FRESENIUS KABI
caring for life

Politica Fresenius Kabi - Reguli corporative obligatorii privind protecția datelor

Cuprins

1 Obiectiv

Grupul Fresenius își desfășoară activitatea la nivel mondial. Aceasta include țări în care au fost sau nu adoptate legi privind protecția datelor. Pentru a reglementa în mod consecvent modul în care sunt manipulate sau prelucrate datele cu caracter personal și ca parte a respectării de către Grupul Fresenius a legilor aplicabile privind protecția datelor, părțile participante la BCR respectă un set intern de BCR pentru prelucrarea datelor cu caracter personal, pentru a crea un nivel uniform și adecvat de protecție a datelor în toate entitățile participante la nivel mondial. Esența BCR este de a armoniza standardul de protecție a datelor în cadrul Grupului Fresenius la un nivel de protecție a datelor în conformitate cu standardele UE. Acest lucru permite un schimb de Date cu caracter personal între toate Părțile cu un nivel adecvat de protecție a datelor la nivel global.

Una dintre principalele părți interesate pentru asigurarea unui nivel adecvat de protecție a datelor este grupul de angajați care prelucrează date cu caracter personal în entitatea Fresenius respectivă. Numai dacă acești angajați sunt conștienți de modul în care trebuie prelucrate datele cu caracter personal și de restricțiile care se aplică, se poate atinge un nivel adecvat de protecție a datelor.

Prezentele BCR conțin garanțiile esențiale și stabilesc domeniul de aplicare, obiectivele, principiile și structura acestora.

2 Abrevieri și termeni

2.1 Abrevieri

Abrevierea	Definiție
BCR	Reguli corporative obligatorii (Binding Corporate Rules)
DPA	Consilier pentru protecția datelor
DPIA	Evaluări ale impactului asupra protecției datelor
DPO	Responsabil cu protecția datelor
SEE	Spațiul Economic European
UE	Uniunea Europeană
GDPR	Regulamentul general privind protecția datelor
LDPA	Consilier local pentru protecția datelor

2.2 Termeni

În prezentele BCR, termenii cu majuscule au următoarele semnificații:

Termen	Definiție
Legile aplicabile privind protecția datelor	înseamnă legislația privind protecția datelor dintr-o jurisdicție în vigoare și aplicabilă unei părți
Legi aplicabile	înseamnă totalitatea legilor dintr-o jurisdicție în vigoare și aplicabile unei părți, cu excepția Legilor aplicabile privind protecția datelor
BCR	înseamnă prezentul document și toate anexele sale
Operator	înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu alte persoane, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal
Consilier pentru protecția datelor	înseamnă consilierul în materie de protecție a datelor numit în cadrul grupului Fresenius la nivel central
Evaluări ale impactului asupra protecției datelor	înseamnă o anumită evaluare a riscurilor în vederea identificării și evaluării riscurilor de confidențialitate pentru activitățile de prelucrare a datelor, care ar putea avea ca rezultat un risc ridicat pentru drepturile și libertățile persoanelor fizice, în vederea atenuării acestor riscuri ridicate
Responsabil cu protecția datelor	înseamnă responsabilul cu protecția datelor numit în cadrul Grupului Fresenius în conformitate cu art. 37 GDPR, care nu primește instrucțiuni privind exercitarea sarcinilor sale
Organizația pentru protecția datelor	înseamnă organizația de protecție a datelor a fiecărei părți, formată din consilierul (consilierii) local(i) pentru protecția datelor și (în cazul în care este necesar din punct de vedere legal) responsabilul respectiv cu protecția datelor
Angajat(ă)	înseamnă orice membru al conducerii sau orice persoană care are o relație de muncă sau cvasi-angajare cu o Parte, cum ar fi angajați, lucrători temporari, ucenici, stagiari, participant la activități de internship, precum și consultanți și orice alte persoane integrate în procesele operaționale ale părții respective.
Acord-cadru	înseamnă contractul dintre părți pentru aderarea la BCR
Grupul Fresenius	în sensul prezentelor BCR înseamnă Fresenius SE & Co. KGaA ("FSE") și toate filialele sale în conformitate cu sec. 15 și următoarele din Legea germană privind societățile pe acțiuni ("Entitatea Fresenius"), cu excepția celor care aparțin segmentelor de activitate Fresenius Kabi, Fresenius Medical Care, Fresenius Helios și Fresenius Vamed; precum și Fresenius Kabi Aktiengesellschaft ("FK AG") și toate filialele sale în conformitate cu sec. 15 și următoarele din Legea germană privind societățile pe acțiuni care aparțin segmentului de afaceri Fresenius Kabi
Prelucrare ulterioară	înseamnă Prelucrarea datelor cu caracter personal de către o Parte situată în afara UE/SEE, în cazul în care datele cu caracter personal au fost inițial transferate de către o Parte obligată de GDPR
Regulamentul general privind protecția datelor	înseamnă Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE
Persoană (persoane)	înseamnă o persoană fizică identificată sau identificabilă; o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un identificator, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online sau la unul sau mai mulți factori specifici identității fizice, fiziologice, genetice, mentale, economice, culturale sau sociale a persoanei fizice respective
Consilier local pentru protecția datelor	înseamnă consilierul local pentru protecția datelor numit în cadrul grupului Fresenius la nivel local
Transfer în continuare	înseamnă transferul de date cu caracter personal de către o Parte situată în afara UE/SEE către un alt destinatar situat în afara UE/SEE, în cazul în care datele cu caracter personal au fost inițial transferate de către o Parte obligată de GDPR
Partea sau părțile	înseamnă entitățile din cadrul grupului Fresenius obligate de BCR și specificate în Global-ANNEX-LE-000067674 Lista părților obligate de BCR.
Date cu caracter personal	înseamnă orice informație referitoare la o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană

Termen	Definiție
	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, un identificator online sau la unul sau mai multe elemente specifice identității fizice, fiziologice, genetice, mentale, economice, culturale sau sociale a persoanei fizice respective
Prelucrare	înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra unor seturi de date cu caracter personal, indiferent dacă sunt sau nu efectuate prin mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.
Persoană împuternicită	înseamnă o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism care prelucrează date cu caracter personal în numele operatorului
Categorii speciale de date cu caracter personal	înseamnă date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice sau apartenența la un sindicat, precum și prelucrarea informațiilor genetice, a informațiilor biometrice în scopul identificării unice a unei persoane, a informațiilor privind sănătatea sau a informațiilor privind viața sexuală sau orientarea sexuală a unei persoane.
Autoritatea de supraveghere	înseamnă o autoritate publică independentă care este instituită de un stat membru în conformitate cu articolul 51 din GDPR
Autoritatea de supraveghere în cauză	înseamnă o autoritate de supraveghere care este vizată de prelucrarea datelor cu caracter personal de către o Parte, deoarece: ▪ Partea respectivă este stabilită pe teritoriul statului membru al autorității de supraveghere respective; ▪ Persoanele fizice care locuiesc în statul membru al autorității de supraveghere respective sunt afectate în mod substanțial sau pot fi afectate în mod substanțial de prelucrare; sau a fost depusă o plângere la autoritatea de supraveghere respectivă
Destinatarul terț	înseamnă un destinatar de date cu caracter personal care nu este parte la BCR
Transfer	înseamnă orice comunicare de date cu caracter personal de la un operator către un alt operator, către o persoană împuternicită sau către orice alt destinatar

În măsura în care termenii nu sunt specificați în această secțiune, se aplică definiția documentului BCR#16 și definițiile conform GDPR.

