B-dul 16 Decembrie 1989 nr.43, 300218 Timişoara ▪ Tel. +40-256-292637, 494403, 490182, 490185, Fax. +40-256-494403
www: neuromed.ro ▪ e-mail: office@neuromed.ro

POLITICA DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

Cuprins:

B-dul 16 Decembrie 1989 nr.43, 300218 Timișoara ■ Tel. +40-256-292637, 494403, 490182, 490185, Fax. +40-256-494403
www: neuromed.ro ■ e-mail: office@neuromed.ro

1. Introducere

1.1 Contextul Regulamentului general privind protecția datelor ("GDPR")

Regulamentul general privind protecția datelor, 679/2016, înlocuiește Directiva UE din 1995 privind protecția datelor și înlocuiește legislația fiecărui stat membru care a fost elaborată în conformitate cu Directiva 95/46 / CE privind protecția datelor. Scopul său este de a proteja "drepturile și libertățile" persoanelor fizice (adică persoanele vii) și de a se asigura că datele cu caracter personal nu sunt prelucrate fără cunoștința lor și, ori de câte ori este posibil, că sunt prelucrate cu consimțământul lor.

1.2 Definițiile utilizate de organizație (extrase din GDPR)

Domeniul material (articolul 2) - GDPR se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

Domeniul de aplicare teritorial (articolul 3) - GDPR se aplică prelucrării datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii. Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activităţile de prelucrare sunt legate de:

a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată; sau

b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii. Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internaţional public.

1.3 Definițiile articolului 4

“Sediul principal” - sediul principal al operatorului în UE va fi locul în care operatorul adoptă principalele decizii cu privire la scopul și mijloacele activităților sale de prelucrare a datelor. Sediul principal al unei persoane imputernicite în UE va fi centrul său administrativ.

"Date cu caracter personal" înseamnă orice informaţii privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare,

B-dul 16 Decembrie 1989 nr.43, 300218 Timișoara ■ Tel. +40-256-292637, 494403, 490182, 490185, Fax. +40-256-494403
www: neuromed.ro ■ e-mail: office@neuromed.ro

un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

“Categorii speciale de date cu caracter personal” - date cu caracter personal care dezvăluie originea rasială sau etnică, opinii politice, convingeri religioase sau filosofice sau apartenența sindicală și prelucrarea datelor genetice, date biometrice în scopul identificării unice a unei persoane fizice, date privind sănătatea sau date privind viața sexuală sau orientarea sexuală a unei persoane fizice.

"Operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

“Persoana vizată” - orice persoană vie care face obiectul datelor cu caracter personal deținute de o organizație.

"Prelucrare" înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

"Creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia.

"Incălcarea securităţii datelor cu caracter personal" înseamnă o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea

"Consimţământ" al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;.

Copil - GDPR definește un copil drept orice persoană cu vârsta sub 16 ani, deși acest lucru poate fi redus la 13 de legislația statelor membre. Prelucrarea datelor cu caracter personal ale unui copil este legală numai dacă a fost obținut consimțământul părinților sau custozilor. Operatorul va depune eforturi rezonabile pentru a verifica, în astfel de cazuri, dacă titularul răspunderii părintești asupra copilului acordă sau autorizează acordul.

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

"Sistem de evidenţă a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;

2. Politica de confidentialitate

2.1. Consiliul de Administrație și conducerea *SCM Neuromed,* cu sediul B-dul 16 Decembrie 1989 nr. 43, Timișoara, se angajează să respecte toate legile relevante ale UE și ale statelor membre cu privire la datele cu caracter personal și protecția "drepturilor și libertăților" persoanelor ale căror informații *SCM Neuromed* le colectează și proceseaza, în conformitate cu Regulamentul general privind protecția datelor (GDPR).

2.2. Conformitatea cu GDPR este descrisă de această politică și de alte politici relevante, cum ar fi Politica de Securitate a Informațiilor (PIMS), împreună cu procesele și procedurile conexe.

2.3. GDPR va fi aplicata de toate persoanele din cadrul *SCM Neuromed* care prelucreaza date cu caracter personal, inclusiv toate persoanele din cadrul *SCM Neuromed* care proceseaza datele personale ale clienților, angajaților, furnizorilor și partenerilor, precum și orice alte date personale pe care organizația le procesează de la orice sursă.

