Politica ARENSIA privind confidenţialitatea şi protecţia datelor

I. Politica privind protecţia datelor

În cadrul operaţiunilor noastre, ARENSIA Exploratory Medicine asigură conformitatea necesară cu nivelul înalt de protecţie a datelor personale şi cerinţele complexe ale Regulamentului General privind Protecţia Datelor (RGPD). Prezenta politică se referă la toate părţile – angajaţi, furnizori de servicii, pacienţi şi sponsori – care furnizează orice volum de informații companiei noastre.

Politica privind protecţia datelor se aplică Companiei ARENSIA Exploratory Medicine la nivel internaţional şi are drept fundament principiile de bază referitoare la protecţia datelor, acceptate la nivel global. Pentru transmiterea transfrontalieră a datelor între unităţile companiei, politica stipulează una dintre condiţiile cadru necesare, asigurând nivelul adecvat de protecţie a datelor prevăzut de Regulamentul General privind Protecţia Datelor[1].

II. Aplicarea legilor naţionale

RGPD se aplică nu numai în cazul organizaţiilor situate pe teritoriul UE, dar şi organizaţiilor situate în afara UE, dacă acestea furnizează bunuri sau servicii pentru, sau monitorizează comportamentul subiecţilor datelor din UE. Se aplică tuturor companiilor care prelucrează şi deţin date cu caracter personal ale subiecţilor datelor cu reşedinţa în Uniunea Europeană, indiferent de localizarea companiei.

III. Definiţii asociate Politicii privind protecţia datelor

„*Date cu caracter personal*" înseamnă orice informaţii care se referă la o persoană fizică identificată sau identificabilă („subiectul datelor"); o persoană fizică identificabilă este o persoană care poate fi identificată, în mod direct sau indirect, în particular prin referire la un element de identificare precum numele, un număr de identificare, date privind localizarea, un element de identificare online sau unul sau mai mulţi factori specifici pentru identitatea fizică, fiziologică, genetică, mentală, economică, culturală sau socială a respectivei persoane fizice;

„Procesare" înseamnă orice operaţiune sau set de operaţiuni care este realizată asupra datelor cu caracter personal sau seturilor de date cu caracter personal, indiferent dacă prin mijloace automatizate sau nu, respectiv obţinerea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, recuperarea, consultarea, utilizarea, divulgarea prin transmitere, difuzarea sau punerea la dispoziţie prin alte mijloace, alinierea sau asocierea, restricţionarea, eliminarea sau distrugerea;

„Operatorul de date personale" este o persoană fizică sau juridică, o autoritate publică, o agenţie sau un alt organism care, separat sau împreună cu alţii, stabileşte scopurile şi mijloacele prelucrării datelor cu caracter personal; în situaţia în care scopurile şi mijloacele prelucrării datelor sunt stabilite prin legislaţia UE sau a unui Stat Membru, operatorul sau criteriile specifice pentru desemnarea sa pot fi prevăzute de legislaţia UE sau legislaţia Statului Membru;

„Procesatorul de date personale" este o persoană fizică sau juridică, o autoritate publică, o agenţie sau un alt organism care prelucrează datele cu caracter personal în numele operatorului de date personale;

[1] Regulamentul (UE) 2016/679 (Regulamentul General privind Protecţia Datelor) –

„Destinatarul” este o persoană fizică sau juridică, o autoritate publică, o agenţie sau un alt organism către care sunt divulgate datele cu caracter personal, indiferent dacă este o terţă parte sau nu. Cu toate acestea, nu vor fi considerate destinatari autorităţile publice care pot primi date cu caracter personal în contextul unei anchete particulare desfăşurate în conformitate cu legislaţia UE sau legislaţia unui Stat Membru; prelucrarea acestor date de către astfel de autorități publice se va face în conformitate cu normele aplicabile privind protecţia datelor, şi în funcţie de scopurile prelucrării.