3 Domeniul de aplicare

3.1 Domeniul de aplicare teritorial

i. BCR se **aplică** în următoarele scenarii:

- Orice prelucrare a datelor cu caracter personal de către părțile situate în UE/SEE (inclusiv transferurile către alte părți, indiferent dacă destinatarii sunt situați în interiorul sau în afara UE/SEE)[1] ;
- Orice prelucrare a datelor cu caracter personal de către părți situate în afara UE/SEE, în cazul în care o astfel de prelucrare este efectuată "în contextul

[1] Art. 3 alin.1 GDPR

activităților unei organizații" a Grupului Fresenius în UE/SEE (inclusiv transferurile către alte părți, indiferent dacă destinatarii sunt situați în interiorul sau în afara UE/SEE) [1] ;

- Orice prelucrare a datelor cu caracter personal ale persoanelor fizice rezidente în UE/SEE, de către părți situate în afara UE/SEE, în cazul în care o astfel de prelucrare este legată de (i) oferirea de bunuri sau servicii persoanelor fizice din UE/SEE, indiferent dacă este necesară o plată din partea persoanei fizice sau (ii) monitorizarea comportamentului acestora, în măsura în care comportamentul lor are loc în UE/SEE (inclusiv transferurile către alte părți, indiferent dacă destinatarii sunt situați în interiorul sau în afara UE/SEE).[2]
- Orice prelucrare ulterioară a datelor cu caracter personal de către părți situate în afara UE/SEE, în cazul în care datele cu caracter personal afectate au fost inițial transferate de către o Parte obligată de GDPR;
- Orice transfer ulterior de date cu caracter personal de către părți situate în afara UE/SEE către un alt destinatar situat în afara UE/SEE, în cazul în care datele cu caracter personal afectate au fost inițial transferate de către o Parte obligată de GDPR.

ii. BCR **nu se aplică** în cazul prelucrării datelor cu caracter personal de către părți situate în afara UE/SEE, în cazul în care o astfel de prelucrare nu este nici

- prestate "în contextul activităților unei organizații" a Fresenius în UE/SEE1
- nici legate de (i) oferirea de bunuri sau servicii persoanelor fizice din UE/SEE, indiferent dacă este necesară o plată din partea persoanei fizice sau (ii) monitorizarea comportamentului acestora, în măsura în care comportamentul lor are loc în UE/SEE,
- nici în ceea ce privește datele cu caracter personal care au fost transferate inițial de către o Parte obligată prin GDPR.

3.2 Domeniul de aplicare material și personal

i. BCR se aplică prelucrării datelor cu caracter personal în totalitate sau parțial prin mijloace automatizate și prelucrării, altfel decât prin mijloace automatizate, a

[2] Art. 3 alin.2 GDPR

datelor cu caracter personal care fac parte dintr-un sistem de arhivare sau sunt destinate să facă parte dintr-un sistem de arhivare.[3]

ii. BCR se aplică, de asemenea, acelor părți care prelucrează date cu caracter personal în calitatea lor de persoană împuternicită (intern) în numele unei alte entități Fresenius; cu toate acestea, numai în măsura în care acestea nu conduc la o contradicție cu un acord respectiv încheiat.

iii. Pentru a evita orice îndoială: Datele cu caracter personal pot[4] fi transferate numai pe baza BCR între părțile care au implementat în mod corespunzător BCR și au confirmat că au luat cu succes măsuri pentru a stabili conformitatea cu BCR.

iv. BCR se aplică prelucrării datelor cu caracter personal de către fiecare Parte enumerată în anexa 1 - Lista părților obligate prin BCR.

v. BCR cuprinde, în general, operațiunile de prelucrare prevăzute în anexa Global-ANNEX-LE-000067672 Natura datelor cu caracter personal transferate.

3.3 Relația dintre BCR și legile aplicabile privind protecția datelor

Fiecare Parte va adera și va respecta prezentele BCR, indiferent de faptul că legile aplicabile privind protecția datelor ar putea prevedea un nivel de protecție diferit sau mai scăzut. Cu toate acestea, în cazul în care și în măsura în care legile aplicabile privind protecția datelor prevăd norme mai stricte privind prelucrarea, părțile vor respecta, în plus față de BCR, aceste norme mai stricte în temeiul legilor aplicabile privind protecția datelor.

3.4 Conflictele dintre legile aplicabile și BCR

Fiecare Parte care are obligații în temeiul GDPR, în cursul evaluării riscurilor în conformitate cu secțiunea 7 înainte de a transfera inițial date cu caracter personal către o altă Parte situată în afara UE/SEE, evaluează dacă aceasta din urmă este capabilă să respecte în practică garanțiile oferite de BCR.

În cazul în care o Parte are motive să creadă că legile aplicabile sau legile aplicabile privind protecția datelor o împiedică pe Partea respectivă sau o altă Parte să respecte BCR și în cazul în care acest eveniment poate avea un impact substanțial asupra

[3] Art. 3 alin.1 GDPR
[4] Artt. 46 alin. 2 lit. b, 47 GDPR

standardelor prevăzute de BCR, Partea respectivă va informa imediat responsabilul cu protecția datelor respectiv pentru a evalua impactul și a soluționa conflictul.

În cazul în care o cerință legală, cum ar fi un ordin obligatoriu de divulgare a datelor cu caracter personal aplicabil unei părți, are efecte negative substanțiale asupra garanțiilor pe care Grupul Fresenius le-a stabilit prin BCR, Partea respectivă va raporta acest aspect, precizând datele solicitate, identitatea organismului solicitant, precum și temeiul juridic, consilierului local pentru protecția datelor, care va informa responsabilul pentru protecția datelor respectiv, care, la rândul său, va informa sediul central din SEE sau entitatea din SEE cu responsabilități delegate. Autoritatea de supraveghere din Hesse, Germania, va fi informată de către responsabilul respectiv cu protecția datelor. Toate informările se vor face fără întârzieri nejustificate.

În cazul în care o astfel de notificare este interzisă de legile aplicabile, Partea va depune toate eforturile pentru a primi permisiunea de a informa responsabilul respectiv cu protecția datelor și, ulterior, autoritatea de supraveghere din Hesse, Germania, cât mai curând posibil, cu informații în cea mai mare măsură posibilă.

În cazul în care unei părți nu i se permite să furnizeze informații specifice cu privire la o cerere, Partea va furniza anual responsabilului cu protecția datelor respectiv informații generale cu privire la cererile primite, cu informații relevante în cea mai mare măsură posibilă (detaliind în special numărul de ordine de divulgare primite și urmate, organismele solicitante, categoriile de persoane fizice afectate și tipurile de date cu caracter personal) pentru a permite informarea autorității de supraveghere din Hesse, Germania.

În orice caz, transferurile de date cu caracter personal efectuate de o Parte către orice autoritate publică nu pot fi masive, disproporționate și nediscriminatorii, într-o manieră care ar depăși ceea ce este necesar într-o societate democratică.

4 Caracterul obligatoriu al BCR / Drepturile beneficiarilor terți

BCR sunt obligatorii pentru fiecare Parte și pentru angajații acesteia. Persoanele fizice sunt beneficiari terți și pot obține drepturi derivate din BCR. Fiecare Parte și fiecare dintre angajații săi este obligat să respecte principiile și obligațiile prevăzute în BCR.