2.4. Responsabilul pentru protecția datelor este responsabil pentru revizuirea anuală a **Registrului de evidenta a activitatilor de prelucrare a datelor** privind orice modificări ale activităților *SCM Neuromed* (determinată de schimbările înregistrate în registrul de cartografiere a datelor) și de orice cerințe suplimentare identificate prin evaluări ale impactului protecției datelor. Acest registru trebuie să fie disponibil la cererea autorității de supraveghere.

2.5. Această politică se aplică tuturor angajaților / personalului [și părților interesate] din cadrul *SCM Neuromed*, cum ar fi furnizorii externalizați. Orice încălcare a GDPR va fi tratată conform politicii disciplinare a *SCM Neuromed* și poate fi, de asemenea, o contraventie, caz în care problema va fi raportată cât mai curând posibil autorităților competente.

2.6. Se așteaptă ca partenerii și orice terțe părți care lucrează cu sau pentru *SCM Neuromed* și care au sau ar putea avea acces la date personale să fi citit, înțeles și să respecte această politică. Nicio terță parte nu poate accesa datele cu caracter personal deținute de *SCM Neuromed* fără să fi încheiat în prealabil un acord de confidențialitate a datelor, care impune terței parti obligații nu mai puțin oneroase decât cele pe care le respecta *SCM Neuromed* și care conferă *SCM Neuromed* dreptul de a verifica respectarea acordului.

3. **Responsabilități** și **roluri** în temeiul **Regulamentului General Privind Protecția Datelor**:

3.1 *SCM Neuromed* este un [operatorul de date și / sau persoana imputernicita] în context GDPR.

3.2 Top managementul și toți cei cu roluri de conducere sau de supraveghere din cadrul Organizației sunt responsabili pentru dezvoltarea și încurajarea practicilor de gestionare a informațiilor în cadrul Organizației; responsabilitățile sunt stabilite în fișele de post individuale.

3.3 Fisa de post si descrierea ocupatiei pentru Responsabil cu Protecția Datelor, un rol specificat în GDPR; DPO este membru al echipei de conducere, raspunde in fata Consiliului de administrație al Organizației pentru gestionarea datelor cu caracter personal în cadrul *SCM Neuromed* și se asigura că respectarea legislației privind protecția datelor și a bunelor practici pot fi demonstrate. Această responsabilitate include:

3.3.1 elaborarea și punerea în aplicare a acestei politici în conformitate cu GDPR

și

3.3.2 gestionarea securității și a riscurilor în ceea ce privește respectarea politicii.

3.4 A fost desemnat **Responsabilul Pentru Protecția Datelor**, care este considerat de către Consiliul de administrație calificat și cu experiență adecvată, pentru a-și asuma răspunderea pentru respectarea continua de către *SCM Neuromed* a politicii, si, în special, *SCM Neuromed* este în conformitate cu GDPR, ca si presedintele, în ceea ce privește prelucrarea datelor care are loc în zona lor de responsabilitate.

3.5 Responsabilul cu Protecția Datelor are responsabilități specifice în ceea ce privește procedurile precum procedura de solicitare a accesului persoanei vizate și reprezintă primul punct de contact pentru angajați / personal care solicită clarificări cu privire la orice aspect al respectării protecției datelor.

3.6 Conformitatea cu legislația privind protecția datelor este responsabilitatea tuturor angajaților din *SCM Neuromed* care procesează datele cu caracter personal.

3.7 Politica de instruire a *SCM Neuromed* stabilește cerințe specifice de formare și conștientizare a personalului *SCM Neuromed* în legătură cu rolurile specifice in domeniul protectiei datelor.

3.8 Angajații / Personalul organizației sunt responsabili pentru a se asigura că datele personale pe care le-au furnizat către *SCM Neuromed* sunt corecte și actualizate.

4. Principii legate de prelucrarea datelor cu caracter personal

Prelucrarea datelor cu caracter personal trebuie să se desfășoare în conformitate cu principiile de protecție a datelor, prevăzute la articolul 5 din GDPR. Politica și procedurile *SCM Neuromed* sunt concepute astfel încât să asigure respectarea principiilor.

4.1 Datele personale trebuie prelucrate în mod **legal, echitabil şi transparent**

Legal - identificați o bază legală înainte de a putea prelucra datele personale. Acestea sunt adesea denumite "condițiile de procesare", de exemplu consimțământul.

Echitabil - pentru ca prelucrarea să fie echitabila, operatorul de date trebuie să pună la dispoziția persoanelor vizate anumite informații cât mai practic posibil. Aceasta se aplică dacă datele cu caracter personal au fost obținute direct de la persoanele vizate sau din alte surse.

