul cercetării, asupra riscurilor care pot rezulta din aceasta cu privire la drepturile și libertățile persoanei în cauză și cu privire la nivelul de protecție necesar vizavi de aceste riscuri. CNIL a realizat un instrument simplu care permite realizarea unei analize de impact, ce poate fi accesată de pe pagina sa de internet. Pentru a afla mai multe despre analiza de impact, puteți consulta:
- **Completați registrul dumneavoastră de activități de prelucrare pentru a indica noua utilizare a datelor și modalitățile** (a se vedea anexa 2: *Registrul activităților de prelucrare*) și informați pacienții cu privire la realizarea acestor studii. Este suficient doar să adăugați o mențiune pe un afiș mic din sala de așteptare.
- Regulile de securitate sunt aceleași ca pentru dosarele pacienților dumneavoastră.(a se vedea anexa 1: *Exemplu de notă de informare*).

Drepturile persoanelor trebuie de asemenea respectate.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

10.3. Care sunt obligațiile dumneavoastră în timpul cercetărilor medicale în parteneriat cu un terț sau care necesită o colectare de date suplimentare?

Dacă participați la cercetări medicale în parteneriat cu un terț sau care necesită o colectare de date suplimentare, fie că este vorba de un institut de cercetare sau de o unitate medicală, pentru ca datele să fie colectate în cadrul îngrijirilor sau în mod specific pentru cercetare, va fi incident un anumit proces.

Promotorul/inițiatorul cercetării, persoana care a avut inițiativa și care conduce proiectul de cercetare (nu trebuie să fie neapărat cea care și realizează în practică cercetarea sau care contribuie la cercetare), trebuie, ca responsabil al colectării, dacă o metodologie de referință există, să procedeze la o declarație de conformitate cu aceasta din urmă. În lipsa acesteia, trebuie să obțină o autorizație de la ANSPDCP.

Atenție!

Formalitățile ce trebuie îndeplinite pe lângă ANSPDCP sunt realizate de către responsabilul cu prelucrarea (DPO).

Promotorul/inițiatorul sau cel care conduce proiectul de cercetare, în calitate de responsabil cu prelucrarea, trebuie să realizeze o analiză de impact dacă prelucrarea datelor este susceptibilă să angajeze un risc ridicat pentru drepturile și libertățile persoanelor fizice și să completeze astfel registrul activităților de prelucrare.

Drepturile persoanelor vizate vor trebui a fi respectate. Acestea vor trebui informate cu privire la cercetare, la utilizarea datelor acestora pentru cercetare, cu privire la finalitatea lor, cu privire la drepturile lor în această privință. Ele dispun în mod special de un drept de acces și de un drept de opunere. Nota de informare trebuie să fie furnizată de către promotorul/inițiatorul studiului.

11. Ce se aplică în cazul telemedicinei?

11.1. Check-list al bunelor pratici ce trebuie respectate:

- Mă asigur că prestatorul de telemedicină aleasă este conform cu reglementarea GDPR;
- Verific prezența mențiunilor obligatorii în contractul său;
- Controlez ca pacientul să fi fost bine informat.

Consacrați o parte a exercițiului dumneavoastră profesional telemedicinei, fie că este vorba despre teleexpertiză sau teleconsultație pe platformele de telemedicină.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

11.2. Obligațiile dumneavoastră suferă schimbări când vine vorba de telemedicină?

Telemedicina este o formă de practică medicală la distanță care utilizează tehnologiile informației și comunicației. Fie că realizați o teleconsultație, fie că realizați o teleexpertiză, realizați un act medical.

Ansamblul obligațiilor dumneavoastră deontologice obișnuite se aplică, la fel și obligațiile referitoare la informațiile pe care trebuie să le cunoașteți despre pacienții dumneavoastră sau despre alți profesioniști din domeniul sănătății care intervin în îngrijirea acestora.

Regulile referitoare la schimbul și partajarea datelor între profesioniști sunt de asemenea aplicabile.