Natura obligatorie a BCR cuprinde:

i. *Caracterul obligatoriu pentru* părți - Grupul Fresenius a introdus BCR în cadrul entităților și a instituit un mecanism care face ca BCR să devină obligatoriu pentru orice Parte enumerată în anexa 1 - Lista părților obligate de BCR. Fiecare entitate Fresenius s-a obligat prin contract să adere la principiile BCR prin semnarea acordului-cadru cu toate părțile participante. În cazul în care acest lucru este necesar pentru ca BCR să fie eficient, fiecare Parte este obligată să pună în aplicare toate cerințele suplimentare pentru a face BCR obligatoriu, conform cerințelor contractuale.

ii. *Caracter obligatoriu pentru* angajați - Angajații sunt obligați să respecte principiile stabilite în BCR ca urmare a obligațiilor generale care decurg din contractul de muncă de a respecta politicile corporative. Punerea în aplicare a BCR și potențialele sancțiuni pentru orice încălcare a BCR față de angajați sunt asigurate de structura internă de conformitate. În cazul în care acest lucru este necesar pentru ca BCR să aibă un astfel de efect obligatoriu față de angajații respectivi, fiecare Parte este obligată să pună în aplicare toate cerințele suplimentare pentru ca BCR să fie obligatoriu, așa cum se prevede în contract.

iii. *Caracterul obligatoriu față de persoanele* fizice (drepturi de beneficiar terț) - Toate părțile se angajează să acorde persoanelor fizice drepturi de beneficiar terț în temeiul BCR în ceea ce privește prelucrarea datelor lor cu caracter personal. În consecință, fiecare Parte recunoaște și acceptă în mod expres că Persoanele fizice vor avea dreptul de a aplica dispozițiile clauzelor 3.3, 3.4, 6.1 - 6.8, 9.1 - 9.7 și 10.1 - 10.4 din prezentul BCR în ceea ce privește prelucrarea datelor lor cu caracter personal și așa cum se stipulează în continuare în secțiunea **Error! Reference source not found.**.

5 Organizația pentru protecția datelor

Grupul Fresenius a înființat o organizație internă pentru protecția datelor și a atribuit roluri și responsabilități în cadrul părților pentru a realiza un cadru de guvernanță și de sprijin adecvat pentru a asigura prelucrarea legală a datelor cu caracter personal. Grupul Fresenius va desemna un DPO acolo unde este necesar și va menține organizația de protecție a datelor pentru a continua guvernanța și sprijinul adecvat pentru fiecare Parte, după cum urmează:

- Responsabilul cu protecția datelor (DPO) monitorizează, evaluează și auditează conformitatea cu BCR și cu legile aplicabile privind protecția datelor, precum și cu politicile și procedurile de protecție a datelor. DPO informează și consiliază Partea și angajații respectivi cu privire la obligațiile care le revin în temeiul BCR și al legilor aplicabile în materie de protecție a datelor, oferă consultanță la cerere și în cazul evaluărilor impactului asupra protecției datelor, investighează încălcările și monitorizează remedierea acestora, propune îmbunătățiri ale sistemului de gestionare a protecției datelor și cooperează cu autoritățile de supraveghere și acționează ca punct de contact principal pentru acestea. DPO este responsabil pentru domeniul de aplicare descris în numirea sa și raportează direct conducerii superioare. În acest rol, DPO acționează în mod independent.
- Consilierul pentru protecția datelor (DPA) oferă sprijin și consultanță în cadrul organizației pentru protecție a datelor, construiește, implementează și menține sistemul de gestionare a protecției datelor pentru a permite prelucrarea legală a datelor cu caracter personal și respectarea BCR și a legilor aplicabile privind protecția datelor. În plus, DPA analizează conceptele de prelucrare a datelor cu caracter personal relevante pentru grupul Fresenius, efectuează evaluări ale riscurilor legate de protecția datelor, oferă consultanță cu privire la acordurile de prelucrare a datelor, sprijină responsabilul procesului de afaceri în ceea ce privește înregistrarea activităților de prelucrare a datelor, oferă consultanță cu privire la evaluările impactului asupra protecției datelor, pregătește răspunsuri la solicitările de informații ale persoanelor vizate și permite LDPA să ofere consultanță competentă.
  Atunci când este necesar, DPA sprijină DPO, la cerere, în cadrul funcției de monitorizare și al contactului cu autoritățile de supraveghere, de exemplu, din cauza unor probleme lingvistice.
- Consilierul local pentru protecția datelor (LDPA) oferă consultanță și sprijin responsabilului de activitate sau de proces pentru toate activitățile entității Fresenius locale respective sau pentru un anumit subiect, oferă sprijin în probleme lingvistice, efectuează evaluări ale riscurilor relevante pentru entitatea locală sau pentru un anumit subiect și revizuiește conceptele și acordurile de prelucrare a datelor relevante, sprijină responsabilul procesului de activitate în ceea ce privește menținerea înregistrării activităților de

prelucrare a datelor și documentarea măsurilor relevante de protecție a datelor. Atunci când este necesar, LDPA sprijină DPA și DPO. LDPA este atribuit doar în cadrul FK AG.

Responsabilul cu protecția datelor al FSE și al tuturor filialelor sale în conformitate cu sec. 15 și următoarele din Legea germană privind societățile pe acțiuni, cu excepția celor care aparțin segmentelor de activitate Fresenius Kabi, Fresenius Medical Care, Fresenius Helios și Fresenius Vamed, poate fi contactat după cum urmează:

Responsabil cu protecția datelor Fresenius SE & KGaA

Fresenius SE & Co. KGaA

Else-Kröner-Str. 1

61352 Bad Homburg v.d.H.

Germania

dataprotectionofficer@fresenius.com

Responsabilul cu protecția datelor al FK AG și al tuturor filialelor sale situate în UE/SEE în conformitate cu sec. 15 și următoarele din Legea germană privind societățile pe acțiuni, care aparțin segmentului de afaceri Fresenius Kabi, pot fi contactați după cum urmează:

Responsabil cu protecția datelor Fresenius Kabi

Fresenius Kabi AG

Else-Kröner-Str. 1

61352 Bad Homburg v.d.H.

Germania

dataprotectionofficer@fresenius-kabi.com

6 Principiile de protecție a datelor în cadrul BCR

Prelucrate, trebuie să fie respectate drepturile și libertățile fundamentale ale persoanelor fizice, în special dreptul acestora la protecția datelor cu caracter personal.

În cadrul domeniului de aplicare al prezentelor BCR, fiecare Parte va respecta următoarele principii atunci când prelucrează date cu caracter personal:

6.1 Legalitate

Fiecare Parte va prelucra datele cu caracter personal numai în mod legal. Temeiul juridic specific al activității respective de prelucrare a datelor va fi documentat în mod corespunzător.

Partea va Prelucra datele cu caracter personal numai pe baza următoarelor temeiuri legale[5]:

i. Pe baza consimțământului persoanei fizice, ceea ce înseamnă indicația liberă, specifică, informată și neechivocă prin care persoana fizică își exprimă acordul cu privire la prelucrarea datelor sale cu caracter personal în unul sau mai multe scopuri specificate;

ii. pentru executarea unui contract la care persoana fizică este parte sau pentru a lua măsuri la cererea persoanei fizice înainte de încheierea unui contract;

iii. pentru respectarea obligațiilor legale sau statutare ale Grupului Fresenius, de exemplu cele legate de impozitare, dispozitive medicale sau obligații de farmacovigilență;

iv. în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea unei autorități oficiale cu care este investită Partea respectivă;

v. pentru a proteja interesele vitale ale unei persoane fizice sau ale unei alte persoane fizice;

vi. în scopul unui interes legitim al părții respective sau al unei alte părți terțe, cu excepția cazului în care persoana fizică are un interes superior ca datele sale cu caracter personal să nu fie prelucrate (a se vedea 9.6.)

Prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsurile de securitate aferente pe baza unuia dintre temeiurile juridice menționate mai sus va fi efectuată numai sub controlul unei autorități de supraveghere sau atunci când prelucrarea este autorizată de Legea aplicabilă privind protecția datelor

[5] Art. 6 GDPR

care prevede garanții adecvate pentru drepturile și libertățile persoanelor fizice. Secțiunea 3.4 rămâne neafectată.

Legile aplicabile privind protecția datelor și legile aplicabile pot stipula dispoziții suplimentare sau divergente cu privire la prelucrarea datelor cu caracter personal ale angajaților. În acest caz, părțile vor prelucra datele cu caracter personal ale angajaților în conformitate cu aceste dispoziții. Secțiuni 3.3 și 3.4 rămân neafectate.

Partea va prelucra categoriile speciale de date cu caracter personal numai pe baza următoarelor temeiuri legale[6]:

i. pe baza consimțământului persoanelor fizice la prelucrarea acestor date cu caracter personal în unul sau mai multe scopuri specificate;

ii. în cazul în care acest lucru este necesar în scopuri de angajare sau de securitate socială;

iii. pentru a proteja interesele vitale ale unei persoane fizice sau ale unei alte persoane fizice, în cazul în care persoana fizică este incapabilă din punct de vedere fizic sau juridic să își dea consimțământul;

iv. dacă datele cu caracter personal au fost făcute publice în mod evident de către persoana în cauză;

v. dacă este necesar pentru constatarea, exercitarea sau apărarea unor pretenții legale;

vi. în cazul în care este necesar din motive de interes public substanțial, în măsura în care este proporțional cu scopul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri adecvate și specifice de protecție a drepturilor fundamentale și a intereselor persoanelor fizice;

vii. în cazul în care este necesar în scopuri de medicină preventivă sau de medicină a muncii, pentru evaluarea capacității de muncă a angajaților, pentru diagnosticarea medicală, pentru furnizarea de asistență sau tratament medical sau social sau pentru gestionarea sistemelor și serviciilor de asistență medicală sau socială;

[6] Art. 9 GDPR

viii. în cazul în care este necesar din motive de interes public în domeniul sănătății publice (transfrontaliere), cum ar fi asigurarea unor standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, garantarea drepturilor persoanelor fizice, în special a secretului profesional; sau

ix. în cazul în care este necesar în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică sau în scopuri statistice, cu condiția ca prelucrarea să respecte esența dreptului la protecția datelor și să ia măsuri adecvate și specifice pentru a proteja drepturile fundamentale și interesele și principiile persoanelor fizice prevăzute în prezentele BCR.

6.2 Transparență și corectitudine

Fiecare Parte va prelucra datele cu caracter personal în mod echitabil și transparent[7], ceea ce înseamnă că, în general, persoanele fizice vor fi informate în mod adecvat în prealabil[8] cu privire la prelucrarea datelor lor cu caracter personal și vor primi informații cu privire la drepturile persoanelor vizate, în conformitate cu secțiunea 9 de mai jos, precum și orice alte drepturi care le sunt conferite de Legile aplicabile privind protecția datelor în legătură cu datele lor personale (a se vedea secțiunea 9 de mai jos).

În cazul în care datele cu caracter personal nu sunt obținute de la persoana în cauză, informațiile vor fi furnizate:

i. într-o perioadă rezonabilă de timp după obținerea datelor cu caracter personal, dar nu mai târziu de o lună; ținând seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;

ii. în cazul în care datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana fizică, cel târziu în momentul primei comunicări cu persoana respectivă; sau

iii. în cazul în care se are în vedere o divulgare către un alt destinatar, cel târziu în momentul în care datele cu caracter personal sunt divulgate pentru prima dată.

[7] Art. 5, alineatul (1), litera (a) din GDPR
[8] Art. 13 & 14 GDPR

Orice informație furnizată persoanelor fizice sau orice comunicare cu o persoană fizică referitoare la prelucrarea datelor sale personale va fi concisă, transparentă, cuprinzătoare și într-o formă ușor accesibilă, folosind un limbaj clar și simplu.

6.2.1 Informații obligatorii

Aceste informații transparente pentru persoana fizică vor include următoarele:

i. identitatea și datele de contact ale părții și, dacă este cazul, ale reprezentantului entității Fresenius;

ii. datele de contact ale responsabilului cu protecția datelor, în cazul în care este desemnat;

iii. scopurile prelucrării datelor cu caracter personal, precum și temeiul juridic al prelucrării;

iv. în cazul în care Prelucrarea se bazează pe un interes legitim, interesele legitime urmărite de Parte sau de o terță parte;

v. destinatarii sau categoriile de destinatari ai datelor cu caracter personal (dacă este cazul);

vi. orice transfer de date cu caracter personal către o țară din afara UE/SEE sau către o organizație internațională, temeiul juridic pe care se bazează un astfel de transfer, inclusiv o trimitere la garanțiile corespunzătoare sau adecvate și la mijloacele prin care se poate obține o copie a acestora sau unde au fost puse la dispoziție.

6.2.2 Informații suplimentare care trebuie furnizate

Pentru a asigura o prelucrare echitabilă și transparentă, se vor furniza următoarele informații suplimentare:

i. perioada pentru care vor fi stocate datele cu caracter personal;

ii. drepturile persoanelor fizice enumerate în secțiunea 9 din prezentele Reguli Corporative Obligatorii;

iii. în cazul în care prelucrarea se bazează pe consimțământ, existența dreptului de retragere a consimțământului în orice moment, care va avea efect numai pentru prelucrarea viitoare a datelor cu caracter personal;

iv. dreptul de a depune o plângere la o autoritate de supraveghere;

v. orice existență a unui proces decizional automatizat, inclusiv crearea de profiluri, și informații semnificative privind logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de prelucrări.

vi. dacă furnizarea de date cu caracter personal este o cerință legală sau contractuală sau o cerință necesară pentru încheierea unui contract, precum și dacă persoana fizică este obligată să furnizeze datele cu caracter personal și care sunt posibilele consecințe în cazul în care datele cu caracter personal nu sunt furnizate;

6.2.3 Informații suplimentare care trebuie furnizate în cazul în care datele sunt colectate de la o terță parte

În cazul în care datele cu caracter personal sunt colectate de la o terță parte diferită de persoana fizică, Partea va furniza informații suplimentare cu privire la:

i. categoriile de date cu caracter personal care sunt prelucrate; și

ii. sursa datelor cu caracter personal.

6.3 Limitarea Scopului

Oricare dintre părți va prelucra datele cu caracter personal numai în scopurile specificate pentru care au fost colectate datele cu caracter personal. Oricare dintre părți nu va prelucra datele cu caracter personal în scopuri incompatibile cu scopurile inițiale, cu excepția cazului în care schimbarea scopului este permisă de legislația UE privind protecția datelor. Se iau măsuri suplimentare pentru a proteja drepturile și libertățile persoanei fizice, cum ar fi consimțământul persoanelor fizice respectiv afectate, oferirea unei oportunități de retragere, limitarea accesului la datele cu caracter personal, controale suplimentare de confidențialitate și securitate, furnizarea de informații persoanei fizice.