"**Transparență**" - GDPR include reguli privind furnizarea catre persoanele vizate de informații privind confidențialitatea în articolele 12, 13 și 14. Acestea sunt detaliate și specifice, punând accentul pe faptul că notificările privind confidențialitatea sunt înțelese și accesibile. Informațiile trebuie comunicate persoanei vizate într-o formă inteligibilă, folosind un limbaj clar și simplu.

Informațiile specifice care trebuie furnizate persoanei vizate trebuie să includă cel puțin:

4.1.1 **identitatea și datele de contact ale operatorului** și, dacă este cazul, ale reprezentantului operatorului;

4.1.2 datele de contact ale responsabilului cu protecția **datelor**;

4.1.3 **scopul prelucrării** pentru care sunt destinate datele cu caracter personal, precum și temeiul juridic al prelucrării;

4.1.4 **perioada** pentru care vor fi stocate datele cu caracter personal;

4.1.5 **existența** drepturilor de a solicita accesul, rectificarea, ștergerea sau opoziția față de prelucrare și condițiile (sau lipsa) de exercitare a acestor drepturi, cum ar fi afectarea legalității prelucrării anterioare;

4.1.6 **categoriile de date** cu caracter personal vizate;

4.1.7 **destinatarii** sau categoriile de destinatari ai datelor cu caracter personal, după caz;

4.1.8 dacă este cazul, că operatorul intenționează să **transfere** date cu caracter personal unui destinatar dintr-o țară terță și nivelul de protecție acordat datelor;

4.1.9 orice informații suplimentare necesare pentru a garanta o prelucrare corectă.

4.2 Datele personale pot fi colectate doar în scopuri specifice, explicite și legitime

Datele obținute în scopurile specificate nu trebuie utilizate într-un scop care diferă de cele care au fost notificate în mod oficial autorității de supraveghere ca parte a registrului de prelucrare a *SCM Neuromed*.

4.3 Datele personale trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru procesare

4.3.1 Responsabilul pentru Protecția Datelor este responsabil pentru asigurarea faptului că *SCM Neuromed*. nu colectează informații care nu sunt strict necesare pentru scopul pentru care sunt obținute (consultați Instrumentul DPIA pentru fluxul de date / cartografiere).

4.3.2 In toate formularele de colectare a datelor (electronice sau pe suport de hârtie), inclusiv cererile de colectare a datelor în noile sisteme informatice, trebuie să fie inclusa o declarație de procesare echitabila sau un link catre politica de confidențialitate care sa fie aprobată de către responsabilul cu protecția datelor.

4.3.3 Responsabilul cu protecția datelor se va asigura că, anual, toate metodele de colectare a datelor sunt revizuite de către [auditul intern / experții externi] pentru a se asigura că datele colectate sunt în continuare adecvate, relevante și limitate

4.4 Datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere ("exactitate")

4.4.1 Datele care sunt stocate de către operatorul de date trebuie revizuite și actualizate, după caz.

4.4.2 Responsabilul cu protecția datelor are responsabilitatea de a se asigura că întreg personalul este instruit cu privire la importanța colectării și menținerii datelor exacte.

4.4.3 De asemenea, este responsabilitatea persoanei vizate să se asigure că datele deținute de *SCM Neuromed* sunt exacte și actualizate. Completarea unui formular de înregistrare sau o cerere de către o persoana vizata va include o declarație conform căreia datele conținute în aceasta sunt corecte la data depunerii.

4.4.4 Angajații / clienții / etc. trebuie să notifice *SCM Neuromed* cu privire la orice schimbări, pentru a permite actualizarea în mod corespunzător a evidențelor personale. Instrucțiuni pentru actualizarea înregistrărilor. Este responsabilitatea *SCM Neuromed* să se asigure că orice notificare privind modificarile este înregistrată și operata.

4.4.5 Responsabilul pentru Protecția Datelor este responsabil de asigurarea aplicării procedurilor și politicilor adecvate pentru păstrarea datelor cu caracter personal corecte și actualizate, ținând cont de volumul de date colectate, de viteza cu care s-ar putea modifica și de orice alți factori relevanți.

4.4.6 Cel puțin o dată pe an, responsabilul cu protecția datelor va examina datele pastrate a tuturor persoanelor vizate, prelucrate de *SCM Neuromed*, in inventarul de date și va identifica orice date care nu mai sunt necesare în contextul scopului înregistrat. Aceste date vor fi șterse / distruse in siguranta, în conformitate cu procedura de stergere/ distrugere in siguranta a suporturilor de stocare.