„Terţă parte” înseamnă o persoană fizică sau juridică, o autoritate publică, o agenţie sau un alt organism, altul/alta decât subiectul datelor, operatorul datelor, procesatorul datelor, şi persoanele care, sub directa autoritate a operatorului sau procesatorului, sunt autorizate să prelucreze datele cu caracter personal;

„Consimţământul” subiectului datelor înseamnă orice indicaţie specifică şi lipsită de echivoc, exprimată în mod liber şi în deplină cunoştinţă de cauză, a dorinţelor subiectului datelor, prin care acesta/aceasta, sub forma unei declaraţii sau printr-o acţiune afirmativă clară, îşi manifestă acordul faţă de prelucrarea datelor sale cu caracter personal;

„Prelucrare transfrontalieră” înseamnă prelucrarea datelor cu caracter personal care are loc în contextul activităţilor desfăşurate la un singur sediu al unui operator sau procesator din UE, dar care afectează în mod semnificativ sau există posibilitatea să afecteze în mod semnificativ subiecţii datelor în mai mult de un Stat Membru.

„Responsabilul cu Protecţia Datelor” (RPD) este o persoană desemnată de operatorul şi de procesatorul de date personale pentru a îndeplini obligaţiile şi responsabilităţile prevăzute la nivelul Uniunii Europene. Această persoană nu primeşte instrucţiuni cu privire la exercitarea atribuţiilor sale, nu va suporta penalizări în legătură cu îndeplinirea atribuţiilor sale, se subordonează direct celui mai înalt nivel de conducere şi îşi asumă obligaţii de păstrare a secretului profesional sau confidenţialităţii cu privire la realizarea atribuţiilor sale. Atribuţiile RPD sunt menţionate în secţiunea XII.

IV. Principiile prelucrării datelor cu caracter personal

1. Legitimitate, corectitudine şi transparenţă

Datele cu caracter personal trebuie prelucrate în spiritul legii, şi într-o manieră corectă şi transparentă în relaţia cu subiectul datelor.

2. Limitarea scopurilor

Datele cu caracter personal trebuie obţinute în scopuri specificate, explicite şi legitime, şi nu trebuie prelucrate în continuare într-o manieră care este incompatibilă cu aceste scopuri; prelucrarea în continuare în scopurile arhivării în interesul public, pentru scopuri de cercetare științifică sau istorică sau în scopuri statistice nu va fi considerată, conform Art. 89(1)[2], ca fiind incompatibilă cu scopurile iniţiale.

3. Minimizarea şi acurateţea datelor

Datele cu caracter personal obţinute trebuie să fie adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate. Datele trebuie să fie corecte şi, acolo unde este necesar, menţinute în formă actualizată; trebuie luate toate măsurile rezonabile pentru a se asigura

[2] Art. 89 Măsuri de protecţie şi derogări RGPD referitoare la prelucrarea în scopurile arhivării în interes public, în scopuri de cercetare ştiinţifică sau istorică sau în scopuri statistice – https://gdpr-info.eu/art-89-gdpr/

ştergerea sau rectificarea fără întârziere a acelor date cu caracter personal care sunt inexacte din perspectiva scopurilor pentru care sunt prelucrate.

4. Limitarea intervalului de păstrare

Datele cu caracter personal trebuie păstrate într-o formă care permite identificarea subiecţilor datelor pentru o perioadă de timp nu mai îndelungată decât este necesar în scopurile pentru care sunt prelucrate datele cu caracter personal; datele cu caracter personal pot fi păstrate pentru intervale mai îndelungate de timp în măsura în care datele cu caracter personal vor fi prelucrate exclusiv în scopurile arhivării în interes public, în scopuri de cercetare ştiinţifică sau istorică, sau în scopuri statistice, conform Art. 89(1)[3], cu condiţia implementării măsurilor tehnice şi organizatorice corespunzătoare prevăzute de acest Regulament în vederea protejării drepturilor şi libertăţilor subiectului datelor.

5. Integritate şi confidenţialitate

Datele obţinute trebuie prelucrate într-o manieră care asigură securitatea corespunzătoare a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale, precum şi împotriva pierderii, distrugerii sau deteriorării accidentale, utilizând măsuri tehnice sau organizatorice potrivite.