În general, scopurile permise pentru prelucrarea ulterioară, care sunt considerate compatibile cu scopul inițial, sunt:

i. arhivare;

ii. auditul intern și investigațiile.

Pentru a stabili dacă Prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, trebuie să se ia în considerare, printre altele, următoarele:

i. orice legătură între scopurile pentru care au fost colectate datele cu caracter personal și scopurile prelucrării ulterioare preconizate;

ii. contextul în care au fost colectate datele cu caracter personal, în special în ceea ce privește relația dintre persoanele fizice și Partea respectivă;

iii. natura datelor cu caracter personal, în special dacă sunt prelucrate categorii speciale de date cu caracter personal, în conformitate cu articolul 9 din GDPR, sau dacă sunt prelucrate date cu caracter personal legate de condamnări penale și infracțiuni, în conformitate cu articolul 10 din GDPR;

iv. posibilele consecințe ale prelucrării ulterioare preconizate pentru persoanele fizice;

v. existența unor măsuri de protecție adecvate, care pot include criptarea sau pseudonimizarea.

Consilierul (local) pe probleme de confidențialitate a datelor va fi în măsură să ofere îndrumări cu privire la dacă și când este permisă o astfel de modificare.

În cazul unei modificări permise a scopului, persoanele fizice trebuie să fie informate cu privire la orice astfel de modificări în conformitate cu secțiunea 6.2 înainte ca datele cu caracter personal să fie prelucrate în acel alt scop.

6.4 Minimizarea datelor

Oricare dintre Părți va colecta și prelucra datele cu caracter personal numai în măsura în care este necesar pentru scopul comercial și despre care persoana vizată este informată (scopul inițial) sau cele care sunt compatibile cu aceste scopuri inițiale în conformitate cu secțiunea 6.3. Oricare dintre Părți nu va colecta sau prelucra date cu caracter personal care sunt fie excesive, fie nerelevante pentru scopul pentru care sunt necesare datele cu caracter personal.

6.5 Acuratețe

Datele cu caracter personal vor fi păstrate de către Grupul Fresenius corecte și actualizate. Fiecare Parte va pune în aplicare proceduri pentru a se asigura că datele inexacte sunt șterse, corectate sau actualizate fără întârziere pe parcursul ciclului de viață respectiv.

6.6 Limitarea stocării

Fiecare Parte va păstra datele cu caracter personal nu mai mult timp decât este necesar pentru scopul pentru care sunt prelucrate datele cu caracter personal, cu excepția cazului în care datele cu caracter personal trebuie păstrate în conformitate cu legea. În cazul în care Datele cu caracter personal trebuie păstrate din alte motive decât scopul inițial (de exemplu, deoarece legile aplicabile impun păstrarea datelor pentru o perioadă mai lungă de timp), accesul la acestea va fi restricționat. În momentul în care nu mai există niciun interes legal sau legitim pentru a mai fi păstrate datele cu caracter personal de către Parte, datele cu caracter personal vor fi anonimizate sau șterse în siguranță.

6.7 Securitate, integritate și confidențialitate

6.7.1 Măsuri tehnice și organizaționale de securitate

Fiecare Parte va lua măsurile tehnice și organizatorice adecvate pentru a proteja datele cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, divulgării neautorizate sau accesului neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod. Fiecare Parte va lua în considerare, în special, stadiul actual al tehnologiei, costurile de punere în aplicare și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile de probabilitate și gravitate diferite pentru drepturile și libertățile persoanelor fizice atunci când pune în aplicare astfel de măsuri tehnice și organizatorice, luând în considerare confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal stocate, prin instalarea și întreținerea sistemelor și serviciilor de prelucrare a datelor configurate pentru a rămâne rezistente la atacurile de securitate cibernetică și la amenințările la adresa securității IT, inclusiv, inter alia, după caz:

i. pseudonimizarea și criptarea datelor cu caracter personal;

ii. capacitatea de a asigura în permanență confidențialitatea, integritatea, disponibilitatea și reziliența sistemelor și serviciilor de prelucrare;

iii. capacitatea de a restabili disponibilitatea și accesul la datele cu caracter personal în timp util în cazul unui incident fizic sau tehnic;

iv. un proces de testare, evaluare și apreciere periodică a eficienței măsurilor tehnice și organizatorice pentru asigurarea securității prelucrării.

6.7.2 Notificarea încălcărilor datelor cu caracter personal

Fiecare Parte se angajează să notifice orice încălcare a securității care duce la distrugerea accidentală sau ilegală sau la pierderea accidentală, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal către Organizația pentru protecția datelor a FSE și FK AG, care, la rândul său, informează sediul central al SEE. În plus, există următoarele obligații de notificare în cazul unei astfel de încălcări a datelor cu caracter personal:

i. orice Parte care face obiectul GDPR și care acționează în calitate de operator notifică autorității de supraveghere orice încălcare a datelor cu caracter personal care poate avea ca rezultat un risc pentru persoanele afectate, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult șaptezeci și două (72) de ore de la data la care a luat cunoștință de încălcarea datelor cu caracter personal;

ii. orice altă Parte, care acționează în calitate de operator notifică autorității de supraveghere vizate orice încălcare a datelor cu caracter personal care ar putea avea ca rezultat un risc pentru persoanele afectate, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult șaptezeci și două (72) de ore de la data la care a luat cunoștință de încălcarea datelor cu caracter personal;

iii. orice Parte care acționează în calitate de persoană împuternicită pentru o altă Parte notifică orice încălcare a securității datelor cu caracter personal părții respective care acționează în calitate de operator și LDPA relevant.

iv. în cazul în care este probabil ca o încălcare a datelor cu caracter personal să genereze un risc ridicat pentru drepturile și libertățile persoanelor afectate, Partea respectivă care acționează în calitate de operator comunică încălcarea datelor cu caracter personal persoanelor afectate fără întârzieri nejustificate.

Fiecare Parte va documenta o astfel de încălcare a securității (cuprinzând faptele legate de încălcare, efectele acesteia și măsurile de remediere luate) și, după consultarea cu Organizația pentru protecția datelor a FSE și FK AG, va pune această documentație la dispoziția autorităților de supraveghere.

6.8 Responsabilitate

Fiecare Parte va adera la principiile stabilite mai sus și va fi în măsură să demonstreze conformitatea cu BCR și, în acest sens, va crea și va păstra documentația corespunzătoare, inclusiv:

i. Păstrarea înregistrărilor privind activitățile de prelucrare, respectiv:

- numele și datele de contact ale operatorului și, dacă este cazul, ale co-operatorului, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- scopurile prelucrării;
- o descriere a categoriilor de persoane fizice și a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- dacă este cazul, transferurile de date cu caracter personal în afara UE sau a unei organizații internaționale, inclusiv garanții adecvate, astfel cum sunt definite în secțiunea 6.8.2;
- dacă este posibil, termenele prevăzute pentru eliminarea diferitelor categorii de date cu caracter personal;
- dacă este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la secțiunea 6.7.

Această evidență ar trebui să fie păstrată în scris, inclusiv în format electronic, și ar trebui să fie pusă la dispoziția autorităților de supraveghere, la cerere.

ii. Implementarea unor măsuri tehnice și organizatorice adecvate care sunt concepute pentru a pune în aplicare principiile de protecție a datelor și pentru a facilita respectarea în practică a cerințelor stabilite de BCR (protecția datelor prin concepție și implicit).

iii. Efectuarea de evaluări ale impactului asupra protecției datelor, astfel cum se prevede în secțiunea 8.