11.3. Care sunt obligațiile în ceea ce privește platforma de telemedicină?

În situația în care decideți să utilizați o platformă de telemedicină cu ocazia activității dumneavoastră, va trebui să vă asigurați că prestatorul (care pune la dispoziția dumneavoastră această platformă și care este sub-prestatorul dumneavoastră) respectă reglementarea.

Contractul de prestare servicii trebuie să indice în mod clar ca prestatorul:

1. Să nu prelucreze datele cu caracter personal decât sub îndrumarea dumneavoastră;
2. Să fie responsabil cu semnarea acordului de confidențialitate de către personal;
3. Să ia toate măsurile necesare de securitate cerute;
4. Să nu recruteze alți prestatori fără autorizația dumneavoastră scrisă prealabilă;
5. Să coopereze cu dumneavoastră pentru respectarea obligațiilor ce decurg din calitatea de responsabil cu prelucrarea, mai ales atunci când pacienții au anumite cereri cu privire la datele lor;
6. Să suprime sau să vă trimită ansamblul datelor cu caracter personal ca urmare a prestațiilor;
7. Să colaboreze în cadrul auditurilor.

Dacă este vorba despre date de sănătate, platforma trebuie găzduită de către persoana care găzduiește date de sănătate, avizată sau certificată.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

12. ANEXA 1: exemplu de notă de informare cu privire la gestiunea unui cabinet medical

Găsiți mai jos un exemplu de notă de informare de utilizat pentru cabinetul dumneavoastră medical.

Medicul dumneavoastră, Dr. XX (adresă) este obligat să colecteze și să păstreze într-un dosar (dosarul dumneavoastră de pacient) informații cu privire la starea dumneavoastră de sănătate.

De ce medicul ține un dosar despre dumneavoastră?

Dosarul pacientului este obligatoriu. Acest dosar are ca finalitate să asigure parcursul dumneavoastră medical și să vă garanteze îngrijirea cea mai adaptată stării dumneavoastră de sănătate. Acesta garantează continuitatea îngrijirii medicale și răspunde exigenței de a avea parte doar de îngrijiri benefice dumneavoastră.

Care este durata acestuia de păstrare?

El este păstrat în principiu timp de XX de ani începând de la data ultimei dumneavoastră consultații.

În cazul unui program găzduit de către un prestator: Dosarul dumneavoastră este găzduit pe serverele XXX, care îndeplinește cerințele de securitate rezonabile cerute de GDPR. Doctorul XX (adresă) este garantul confidențialității datelor de sănătate. Puteți să vă opuneți externalizării datelor dumneavoastră fie contactând direct medicul dumneavoastră fie contactând direct pe cel care găzduiește datele de sănătate prin curier poștal sau la adresa electronică XX.

Care sunt destinatarii informațiilor ce figurează în dosarul dumneavoastră?

Singurii care au acces la informațiile ce figurează în dosarul dumneavoastră sunt medicul dumneavoastră și, într-o anumită măsură, ținând cont de natura misiunii, personalul acestuia. Medicul, cu consimțământul dumneavoastră, va putea în mod egal să transmită altor profesioniști din domeniul sănătății informații cu privire la starea dumneavoastră de sănătate. În final, pentru a permite decontarea actelor realizate, medicul dumneavoastră este obligat să transmită (electronic sau nu) fișele de îngrijire, precum și orice alt document necesar, casei de sănătate de care aparțineți..

Care sunt drepturile dumneavoastră și cum le puteți exercita?

Puteți avea acces la informațiile care figurează în dosarul dumneavoastră. Dispuneți, de altfel, în anumite condiții, de un drept de rectificare, de ștergere al acestor informații sau de un drept de a vă opune sau de a le limita utilizarea.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

Pentru orice întrebare referitoare la protecția datelor dumneavoastră sau pentru a vă exercita drepturile, puteți să vă adresați direct medicului dumneavoastră. În cazul în care întâmpinați dificultăți, puteți de asemenea să sesizați ANSPDCP.