V. Credibilitatea prelucrării datelor

Obţinerea, prelucrarea şi utilizarea datelor cu caracter personal este permisă doar în conformitate cu următoarele baze legale ale RGPD. Confidenţialitatea şi securitatea datelor cu caracter personal obţinute reprezintă o prioritate pentru ARENSIA Exploratory Medicine şi este în egală măsură important pentru ARENSIA ca toată lumea să înţeleagă modul în care gestionăm aceste date:

1. Datele pacientului

Pentru desfăşurarea unui studiu clinic în conformitate cu Declaraţia de la Helsinki şi cu ghidul Comisiei Internaţionale pentru Armonizare (*International Committee of Harmonization* - ICH) pentru Buna Practică în Studiul Clinic (BPSC), adunăm date în parametrii prevăzuţi în protocolul de studiu aprobat şi avizat favorabil. Astfel de date pot include informaţii referitoare la starea sănătăţii şi alte date sensibile.

2. Datele angajatului

Pentru desfăşurarea activităţii de afaceri la nivel global şi pentru respectarea reglementărilor de stat (codul muncii, legislaţie fiscală, asigurări, etc.), adunăm diverse date cu caracter personal şi alte tipuri de date în funcţie de responsabilităţile dvs. de serviciu, naţionalitate, situarea locului de muncă şi alţi factori.

Astfel de date pot include:

- Numele;
- Codul numeric personal;
- Numărul de telefon;
- Adresa e-mail;
- Datele bancare şi alte informaţii financiare;

[3] Art. 89 Măsuri de protecţie şi derogări RGPD referitoare la prelucrarea în scopurile arhivării în interes public, în scopuri de cercetare ştiinţifică sau istorică sau în scopuri statistice – https://gdpr-info.eu/art-89-gdpr/

- Numere de identificare faţă de instituţiile statului – numere de asigurări sociale, codul fiscal, permisul de conducere;
- Date referitoare la familie

Putem utiliza datele după cum urmează:

- pentru identificarea personală a unui individ;
- pentru comunicarea cu o persoană;
- pentru respectarea cerinţelor de resurse umane;
- pentru respectarea reglementărilor de stat;
- pentru asigurarea beneficiilor angajaţilor (despăgubiri, asigurare de sănătate, rambursări ale cheltuielilor, etc.)

3. Datele clienţilor şi ale terţilor

În vederea desfăşurării activităţii de afaceri şi pentru îndeplinirea obligaţiilor contractuale, adunăm date ale partenerilor contractuali, precum sponsorii, sub-contractorii şi furnizorii de servicii. Astfel de date pot include numele, adresa email de serviciu, numărul de telefon de la birou, datele bancare şi alte informaţii financiare ale companiei. ARENSIA ia măsuri de precauţie pentru a împiedica divulgarea datelor cu caracter personal către terţi, altfel decât în conformitate cu instrucţiunile, şi cu limitare la divulgări către agenţi şi sub-contractori ai furnizorului de servicii, şi în situaţia în care ARENSIA a primit acordul prealabil în scris al clientului sau terţei părţi, sau în situaţia în care respectiva divulgare este prevăzută prin lege.

VI. Prelucrarea datelor contractuale

Prelucrarea datelor „în numele operatorului" înseamnă că un furnizor de servicii este angajat să prelucreze datele cu caracter personal, fără a i se atribui vreo responsabilitate pentru activitatea de afaceri asociată. În aceste situaţii, trebuie încheiat un *acord de protecţie a datelor prelucrate în numele operatorului* cu furnizorii externi şi între afiliaţii din cadrul companiei ARENSIA. Clientul reţine responsabilitatea deplină pentru realizarea corectă a prelucrării datelor. Furnizorul de servicii poate prelucra datele cu caracter personal doar conform cu instrucţiunile primite de la client. Astfel de servicii ar putea fi utilizate pentru contabilitatea salariilor la nivel local.

VII. Drepturile subiectului datelor

1. Dreptul de acces

Printre drepturile extinse ale subiecţilor datelor subliniate de RGPD este şi dreptul subiectului datelor de a obţine de la operatorul de date confirmarea dacă datele cu caracter personal care îl privesc sunt sau nu în curs de prelucrare, unde şi în ce scop. Totodată, operatorul de date va furniza gratuit o copie a datelor cu caracter personal, în format electronic. Această modificare este o schimbare dramatică în sensul transparenţei datelor şi asigurării de mai multe drepturi pentru subiecţii datelor.