6.8.1 Angajarea persoanelor împuternicite

Fiecare Parte va angaja numai persoane împuternicite care oferă garanții suficiente pentru a implementa măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea

să respecte cerințele BCR și legile aplicabile privind protecția datelor (în special GDPR) și să asigure protecția drepturilor persoanelor fizice.

Orice prelucrare efectuată de către o persoană împuternicită va fi reglementată de un contract sau de un alt act juridic care este obligatoriu pentru persoana împuternicită în ceea ce privește operatorul și care stipulează, printre altele:

i. că persoana împuternicită trebuie să prelucreze datele cu caracter personal numai în conformitate cu instrucțiunile primite de la operatorul de date;

ii. că persoana împuternicită de către operator trebuie să mențină măsuri tehnice și organizatorice adecvate pentru a proteja datele cu caracter personal;

iii. că persoana împuternicită să prelucreze datele cu caracter personal se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație legală corespunzătoare de confidențialitate;

iv. faptul că persoana împuternicită de către operator trebuie să șteargă sau să returneze toate datele cu caracter personal după încheierea furnizării serviciilor legate de prelucrare și să șteargă copiile existente;

v. faptul că persoana împuternicită de către operator poate angaja numai subcontractanți care oferă garanții suficiente pentru a pune în aplicare măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele BCR și legile aplicabile privind protecția datelor, pe baza unor mijloace contractuale scrise care să impună subcontractanților același nivel de obligații în materie de protecție a datelor ca și cele stabilite între Parte și persoana împuternicită.

vi. că persoana împuternicită de către operator va sprijini Partea respectivă în îndeplinirea obligațiilor sale de a răspunde la cererile persoanelor fizice;

vii. că persoana împuternicită de către operator pune la dispoziție toate informațiile necesare pentru a demonstra respectarea prezentei secțiuni și permite și contribuie la audituri, inclusiv la inspecții efectuate de Partea respectivă sau de un alt auditor convenit;

viii. că persoana împuternicită de către operator va asista Partea respectivă în asigurarea respectării obligațiilor menționate la secțiunile 6.7 și 7.

6.8.2 Transferurile (ulterioare) de date cu caracter personal

Părțile vor pune în aplicare măsuri pentru a proteja în mod adecvat transferurile de date cu caracter personal către terți destinatari situați în afara SEE, în conformitate cu prezentele BCR.

Datele cu caracter personal pot fi transferate către un destinatar terț din afara SEE numai în cazul în care este îndeplinită cel puțin una dintre următoarele condiții:

i. destinatarul terț este situat într-o țară care a fost recunoscută de către Comisia Europeană ca oferind un nivel adecvat de protecție a datelor cu caracter personal (așa-numitele țări din "lista albă") și - în măsura în care este aplicabil - destinatarul terț îndeplinește toate cerințele suplimentare în conformitate cu cerințele de adecvare aplicabile; sau

ii. în cazul în care destinatarul terț a oferit garanții adecvate și cu condiția ca persoanele fizice să aibă la dispoziție drepturi individuale executorii și căi de atac eficiente; de exemplu, în temeiul unor clauze contractuale standard adoptate de Comisia Europeană; sau

Prin derogare de la alternativele menționate mai sus, datele cu caracter personal pot fi transferate și în cazul în care se aplică una dintre următoarele excepții:

i. persoana fizică și-a dat consimțământul explicit pentru transferul datelor sale cu caracter personal după ce a fost informată cu privire la riscurile posibile ale unor astfel de transferuri; sau

ii. Transferul de date cu caracter personal este necesar (i) pentru a executa un contract cu persoana fizică sau pentru a pune în aplicare măsuri precontractuale luate la cererea persoanei fizice; sau (ii) pentru a executa sau a încheia un contract încheiat în interesul persoanei fizice între operator și o altă persoană fizică sau juridică; sau

iii. Transferul datelor cu caracter personal este necesar (i) pentru a proteja interesele vitale ale persoanei fizice sau ale altor persoane (de exemplu, în cazul unei situații de viață sau de moarte), în cazul în care persoana fizică sau juridică este incapabilă să își dea consimțământul, sau (ii) pentru a permite Fresenius să stabilească, să exercite sau să apere un drept legal sau (iii) din motive importante de interes public; sau

iv. transferul se face dintr-un registru care, în conformitate cu legislația UE sau a statelor membre, este destinat să furnizeze informații publicului și care este deschis consultării fie de către publicul larg, fie de către orice persoană care poate demonstra un interes legitim, dar numai în măsura în care sunt îndeplinite condițiile prevăzute de legislația UE sau a statelor membre pentru consultare în cazul respectiv.

În cazul în care nu este îndeplinită niciuna dintre condițiile de mai sus, iar transferul nu este repetitiv, nu privește decât un număr limitat de persoane vizate, este necesar în scopul unor interese legitime imperioase, iar acestea nu sunt înlăturate de interesele sau drepturile și libertățile persoanei vizate, Partea expeditoare va evalua circumstanțele în care are loc transferul de date și va oferi garanții adecvate cu privire la protecția datelor cu caracter personal și va informa autoritatea de supraveghere în cauză cu privire la transfer.

Pentru evitarea oricărui dubiu, condițiile menționate mai sus se aplică, de asemenea, pentru orice transfer ulterior de date cu caracter personal de către o Parte situată în afara UE/SEE către un destinatar terț situat în afara UE/SEE, în cazul în care datele cu caracter personal afectate au fost inițial transferate de către o Parte situată în UE/SEE.

7 Evaluarea riscului de protecție a datelor

Fiecare Parte va efectua o evaluare a riscurilor în materie de protecție a datelor pentru orice activitate de prelucrare a datelor referitoare la datele cu caracter personal. Evaluarea riscurilor privind protecția datelor este un proces formal de evaluare a impactului oricărei activități de prelucrare a datelor asupra drepturilor și libertăților persoanelor în cauză (riscuri privind viața privată). Evaluarea riscurilor se realizează ca o analiză detaliată a unei Activități de prelucrare a datelor și are rolul de a identifica:

i. Riscurile pentru viața privată a persoanelor fizice care rezultă din activitatea de prelucrare a datelor;

ii. cerințele aplicabile care decurg din BCR și din legile aplicabile privind protecția datelor; și

iii. măsuri adecvate pentru a îndeplini aceste cerințe și pentru a atenua riscurile identificate în materie de confidențialitate.

În special, înainte de a transfera date cu caracter personal către o altă Parte situată în afara UE/SEE, fiecare Parte evaluează dacă aceasta din urmă este capabilă să respecte garanțiile oferite de BCR în practică, luând în considerare contextul și scopul transferului de date, posibila interferență creată de legile aplicabile sau de legile aplicabile privind protecția datelor din țara terță în cauză cu drepturile fundamentale ale persoanelor fizice. În caz contrar, părțile evaluează dacă pot oferi măsuri/controale tehnice, organizatorice sau contractuale suplimentare pentru a asigura un nivel de protecție esențial echivalent cu cel oferit în UE. În cazul în care astfel de măsuri nu ar putea fi furnizate, Partea nu efectuează transferul. În cazul în care Partea transferă deja date cu caracter personal, transferul este suspendat sau încetează. Datele cu caracter personal deja transferate sau copii ale acestora trebuie returnate Părții expeditoare sau distruse în întregime de către destinatar. Orice evaluare efectuată în temeiul prezentului alineat este revizuită în mod regulat.