Această notă de informare trebuie în mod normal să fie adaptată situației dumneavoastră. Ea nu vizează decât gestiunea dosarelor pacienților. Dacă alte prelucrări sunt realizate (*de exemplu*, cercetare, utilizarea unei platforme securizate de gestiune a întâlnirilor), trebuie să realizați o informare specifică cu privire la prelucrările în cauză, mai ales cu privire la finalitatea acestora, la fundamentul legal, la durata conservării datelor.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

13. ANEXA 2. Registrul activităților de prelucrare

Găsiți mai jos un model pre-completat al unui registru de activități de prelucrare pentru un medic liber profesionist. Acest model trebuie adaptat în funcție de situația dumneavoastră particulară și trebuie completat cu precizie (editorul de program sau prestatorul informatic care asigură mentenanța poate să vă dea informațiile necesare).

Registrul poate fi ținut pe suport de hârtie sau pe suport informatic.

Registrul activităților de prelucrare al Dr. Hippocrate

Coordonatele responsabilului organizației (responsabilul cu prelucrarea datelor sau reprezentantul acestuia dacă responsabilul este situat în afara UE)	Dr. Charles Hippocrate Strada Brasov, nr. 17, sector 3 București 0216556565 charles.hipocrate@cabinethippocrate.ro
Numele și coordonatele delegatului cu protecția datelor (dacă ați desemnat un DPO)	/

Activitățile organizației care implică prelucrarea datelor personale

Completați aici activitățile pentru care prelucrați date personale:

Activități	**Desemnarea activităților (exemple)**
Activitatea 1	Parcursul pacienților
Activitatea 2	Întâlniri
Activitatea 3	Studii interne
Activitatea 4	Gestiunea plății
Activitatea 5	Gestiunea furnizorilor
Activitatea 6	Securizarea locurilor (în caz de utilizare a unui dispozitiv de supraveghere video sau cartelă de securitate)

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

Activitatea 7	.....

Trebuie să creați și să țineți la zi o fișă de registru per activitate. Modelul de fișă de registru pentru activitatea 1 este disponibilă mai jos.

Fișa registrului activității de urmat a pacienților

Data creării fișei	1/07/2018
Data ultimei actualizări a fișei	/
Numele responsabilului principal cu prelucrarea (în cazul în care responsabilitatea acestei prelucrări a datelor este partajată cu un alt organism)	/
Numele programului sau aplicației (dacă este potrivit)	Logiciel Diocles

Obiectivele urmărite

Descrieți în mod clar obiectul prelucrării datelor personale și funcțiile acestora.

Programul Diocles permite urmărirea pacienților cabinetului. El mă ajută în activitatea mea de prevenție, de diagnostic și de îngrijire dar și la gestiunea cabinetului. Acesta permite următoarele acțiuni:

- Gestiunea întâlnirilor;
- Gestiunea dosarelor medicale;
- Redactarea prescripțiilor medicale;
- Trimiterea mesajelor către colegi;
- Găzduirea și teletransmiterea fișelor de îngrijiri.

Categoriile de persoane vizate:

Completați diferitele tipuri de persoane de la care colectați sau utilizați date.

Pacienți

Profesioniști din domeniul sănătății

Dacă este cazul, familia pacientului

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

.....

Categorii de date colectate

Completați diferitele date prelucrate:

- Stare civilă, identitate, date de identificare, imagini (nume, prenume, adresă, fotografie, data și locul nașterii etc)
- Viața personală (obiceiuri, situație familială etc) dacă este necesar pentru îngrijirea pacientului
- Viață profesională
- Profesia sau condițiile de muncă dacă aceste date au un impact asupra îngrijirii medicale
- Informații de ordin economic și financiar (venituri, situație financiară, date bancare etc)
- Date de conexiune (adresă ip, logs etc)
- Date de localizare (deplasare, date GPS, GSM etc)
- Internet (cookies, urmăriri, date de navigație etc)
- Alte categorii de date (precizați-le)

Datele cu caracter sensibil sunt și ele prelucrate?