2. Dreptul de rectificare

Subiectul datelor va avea dreptul de a obţine de la operatorul datelor, fără nicio întârziere nejustificată, rectificarea datelor cu caracter personal inexacte care îl/o privesc. Având în vedere scopurile prelucrării,

subiectul datelor va avea dreptul să ceară completarea datelor cu caracter personal incomplete, inclusiv mijloacele de furnizare a unei declaraţii suplimentare.

3. Dreptul de a fi uitat

Cunoscut şi sub denumirea de ştergere a datelor, dreptul de a fi uitat permite subiectului datelor să ceară operatorului datelor să şteargă datele sale cu caracter personal, să oprească difuzarea acestor date, şi posibil să solicite terţilor să oprească prelucrarea datelor. Condiţiile pentru ştergerea datelor includ ca datele să nu mai fie relevante pentru scopurile iniţiale ale prelucrării, sau retragerea consimţământului de către subiectul datelor. De asemenea, trebuie reţinut faptul că acest drept solicită operatorilor de date să compare drepturile subiecţilor cu „interesul public în cazul disponibilității datelor" atunci când iau în considerare astfel de cereri.

4. Dreptul la restricţionarea prelucrării

Condiţiile pentru exprimarea consimţământului sunt întărite, deoarece solicitarea consimţământului se face într-o formă inteligibilă şi uşor accesibilă, scopul prelucrării datelor fiind precizat printr-o anexă la respectivul consimţământ. Consimţământul este clar şi delimitat de alte aspecte, şi este furnizat într-o formă inteligibilă şi uşor de accesat, utilizându-se un limbaj neechivoc şi simplu în fiecare document furnizat de ARENSIA: contracte de muncă, contracte cu clienţii şi cu furnizorii, inclusiv documente asigurate de Sponsor prin intermediul ARENSIA. Respectiv Formularul de consimţământ informat (FCI). Retragerea consimţământului este la fel de uşor de realizat ca şi exprimarea acestuia.

5. Dreptul la transferabilitatea datelor

RGPD introduce transferabilitatea datelor – dreptul subiectului datelor de a primi datele cu caracter personal care îl privesc, pe care le-a furnizat anterior într-un „format de uz comun şi care poate fi citit de calculator" şi de a transmite datele respective către un alt operator de date.

6. Dreptul de a obiecta

Pe baza acestor prevederi, subiectul datelor va avea dreptul de a obiecta oricând, din motive referitoare la situaţia sa particulară, faţă de prelucrarea datelor cu caracter personal care îl/o privesc. Operatorul datelor nu va mai prelucra datele cu caracter personal dacă nu demonstrează că există motive legitime care îl obligă să efectueze prelucrarea datelor şi care prevalează faţă de interesele, drepturile şi libertăţile subiectului datelor, sau pentru înaintarea, exercitarea sau apărarea acţiunilor în justiţie.

VIII. Confidenţialitatea prelucrării datelor

Datele cu caracter personal fac obiectul obligaţiei de menţinere a confidenţialităţii datelor. Este interzisă orice obţinere, prelucrare sau utilizare neautorizată a acestor date de către angajat. Nu este permisă nicio prelucrare a datelor de către un angajat care nu a fost autorizat să facă acest lucru în cadrul atribuţiilor sale legitime. Se aplică principiul „necesităţii de a cunoaşte". Angajaţii pot avea acces la informaţiile personale doar în măsura în care acest lucru este necesar pentru tipul şi sfera de aplicare a atribuţiei în cauză. Pentru acest lucru este nevoie de repartizarea şi separarea atentă, precum şi de implementarea anumitor roluri şi responsabilităţi.

Angajaţilor li se interzice să utilizeze datele cu caracter personal în scopuri particulare sau comerciale, să le divulge persoanelor neautorizate, sau să le pună oricui la dispoziţie în orice alt mod. Supraveghetorii trebuie să îşi informeze angajaţii la începutul relaţiei de muncă despre obligaţia de proteja

confidenţialitatea datelor. Această obligaţie va rămâne în vigoare chiar şi după încetarea contractului de muncă.