4.4.7 Responsabilul pentru Protecția Datelor este responsabil de a răspunde solicitărilor de rectificare de la persoanele vizate în termen de o lună (Procedura de Solicitare a Accesului persoanei vizate). Aceasta poate fi extinsă la încă două luni pentru solicitări complexe. Dacă *SCM Neuromed* decide să nu se conformeze cererii, responsabilul cu protecția datelor trebuie să răspundă persoanei vizate pentru a-și explica raționamentul și să o informeze cu privire la dreptul lor de a depune o plangere autorității de supraveghere și de a solicita căi de atac.

4.4.8 Responsabilul cu Protecția Datelor este responsabil de luarea măsurilor adecvate care, în cazul în care organizațiile terțe părți ar fi primit date cu caracter personal inexacte sau neactualizate, să le informeze că acestea sunt inexacte și / sau expirate și nu trebuie să fie utilizate; Responsabilul cu Protecția Datelor este responsabil și pentru transmiterea oricărei corecții a datelor cu caracter personal părții terțe în cazul în care acest lucru este necesar.

4.5 Datele cu caracter personal trebuie păstrate într-o formă care să permită identificarea persoanei vizate numai atâta timp cât este necesar pentru prelucrare.

4.5.1 În cazul în care datele cu caracter personal sunt păstrate peste data prelucrării, acestea vor fi [minimizate / criptate / pseudonime] pentru a proteja identitatea persoanei vizate în cazul unei încălcări a datelor.

4.5.2 Datele cu caracter personal vor fi păstrate în conformitate cu procedura de păstrare a înregistrărilor și, odată ce data de pastrare a fost depasita, aceste date trebuie să fie distruse în siguranță, așa cum se prevede această procedură.

4.5.3 Responsabilul cu protecția datelor trebuie să aprobe în mod specific orice pastrare a datelor care depășește perioadele de păstrare definite în Procedura de păstrare a înregistrărilor și trebuie să se asigure că justificarea este facuta în mod clar și în conformitate cu cerințele legale privind protecția datelor. Această aprobare se va face in scris

4.6 Datele personale trebuie prelucrate într-o manieră care să asigure securitatea corespunzătoare

Responsabilul cu protecția datelor va efectua o evaluare a riscurilor, luând în considerare toate circumstanțele operațiunilor de procesare a *SCM Neuromed*.

La determinarea caracterului adecvat, responsabilul cu protecția datelor ar trebui să ia în considerare, de asemenea, amploarea eventualelor daune sau pierderi care ar putea fi cauzate persoanelor (de exemplu, personalului sau clienților) în cazul unei încălcări a securității, efectul oricărei încălcări a securității asupra *SCM Neuromed*, și orice daune reputaționale posibile, inclusiv pierderea posibilă a încrederii clienților.

La evaluarea măsurilor tehnice adecvate, responsabilul cu protecția datelor va lua în considerare cel putin următoarele:

- Protecția prin parolă;
- Blocarea automată a terminalelor (calculator/laptop etc) cand nu sunt folosite (idle state);
- Eliminarea drepturilor de acces pentru USB și alte suporturi de memorie
- Software de verificare a virușilor și firewall-uri
- Drepturile de acces in functie de roluri, inclusiv cele atribuite personalului temporar;
- Securitatea rețelelor locale si WAN;
- Tehnologii de îmbunătățire a confidențialității, cum ar fi **pseudonimizarea** și anonimizarea;
- Identificarea standardelor internaționale de securitate relevante pentru <*numele organizatiei*>

La evaluarea măsurilor organizatorice adecvate, responsabilul cu protecția datelor va lua în considerare si următoarele:

- Nivelurile potrivite de instruire în cadrul Organizației;
- Includerea masurilor privind protecția datelor în contractele de muncă;
- Identificarea măsurilor de acțiune disciplinară pentru încălcarea datelor;
- Monitorizarea personalului pentru respectarea standardelor de securitate relevante;
- Controlul accesului fizic la înregistrările electronice și pe hârtie;
- Stocarea datelor pe suport de hârtie în dulapuri securizate;
- Restricționarea utilizării dispozitivelor electronice portabile în afara locului de muncă;
- Restricționarea folosirii dispozitivelor personale ale angajatului la locul de muncă;
- Adoptarea unor reguli clare despre parole;
- Realizarea de copii de rezervă periodică a datelor personale
- Impunerea obligațiilor contractuale asupra organizațiilor importatoare de a lua măsuri de securitate corespunzătoare atunci când transferă date în afara SEE.