Evaluarea riscurilor constă în următoarele etape principale:

i. Pre-evaluare

   Evaluarea prealabilă determină riscurile inerente de confidențialitate care rezultă dintr-o activitate de prelucrare a datelor și le califică drept ridicate, medii sau scăzute. Rezultatele preevaluării determină etapele ulterioare ale evaluării riscurilor.

ii. Evaluarea controalelor

   În cadrul evaluării controalelor, măsurile/controalele puse în aplicare sau care trebuie puse în aplicare sunt determinate și documentate în funcție de trei niveluri de maturitate pentru a atenua riscurile inerente definite de evaluarea prealabilă și, dacă este cazul, din cauza unui risc ridicat, definit de DPIA, precum și pentru a îndeplini cerințele din BCR și din legile aplicabile privind protecția datelor.

iii. Evaluarea caracterului adecvat al controalelor privind protecția datelor

   Caracterul adecvat al măsurilor tehnice, organizatorice sau contractuale implementate sau care urmează să fie implementate este evaluat pentru a determina riscurile reziduale în materie de confidențialitate.

iv. Raportarea riscurilor

Lacunele de control identificate și potențialele riscuri reziduale sunt raportate și documentate. Lacunele și riscurile trebuie remediate, iar măsurile tehnice și organizatorice de atenuare trebuie puse în aplicare înainte de începerea activității de prelucrare a datelor.

În cazul în care evaluarea prealabilă are ca rezultat un risc ridicat de confidențialitate, o evaluare a impactului prelucrării datelor (DPIA) trebuie să fie efectuată suplimentar de către consilierul (local) în materie de confidențialitate a datelor și aprobată de responsabilul cu protecția datelor respectiv.

8 Evaluări ale impactului asupra protecției datelor[9]

Fiecare Parte va efectua o evaluare a impactului asupra protecției datelor (DPIA) în cazul în care prelucrarea datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice înainte de prelucrare. Se va solicita sfatul responsabilului cu protecția datelor respectiv.

Pentru a evalua dacă este necesară o DPIA, Partea va lua în considerare tipul de prelucrare, utilizarea de noi tehnologii, precum și natura, domeniul de aplicare, contextul și scopurile prelucrării. În cazul în care o DPIA identifică un risc ridicat al unei activități specifice de prelucrare a datelor, Partea responsabilă va pune în aplicare măsuri adecvate pentru a atenua aceste riscuri înainte de începerea prelucrării. În cazul în care o DPIA indică faptul că Prelucrarea ar duce în continuare la un risc ridicat, luând în considerare măsurile luate pentru a atenua riscul, ar trebui consultată Autoritatea de supraveghere în cauză, înainte de Prelucrare.

DPIA va fi necesară în special în cazul:

i. Prelucrarea sistematică, extinsă și automatizată a datelor cu caracter personal, inclusiv crearea de profiluri și în cazul în care deciziile care au efecte semnificative asupra persoanelor fizice, sau

ii. prelucrarea pe scară largă a unor categorii speciale de date cu caracter personal sau referitoare la condamnări penale și infracțiuni.

9 Drepturile persoanelor fizice[10]

Fiecare Parte va permite persoanelor fizice să își exercite următoarele drepturi.

[9] Art.35 GDPR
[10] Capitolul III GDPR

Fiecare Parte va informa destinatarii dacă și în măsura în care o persoană fizică solicită rectificarea, ștergerea sau restricționarea datelor cu caracter personal, cu excepția cazului în care acest lucru se dovedește imposibil sau implică un efort disproporționat. Părțile vor informa persoana fizică despre acești destinatari la cererea persoanei fizice. Orice solicitare pe care o Parte o poate primi de la o persoană fizică în legătură cu drepturile sale menționate mai sus va fi tratată în conformitate cu procedura de tratare a reclamațiilor BCR, astfel cum este descrisă în secțiunea 10.2.

9.1 Dreptul de acces la datele cu caracter personal

Persoana fizică are dreptul de a solicita accesul/să primească informații despre datele sale personale, scopul prelucrării, categoriile de date personale vizate, destinatarii datelor personale, perioadele de stocare a datelor personale sau criteriile acestora, existența dreptului de a solicita rectificarea sau ștergerea datelor personale sau restricționarea prelucrării datelor personale care o privesc sau de a se opune unei astfel de prelucrări, dreptul de a depune o plângere la o Autoritate de supraveghere și sursa Datelor cu caracter personal, în cazul în care Datele cu caracter personal nu sunt colectate de la persoana vizată, orice existență a procesului decizional automatizat, inclusiv crearea de profiluri, orice transfer către o țară din afara UE/SEE și obținerea unei copii a datelor cu caracter personal care fac obiectul prelucrării (a se vedea, de asemenea, sec. 6.2).

9.2 Dreptul de rectificare a datelor cu caracter personal

Persoana fizică are dreptul de a solicita rectificarea datelor cu caracter personal inexacte sau incomplete care o privesc și care sunt prelucrate de o Parte și de a obține completarea datelor cu caracter personal incomplete.

9.3 Dreptul de a șterge datele cu caracter personal

Persoana fizică are dreptul de a solicita ștergerea datelor sale cu caracter personal prelucrate de o Parte, cu condiția și în măsura în care este îndeplinită una dintre următoarele condiții: (i) datele cu caracter personal nu mai sunt necesare în legătură cu scopurile pentru care au fost colectate sau prelucrate în alt mod, (ii) persoana fizică își retrage consimțământul pe care se bazează prelucrarea și în cazul în care nu există niciun alt temei juridic pentru prelucrare, (iii) persoana fizică se opune prelucrării în conformitate cu și nu există motive legitime imperative pentru prelucrare, sau persoana fizică se opune prelucrării în scopul marketingului direct, care include crearea de profiluri în măsura în care este legată de un astfel de marketing direct, (iv) datele cu caracter

personal au fost prelucrate în mod ilegal sau (v) datele cu caracter personal trebuie șterse pentru a respecta o obligație legală din legislația aplicabilă la care este supus operatorul. Trebuie respectate obligațiile existente privind păstrarea datelor și/sau interesele conflictuale; se aplică secțiunea 3.4.

9.4 Dreptul de a restricționa prelucrarea datelor cu caracter personal

Persoana fizică are dreptul de a solicita restricționarea prelucrării datelor sale cu caracter personal dacă (i) exactitatea datelor cu caracter personal este contestată de persoana fizică sau dacă persoana fizică s-a opus prelucrării (a se vedea mai jos secțiunea 9.6), pentru o perioadă care să permită părții respective să verifice exactitatea datelor cu caracter personal sau dacă motivele legitime ale Părții respective prevalează asupra celor ale persoanei fizice; sau (ii) Prelucrarea este ilegală, respectiv nu mai este necesară în scopurile urmărite, dar persoana fizică se opune ștergerii datelor cu caracter personal și solicită în schimb restricționarea utilizării acestora (de exemplu, dacă datele cu caracter personal sunt necesare pentru constatarea, exercitarea sau apărarea unor pretenții legale).

9.5 Dreptul de a primi date cu caracter personal într-un format portabil și de a transmite date cu caracter personal

În cazul în care datele cu caracter personal au fost furnizate de către persoana fizică și prelucrarea se bazează pe consimțământul persoanei fizice sau pe un contract încheiat cu persoana fizică, iar prelucrarea este efectuată prin mijloace automatizate, persoana fizică are dreptul de a primi datele sale personale într-un format utilizat în mod obișnuit și care poate fi citit automat și de a transmite aceste date (în măsura în care acest lucru este posibil din punct de vedere tehnic) fără obstacole pentru a permite persoanei fizice să utilizeze servicii similare de la un alt operator.