Colectarea anumitor date, în mod particular cele sensibile, este strict reglementată de GDPR și este necesară o anume vigilență în ceea ce le privește. Este vorba despre datele care relevă fără drept originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice sau apartenența sindicală a persoanelor, date genetice sau biometrice, date privind sănătatea, viața sexuală sau orientarea sexuală a persoanelor, date referitoare la condamnările penale sau la infracțiuni, dar și cu privire la numărul de identificare național unic sau numărul de securitate socială.

Da ☐ Nu ☐

Dacă da, care? : Date referitoare la sănătate

Durata conservării categoriilor de date

Cât timp conservați aceste date?

☐ ____ zile

☐ ____ luni

☐ ____ ani

☐ altă durată _____

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

Dacă nu puteți indica o durată exprimată în cifre, precizați criteriile utilizate pentru a determina termenul de ștergere (de exemplu 3 ani începând de la terminarea raportului contractual)

Dacă categoriile de date nu sunt supuse acelorași durate de păstrare, aceste diferențe vor trebui să apară în registru.

Categorii de destinatari ai datelor

- Destinatari interni
  - Secretar medical
  - .....
  - .....
  - .....
- Organisme externe
  - Case de sănătăte
  - Profesioniști din domeniul sănătății care intervin în cadrul îngrijirii
  - .....
  - .....
- Sub-prestatori

  Exemplu: găzduitori, prestatori și mentenanță informatică etc

- Editorul programului Diocese dacă asigură o prestare de mentenanță informatică sau de găzduire a datelor de sănătate
- .....
- .....
- .....

Transferul datelor în afara UE

Datele personale sunt transmise în afara UE?

Da ☐ Nu ☐

Dacă da, către care țară:

.....

În anumite situații (transferul către o țară terță căreia nu îi este incidentă o decizie a Comisiei Europene și fără garanțiile menționate la art. 46 și 47 din RGPD), garanții specifice vor fi prevăzute și documentate în registru (art 49 RGPD). Consultați site-ul ANSPDCP.

Măsurile de securitate

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

Descrieți măsurile de securitate organizaționale și tehnice prevăzute pentru a menține confidențialitatea datelor.

Nivelul de securitate trebuie să fie adaptat riscurilor ridicate de prelucrare. Exemplele următoare constituie garanții de bază ce trebuie prevăzute și care trebuie să fie completate. Dacă nu dispuneți de aceste informații, solicitați-le editorului dumneavoastră de program.

Controlul de acces al utilizatorilor

Descrieți măsurile: acces cu cardul pentru doctorul XX, acces pe bază de username și parolă etc.

Măsuri de urmărire

Precizați natura datelor urmărite (exemplu: includerea în jurnal a accesului utilizatorilor), datele înregistrate (exemplu: nume de utilizator, data și ora conectării etc) și durata lor de păstrare.

Includerea în jurnal a accesului utilizatorilor pe 6 luni cu păstrarea numelui de utilizator, datei, orei de conexiune, duratei de conexiune și documentelor sau dosarelor consultate.

Măsuri de protecție a programelor (antivirus, punerea la zi , teste etc)

Descrieți măsurile:

Instalarea de antivirus și de stingător de incendiu

Protecția datelor

Descrieți modalitățile:

Datele protejate per săptămână pe un server distinct

Numerotarea datelor

Descrieți măsurile (exemplu: site accesibil pe https, utilizare de TLS etc)

Programul numerotează datele conținute.

Controlul sub-prestatorilor

Descrieți modalitățile:

Verificarea angajamentelor luate de către acesta cu privire la securitatea datelor în cadrul contractului de prestare.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

Alte măsuri

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

14. Definiții

Dată cu caracter personal sau dată personală: ea este definită ca orice informație care se raportează la o persoană fizică identificată sau identificabilă, adică o persoană fizică care poate fi identificată, direct sau indirect, mai ales prin referire la un element de identificare, precum un nume, un număr de identificare, date de localizare, identificat în linie sau la mai multe elemente specifice proprii identității sale fizice, psihologice, genetice, psihice, economice, culturale sau sociale.