IX. Securitatea prelucrării datelor

Datele cu caracter personal trebuie să fie protejate de accesul neautorizat şi de prelucrarea sau divulgarea ilegală, precum şi de pierderea, modificarea sau distrugerea accidentală. Acest lucru este valabil indiferent dacă datele sunt prelucrate electronic sau pe hârtie. Înainte de introducerea de noi metode pentru prelucrarea datelor, în special de noi sisteme IT, trebuie definite şi puse în aplicare măsuri tehnice şi organizatorice de protejare a datelor cu caracter personal. Aceste măsuri trebuie să se bazeze pe tehnologia curentă, riscurile prelucrării şi necesitatea de protejare a datelor.

În particular, departamentul responsabil se poate consulta cu serviciul IT sau cu Responsabilul cu Protecţia Datelor (RPD). Măsurile tehnice şi organizatorice pentru protejarea datelor cu caracter personal fac parte din atribuţiile Responsabilului cu Protecţia Datelor şi trebuie adaptate continuu la progresul tehnic şi modificările organizatorice.

X. Controlul protecţiei datelor

Respectarea Politicii privind protecţia datelor şi a legilor aplicabile referitoare la protecţia datelor este verificată în mod periodic prin audituri asupra protecţiei datelor şi alte forme de control. Realizarea acestor controale este responsabilitatea RPD şi a altor unităţi ale companiei cu drepturi de audit sau a auditorilor externi angajaţi în acest scop. Rezultatele controalelor privind protecţia datelor trebuie raportate către RPD. Conducerea ARENSIA Exploratory Medicine trebuie informată despre rezultatele principale în cadrul obligaţiilor de raportare asociate. La cerere, rezultatele controalelor privind protecţia datelor vor fi puse la dispoziţia autorităţii responsabile cu protecţia datelor. Autoritatea responsabilă cu protecţia datelor poate efectua propriile controale privind conformitatea cu prevederile prezentei Politici, în măsura permisă de legea naţională.

XI. Incidente, responsabilităţi şi sancţiuni asociate protecţiei datelor

Reglementările propuse cu privire la încălcări ale securităţii datelor se referă in principal la politicile de notificare ale companiilor care au suferit încălcări ale securităţii datelor. Încălcările securităţii datelor care pot reprezenta un risc pentru persoanele fizice (de exemplu, o dezvăluire neautorizată a numărului de cont bancar sau a detaliilor privind asigurarea de sănătate) trebuie comunicate Agenţiei respective de protecţie a datelor în decurs de 72 de ore, precum şi persoanelor afectate, fără nicio întârziere nejustificată.

XII. Responsabilul cu Protecţia Datelor (RPD)

Un responsabil cu protecţia datelor (RPD) este o funcţie de conducere în cadrul departamentului de securitate al companiei, solicitată de Regulamentul General privind Protecţia Datelor (RGPD). Responsabilii cu protecţia datelor au responsabilitatea de a supraveghea strategia de protecţie a datelor şi implementarea acesteia, pentru a asigura conformitatea cu normele RGPD.

Responsabilităţile RPD:

- Instruirea departamentelor şi angajaţilor companiei cu privire la cerinţele de conformitate importante
- Pregătirea personalului implicat în prelucrarea datelor

- Desfăşurarea de audituri pentru asigurarea conformităţii şi abordarea în mod proactiv a posibilelor probleme
- Acţionarea ca persoană de contact între companie şi autorităţile de supraveghere RGPD
- Monitorizarea performanţei şi furnizarea de recomandări privind impactul eforturilor de protecţie a datelor
- Întocmirea unor evidenţe cuprinzătoare privind toate activităţile de prelucrare a datelor desfăşurate de companie, inclusiv scopul tuturor activităţilor de prelucrare, care trebuie făcute publice la cerere
- Interacţionarea cu subiecţii datelor pentru a-i informa despre modul în care sunt utilizate datele lor, despre drepturile pe care le au de a solicita ştergerea datelor lor cu caracter personal, şi ce măsuri are compania instituite pentru protejarea informaţiilor lor personale.

XIII. Protecţia datelor la ARENSIA

Principiile descrise în prezenta Politică şi prevăzute de RGPD sunt implementate in cadrul sistemelor ARENSIA prin *Instrucţiunile de lucru* respective, care acoperă domeniile menţionate.