Ar trebui să se acorde atenţie riscurilor pe care le prezintă prelucrarea datelor, care pot duce la prejudicii aduse persoanelor fizice ale căror date sunt prelucrate.

4.7 Operatorul trebuie să poată demonstra conformitatea cu celelalte principii ale GDPR (responsabilitatea)

GDPR include prevederi care promovează responsabilitatea și guvernanța. Acestea completează cerințele de transparență ale GDPR. Principiul responsabilității prevăzut la articolul 5 alineatul (2) impune să demonstrați că respectați principiile și afirmați în mod explicit că aceasta este responsabilitatea dvs.

SCM Neuromed va demonstra conformitatea cu principiile protecției datelor prin implementarea politicilor de protecție a datelor, respectarea codurilor de conduită, punerea în aplicare a măsurilor tehnice și organizatorice, precum și adoptarea unor tehnici precum protecția datelor începând cu momentul conceperii, DPIA, procedurile de notificare a încălcărilor și planurile de raspuns la incidente.

5 Drepturile persoanelor vizate

5.1 Persoanele vizate au următoarele drepturi în ceea ce privește prelucrarea datelor și inregistrarile acestor date:

5.1.2 Să solicite acces cu privire la informațiile deținute și referitoare la cei carora le-au fost dezvăluite.

5.1.3 Sa se opuna prelucrarii care ar putea provoca daune sau prejudicii.

5.1.4 Sa se opuna prelucrarii în scopul marketingul direct.

5.1.5 Să fie informați cu privire la procesul decizional individual automatizat, inclusiv crearea de profiluri.

5.1.6 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.

5.1.7 Să solicite despăgubiri în cazul în care suferă daune prin orice încălcare a GDPR.

5.1.8 Să ia măsuri pentru rectificarea, blocarea, ștergerea, inclusiv dreptul de a fi uitat sau distrugerea datelor inexacte.

5.1.9 Să solicite autorității de supraveghere să evalueze dacă o prevedere a GDPR a fost încălcată.

5.1.10 Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal.

5.1.11 Persoana vizată are dreptul de a se opune crearii de profile fara existenta unui consimtamant

5.2 *SCM Neuromed* asigură persoanele vizate ca isi pot exercita aceste drepturi:

5.2.2 Persoanele vizate pot face cereri de acces la date, conform Procedurii de solicitare a accesului persoanei vizate; această procedură descrie, de asemenea, modul în care *SCM Neuromed*se va asigura că răspunsul său la solicitarea de acces la date respectă cerințele GDPR.

5.2.3 Persoanele vizate au dreptul sa depuna o plangere către *SCM Neuromed*în legătură cu prelucrarea datelor lor personale, solicitarile din partea persoanelor vizate si modul în care au fost soluționate plângerile se vor face în conformitate cu procedura privind reclamațiile.

6 Consimțământul

6.1 *SCM Neuromed* înțelege "consimtamantul" ca fiind al persoanei vizate orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate. Persoana vizată își poate retrage consimțământul în orice moment.

6.2 *SCM Neuromed* înțelege că prin "consimtamantul" persoana vizată a fost pe deplin informată cu privire la prelucrarea datelor personale şi a solicitat acordul în timp ce se află într-o stare de spirit adecvată pentru a face acest lucru şi fără a se exercita presiuni asupra ei. Consimțământul obținut sub presiune sau pe baza unor informații înșelătoare nu va constitui o bază valabilă pentru procesare.

6.3 Trebuie să existe o comunicare activă între părți pentru a demonstra consimțământul activ. Consimțământul nu poate fi dedus din lipsa de răspuns la o comunicare. Operatorul trebuie să poată demonstra obtinerea consimțământului pentru operațiunea de procesare.

6.4 Pentru datele sensibile, trebuie obținut un acord scris explicit a persoanelor vizate, cu excepția cazului în care există o bază legala de procesare alternativă.

6.5 În majoritatea cazurilor, consimțământul de prelucrare a datelor personale şi sensibile este obținut în mod obișnuit de *SCM Neuromed* utilizând declaratiile de consimțământ standard.

6.6 În cazul în care *SCM Neuromed* oferă servicii on-line copiilor, trebuie obținut consimtamantul parintelui sau al reprezentantului legal al copilului. Această cerință se aplică copiilor cu vârsta sub 16 ani (cu excepția cazului în care statul membru prevede o limită de vârstă mai mică, care nu poate fi mai mică de 13).