Date referitoare la sănătate: acestea desemnează datele cu caracter personal referitoare la sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de îngrijire de sănătate, care revelă informații cu privire la starea de sănătate a persoanei în cauză.

Prelucrare: în reglementarea referitoare la protecția datelor nu are sensul medical obișnuit. Acest termen desemnează orice operațiune sau orice ansamblu de operațiuni efectuate sau nu cu ajutorul procedeelor automatizate și aplicate datelor sau ansamblului de date cu caracter personal, precum colectarea, înregistrarea, organizarea, structurarea, conservarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, comunicarea prin transmiterea, difuzare sau orice altă formă de punere la dispoziție, compararea sau interconectarea, limitarea, ștergerea sau distrugerea. Este vorba deci, despre orice acțiune realizată asupra datelor personale dar și ca urmare a colectării acestor date.

Responsabilul cu prelucrarea datelor: este vorba despre persoana fizică sau juridică, autoritate publică, serviciu sau un alt organism care, singur sau împreună cu alții, determină finalitățile și mijloacele prelucrării.

Persoana vizată: persoana fizică (spre deosebire de o persoană juridică, societate privată, organism sau autoritate publică) identificată sau identificabilă față de care se raportează o informație.

Destinatar: persoana fizică sau juridică, autoritate publică, serviciu sau orice alt organism care primește comunicarea datelor cu caracter personal, indiferent că este vorba de un terț sau nu.

Sub-prestator (persoană împuternicită): persoana fizică sau juridică, autoritate publică, serviciu sau alt organism care prelucrează datele cu caracter personal pentru responsabilul cu prelucrarea.

ANSPDCP: autoritatea competentă pentru protecția datelor personale în ANSPDCP. Găsiți informații cu privire la reglementare pe pagina lor de internet: www.dataprotection.ro

Caz practic de sinteză pentru o bună înțelegere a termenilor anteriori

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro

Doctorul Hippocrate își exercită profesia singur, în mod liberal. El primește, pentru prima dată, pe pacientul Alphonse. Acesta din urmă îi vorbește doctorului despre problemele sale cu spatele, sechele ale unui vechi accident. Dr Hippocrate creează un dosar de pacient în programul său Diocles, pe care l-a pus în practică acum o lună și notează acolo observațiile sale. Un coleg de-al său i-a recomandat acestuia acest program foarte simplu de utilizat, accesibil de la distanță și care îi asigură securitatea dosarelor. La finalul consultației, Dr Hippocrate efectuează teletransmiterea datelor către securitatea socială grație cartelei de pacient al lui Alphonse. Doctorul îi dă lui Alphonse o prescripție medicală și redactează o scrisoare către unul din colegii săi specialiști, pe care i-o va trimite acestuia din urmă.

În această situație, este vorba despre o prelucrare a datelor personale?

Răspunsul este da:

Date cu caracter personal: nume, prenume, informații referitoare la problemele de spate, istoric medical în legătură cu accidentul, numărul de securitate socială.

Date de sănătate: informații legate în mod specific de starea de sănătate (probleme de spate, istoric medical în legătură cu accidentul)

Prelucrare: înregistrarea datelor ce-l privesc pe Alphonse în programul Diocles. Găzduirea datelor de către editorul programului Diocles sau de către sub-prestatorul acestuia, teletransmiterea către securitatea socială, schimbul de date cu un coleg.

Responsabilul cu prelucrarea: Dr Hippocrate

Persoana vizată: Alphonse

Destinatari: securitatea socială, colegul, secretarul medical

Sub-prestator (*persoană împuternicită*): editorul programului Diocles sau sub-prestatorul care se ocupă cu găzduirea datelor.

Material conceput de Andreea Codirlă, adaptat după autoritatea din Franța.

avocatoo | powered by LegalUp
Ai nevoie de ajutor?
Scrie-ne pe gdpr@avocatoo.ro