7 Securitatea datelor

7.1 Toți angajații / personalul sunt responsabili pentru a asigura că toate datele personale pe care *SCM Neuromed* le dețin și pentru care este responsabil, sunt păstrate în siguranță și nu sunt divulgate în niciun fel unei terțe părți decât dacă acea terță parte a fost autorizată în mod specific prin *SCM Neuromed* să primească aceste informații și a încheiat un acord de confidențialitate.

7.2 Toate datele personale ar trebui să fie accesibile numai celor care au nevoie să le folosească și accesul poate fi acordat numai în conformitate cu Politica de control al accesului. Toate datele cu caracter personal trebuie procesate in siguranta și trebuie păstrate:

- intr-o camera inchisa cu acces controlat; și / sau
- într-un sertar închis sau într-un dulap; și / sau
- daca sunt pastrate pe computere, protejate prin parolă în conformitate cu cerințele organizatiei din Politica de control al accesului și / sau
- stocate pe suporturi (detașabile) care sunt criptate

7.3 Trebuie avuta grija ca ecranele și terminalele PC să nu fie vizibile decat angajaților/ personalului autorizat al *SCM Neuromed*. Toți angajații / personalul sunt obligați să încheie un acord de utilizare acceptabilă înainte de a li se permite accesul la informațiile organizaționale de orice fel, care detaliază normele privind timpul in care ecranul intra in idle (lock).

7.4 Înregistrările in format fizic nu pot fi lăsate acolo unde pot fi accesate de personal neautorizat și nu pot fi înlăturate din sediu fără autorizație explicită [scrisă]. Imediat ce înregistrările in format fizic nu mai sunt necesare pentru clienții de zi cu zi, acestea trebuie să fie distruse in siguranta, în conformitate cu o anumita procedura

7.5 Datele personale pot fi șterse sau eliminate numai în conformitate cu procedura de păstrare a înregistrărilor. Înregistrările in format fizic care au ajuns la scadenta, trebuie să fie mărunțite și aruncate ca "deșeuri confidențiale".

7.6 Prelucrarea datelor cu caracter personal "în afara sediului" prezintă un risc potențial mai mare decat pierderea, furtul sau deteriorarea datelor cu caracter personal. Personalul trebuie să fie autorizat în mod specific să proceseze datele în afara sediului.

8 Divulgarea datelor

8.1 *SCM Neuromed* trebuie să se asigure că datele cu caracter personal nu sunt divulgate terților neautorizați, care includ membri ai familiei, prieteni, organisme guvernamentale și, în anumite circumstanțe, Poliția. Toți angajații / personalul trebuie să fie atenți atunci când sunt rugați să dezvăluie datele personale deținute de o altă persoană unei terțe părți [și vor fi obligați să participe la o formare specifică care să le permită să gestioneze eficient astfel de riscuri]. Este important să se țină seama de faptul conform caruia divulgarea informațiilor este sau nu relevantă pentru desfășurarea activității *SCM Neuromed*.

8.2 GDPR permite anumite dezvăluiri fără consimțământ atâta timp cât informațiile sunt solicitate pentru unul sau mai multe din următoarele scopuri:

8.2.1 - protejarea securității naționale;

8.2.2 - prevenirea sau depistarea infracțiunilor, inclusiv reținerea sau urmărirea penală a infractorilor;

8.2.3 - îndeplinirea funcțiilor de reglementare (include sănătatea, siguranța și bunăstarea persoanelor la locul de muncă);

8.2.4 - pentru a preveni vătămarea gravă a unui terț;

8.2.5 - pentru a proteja interesele vitale ale individului, aceasta se referă la situațiile de viață și de moarte.

8.3 Toate solicitările de furnizare a datelor pentru unul dintre aceste motive trebuie să fie susținute de o documentație adecvată, iar toate aceste dezvăluiri trebuie să fie autorizate în mod specific de către Responsabilul pentru Protecția Datelor.

9 Pastrarea și eliminarea datelor

9.1 *SCM Neuromed* nu va păstra datele cu caracter personal într-o formă care să permită identificarea persoanelor vizate pentru o perioadă mai lungă decât este necesar, în raport cu scopul (scopurile) pentru care datele au fost colectate inițial.

9.2 *SCM Neuromed* poate stoca date pentru perioade mai lungi în cazul în care datele cu caracter personal vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri științifice sau istorice de cercetare sau în scopuri statistice, sub rezerva punerii în aplicare a măsurilor tehnice și organizatorice adecvate pentru protejarea drepturilor și libertăților persoanei vizate.

9.3 Perioada de păstrare pentru fiecare categorie de date cu caracter personal va fi stabilită în Procedura de păstrare a înregistrărilor împreună cu criteriile utilizate pentru stabilirea acestei perioade, inclusiv obligațiile legale ale *SCM Neuromed* care trebuie să păstreze datele.

9.4 Procedurile de păstrare a datelor și procedurile de stergere a datelor ale *SCM Neuromed* se vor aplica în toate cazurile.

9.5 Datele cu caracter personal trebuie să fie eliminate în siguranță, în conformitate cu al șaselea principiu al GDPR - prelucrate într-un mod adecvat pentru a menține securitatea, protejând astfel "drepturile și libertățile" persoanelor vizate. Orice eliminare a datelor se va face în conformitate cu procedura de stergere.

10 Transferuri de date

11.1Toate transferurile de date din Spațiul Economic European (SEE) către țările din Spațiul Economic Neeuropean (menționate în GDPR ca "țări terțe") sunt ilegale, cu excepția cazului în care există un "nivel adecvat de protecție a drepturilor fundamentale ale persoanele vizate ".

Transferul de date cu caracter personal în afara SEE este interzis, cu excepția cazului în care se aplică una sau mai multe garanții sau excepții specificate:

10.1.1 O decizie de adecvare

Transferul de date cu caracter personal către o ţară terţă sau o organizaţie internaţională se poate realiza atunci când Comisia a decis că ţara terţă, un teritoriu ori unul sau mai multe sectoare specificate din acea ţară terţă sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat. Transferurile realizate în aceste condiţii nu necesită autorizări speciale. Țările care sunt membre ale Spațiului Economic European (SEE), dar nu și ale UE sunt acceptate ca îndeplinind condițiile unei decizii de adecvare.

O listă a țărilor care îndeplinesc în prezent cerințele de adecvare ale Comisiei este publicată în Jurnalul Oficial al Uniunii Europene. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

10.1.2 Privacy Shield

Dacă *SCM Neuromed* dorește să transfere date personale din UE unei organizații din Statele Unite, ar trebui să verifice dacă organizația este înscrisă în cadrul Privacy Shield la Departamentul de Comerț din S.U.A. Obligația aplicabilă societăților inscrise in Privacy Shield este inclusă în Principiile privind confidentialitatea datelor. Departamentul de Comerț din S.U.A este responsabil pentru gestionarea și administrarea Privacy Shield și pentru asigurarea faptului că organizatiile își respectă angajamentele. Pentru a se putea certifica, companiile trebuie să aibă o politică de confidențialitate în conformitate cu principiile de confidențialitate, de ex. utilizare, stocare și transfer de date personale în conformitate cu un set puternic de reguli și garanții de protecție a datelor. Protecția datelor cu caracter personal se aplică indiferent dacă datele cu caracter personal au legătură cu un rezident al UE sau nu. Organizațiile trebuie să-și reînnoiască "statutul de membru" in cadrul Privacy Shield în fiecare an. Dacă nu, ele nu mai pot primi și utiliza datele cu caracter personal din UE.

<u>Evaluarea adecvării de către operatorul de date</u>

La evaluarea adecvării, operatorul care transfera date din UK ar trebui să țină seama de următorii factori:

- natura informațiilor transferate;
- țara sau teritoriul de origine și destinația finală a informațiilor;
- modul în care informațiile vor fi utilizate și pentru cât timp;
- legile și practicile țării cesionarului, inclusiv practicile în materie de protecţie a datelor cu caracter personal relevante și obligațiile internaționale; și
- măsurile de securitate care trebuie luate în ceea ce privește datele din locația externa (valabil doar pentru UK)

10.1.3 Reguli corporatiste obligatorii

SCM Neuromed poate adopta reguli corporatiste obligatorii aprobate pentru transferul de date în afara UE. Acest lucru necesită prezentarea către autoritatea de supraveghere competentă spre aprobare a regulilor pe care încearcă să se bazeze *SCM Neuromed*.

10.1.4 Clauze de contract standard

SCM Neuromed poate adopta clauze contractuale standard aprobate pentru transferul de date în afara SEE. Dacă *SCM Neuromed* adoptă [clauzele contract standard aprobat de autoritatea de supraveghere competentă], atunci există o recunoaștere automată a gradului de adecvare.

10.1.5 Excepţii

În lipsa unei decizii de adecvare, a calitatii de membru a Privacy Shield, a regulilor corporatiste obligatorii și / sau a clauzelor de contract standard, transferul datelor cu caracter personal într-o țară terță sau într-o organizație internațională are loc numai în următoarele condiții:

- persoana vizată și-a dat acordul în mod explicit cu privire la transferul propus, după ce a fost informat cu privire la riscurile posibile ale unor astfel de transferuri pentru persoana vizată, din cauza lipsei unei decizii de adecvare și a garanțiilor adecvate;
- transferul este necesar pentru executarea unui contract între persoana vizată și operator sau implementarea măsurilor precontractuale luate la cererea persoanei vizate;
- transferul este necesar pentru încheierea sau executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;
- transferul este necesar din motive importante de interes public;
- transferul este necesar pentru stabilirea, exercitarea sau apărarea revendicărilor legale; și / sau

- transferul este necesar pentru a proteja interesele vitale ale persoanei vizate sau ale altor persoane, în cazul în care persoana vizată nu este capabilă din punct de vedere fizic sau legal să-și dea consimțământul.

11 Sistem de evidenţă a activităţilor de prelucrare si cartografierea datelor

11.1 *SCM Neuromed* a stabilit un Sistem de evidenţă a activităţilor de prelucrare și CARTOGRAFIERE A DATELOR, ca parte a strategiei sale de abordare a riscurilor și a oportunităților în cadrul proiectului său de conformitate cu GDPR. Sistemul de evidenţă a a activităţilor de prelucrare și cartografierea datelor se refera la

- procesele care utilizează date cu caracter personal;
- sursa datelor personale;
- volumul de date corespunzatoare persoanelor vizate;
- descrierea fiecărui element de date cu caracter personal;
- activitatile de prelucrare;
- menținerea inventarului de categorii de date prelucrate;
- documentarea scopului (scopurilor) pentru care se utilizează fiecare categorie de date cu caracter personal;
- destinatarii și potențialii beneficiari ai datelor cu caracter personal;
- rolul *SCM Neuromed* pe întregul flux de date;
- sisteme de stocare;
- orice transfer de date; și
- toate cerințele privind păstrare și stergerea datelor cu caracter personal.

11.2 *SCM Neuromed* este conștient de orice riscuri asociate procesării anumitor tipuri de date cu caracter personal.

11.2.1 *SCM Neuromed* evaluează nivelul riscului pentru procesarea datelor cu caracter personal ale persoanelor vizate. **Evaluările impactului privind protecția datelor (DPIAs)** se efectuează tinand seama de prelucrarea datelor cu caracter personal de catre *SCM Neuromed* și de prelucrarea efectuată de alte organizații în numele *SCM Neuromed*

11.2.2 *SCM Neuromed* trebuie să gestioneze orice riscuri identificate de evaluarea riscurilor pentru a reduce probabilitatea neconformității cu această politică.

11.2.3 Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal. O evaluare unică poate aborda un set de operaţiuni de prelucrare similare care prezintă riscuri ridicate similare.

11.2.4 În cazul în care, rezultatul DPIA releva fapul că *SCM Neuromed* este pe cale sa inceapa o prelucrare a datelor cu caracter personal care ar putea cauza daune și / sau prejudicii persoanelor vizate, decizia de a incepe procesarea de catre *SCM Neuromed* revine responsabilului cu protecția datelor.

11.2.5 Responsabilul cu protecția datelor trebuie sa anunte aceasta situatie autorității de supraveghere, în cazul în care există motive de îngrijorare semnificative, fie în legătură cu daune și / sau prejudicii, fie cu volumul de date.

11.2.6 Alegerea de Standarde de securitate adecvate [ex: ISO 27001, etc.] și aplicarea lor pentru a reduce nivelul de risc asociat procesării datelor individuale la un nivel acceptabil

Aprobarea procedurii

Acest document a fost aprobat de catre Responsabilul cu Protectia Datelor si este responsabil ca prezenta procedura sa fie revizuita in conformitate cu cerintele revizuite ale *Regulamentului General de Prelucrare a Datelor (EU GDPR)*.

O editie actualizata a acestei proceduri este disponibila [tuturor/ celor specificati] membrilor organizatiei pe www.neuromed.ro.

Aceasta politica a fost aprobata de catre Consiliul de Administratie al organizatiei la 23.05.2018 si emisa intr-o versiune revizuita sub semnatura Presedintelui.

Semnatura Data 23.05.2018

Situatia editiilor si a reviziilor in cadrul editiilor procedurii:

Editia	Componenta revizuita	Aprobare	Data editiei
1	Editia 1	Presedinte	23.05.2018