9.6 Dreptul de a obiecta la prelucrarea datelor cu caracter personal

Persoana fizică are dreptul de a se opune, din motive legate de situația sa particulară, prelucrării datelor sale cu caracter personal pe baza intereselor legitime sau a intereselor publice ale părților sau ale unei terțe părți (acest drept nu se aplică în cazul în care o dispoziție legală impune prelucrarea datelor cu caracter personal). Prelucrarea va înceta, cu excepția cazului în care Partea respectivă demonstrează că există motive legitime imperioase pentru prelucrare care prevalează asupra intereselor, drepturilor și libertăților persoanei fizice sau pentru constatarea, exercitarea sau apărarea unor pretenții legale.

În plus, persoana fizică are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc în scopuri de marketing direct, ceea ce include crearea de profiluri în măsura în care este legată de un astfel de marketing direct.

9.7 Dreptul de a nu face obiectul unui proces decizional automatizat

Persoanele fizice vor avea, de asemenea, dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automatizată, inclusiv crearea de profiluri, de către o Parte care ar putea conduce la efecte juridice sau la efecte semnificative similare asupra persoanei fizice, cu excepția cazului în care decizia respectivă:

i. este necesară pentru încheierea sau executarea unui contract între persoana fizică și Partea respectivă sau se bazează pe consimțământul explicit al persoanei fizice, cu condiția ca Partea respectivă să fi pus în aplicare măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei fizice, cel puțin dreptul de a obține o intervenție umană din partea Părții, de a-și exprima punctul de vedere și de a contesta decizia; sau

ii. este autorizată de legislația aplicabilă căreia îi este supusă Partea respectivă și care prevede, de asemenea, măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei fizice. Secțiunea 3.4 rămâne neafectată.

În acest scop, categoriile speciale de date cu caracter personal pot fi prelucrate numai dacă persoana fizică și-a dat consimțământul explicit sau dacă acest lucru este autorizat de legislația aplicabilă la care este supusă Partea respectivă, care trebuie să fie proporțională cu scopul urmărit, să respecte esența dreptului la protecția datelor și să prevadă măsuri adecvate și specifice pentru a proteja drepturile fundamentale și interesele persoanei fizice.

10 Conformitatea cu BCR

10.1 Accesul la BCR

Fiecare Parte va pune la dispoziție versiunea completă a BCR, în special acele secțiuni care conferă drepturi persoanelor fizice, în special secțiunea 3.3, 3.4, 4, 6.1-6.8, 9.1-9.7 și 10.1-10.4 din BCR, disponibile pentru persoanele fizice în exterior prin intermediul World Wide Web pe site-ul web dedicat al Grupului Fresenius. Întregul BCR va fi, de asemenea, disponibil la nivel intern prin intermediul intranetului (intraneturilor) Grupului Fresenius. De asemenea, Persoanele fizice pot accesa versiunile complete ale

BCR aprobate pentru publicare, contactând responsabilul cu protecția datelor respectiv sau orice membru al Organizației pentru protecția datelor.

10.2 Gestionarea reclamațiilor BCR

Fiecare persoană fizică are dreptul de a reclama încălcarea BCR, de a se adresa drepturilor sale individuale, astfel cum sunt prevăzute în sec. 9 din prezentele BCR, să aplice orice alt drept al BCR sau să adreseze orice altă solicitare Organizației pentru protecția datelor. Fresenius va pune în aplicare proceduri pentru a se asigura că o astfel de plângere este soluționată.

Reclamațiile înseamnă orice raport care reclamă o potențială încălcare a BCR, a legilor aplicabile privind protecția datelor, a ordinelor emise de autoritățile de supraveghere, a politicilor și orientărilor interne sau a autoangajamentelor voluntare referitoare la protecția datelor. În schimb, solicitările privind drepturile persoanelor vizate sunt toate solicitările unei persoane fizice care se referă la drepturile conform secțiunii 9 din prezentele BCR, în conformitate cu o procedură de tratare a cererilor persoanelor vizate.

Astfel de reclamații pot fi depuse prin mai multe canale de depunere a unei reclamații. O solicitare poate fi transmisă, de exemplu, prin telefon sau în scris, de exemplu, prin e-mail sau scrisoare, sau verbal, adresându-se responsabilului respectiv cu protecția datelor, consilierului (local) respectiv pentru protecția datelor sau liniei telefonice de asistență pentru conformitate. Canalele de comunicare respective sunt publicate pe site-ul web Fresenius World Wide Web și pe site-urile interne ale Grupului Fresenius, furnizând toate informațiile necesare (https://www.fresenius.com/compliance - rapoarte privind potențiale cazuri de conformitate sau https://www.fresenius-kabi.com/responsibilities/compliance).

Reclamațiile abuzive, în special dacă sunt în mod evident nefondate sau excesive, în special din cauza caracterului lor repetitiv, sau care constituie acțiuni jignitoare la adresa Fresenius sau a oricărui Angajat vor fi respinse. În acest caz, persoanei fizice i se va explica în scris motivul refuzului și i se va acorda dreptul la recurs.

În cazul în care plângerea este considerată justificată, Partea va lua măsuri adecvate pentru a o soluționa, depunând eforturi rezonabile pentru a rectifica și remedia situația care a dat naștere plângerii. Persoana fizică va fi informată în scris cu privire la faptul că vor fi sau au fost inițiate acțiuni adecvate pentru soluționarea plângerii. În orice caz, persoana fizică va fi informată cu privire la dreptul său de a depune o plângere în fața

unei instanțe sau o plângere la o autoritate de supraveghere în conformitate cu secțiunea 10.3 în cazul în care nu este mulțumită de modul în care a fost tratată plângerea sa.

În cazul cererilor persoanelor vizate, responsabilul cu protecția datelor, cu sprijinul consilierului (local) pentru protecția datelor, va încerca, în măsura posibilităților, să ofere un răspuns substanțial persoanei în cauză în termen de o (1) lună calendaristică de la primirea plângerii. În cazul în care nu este posibil să se furnizeze un răspuns substanțial în termen de o (1) lună calendaristică, de exemplu din cauza naturii plângerii, persoana fizică va fi notificată de către responsabilul cu protecția datelor respectiv, cu sprijinul consilierului (local) pentru protecția datelor respectiv, oferind o estimare a datei la care se poate aștepta să primească un răspuns substanțial. Un răspuns substanțial va fi furnizat în termen de cel mult trei (3) luni de la primirea unei plângeri.

În plus, datele de contact ale responsabilului cu protecția datelor și ale altor membri ai Organizației pentru protecția datelor sunt furnizate mai sus, în secțiunea 5 din prezentele Reguli corporative obligatorii.

Organizația pentru protecția datelor documentează acțiunile persoanelor în conformitate cu prezenta secțiune 10.2.

10.3 Răspundere și executare

Persoanele fizice care sunt afectate sau au suferit daune ca urmare a prelucrării datelor lor personale respective, care este ilegală sau contrară părților executorii ale BCR, astfel cum sunt prevăzute în secțiunea 4, fie de către o Parte, fie de către o persoană împuternicită de operator sau un subcontractant angajat, au dreptul de a introduce acțiuni sau proceduri pentru a pune în aplicare aceste părți ale BCR și, dacă este cazul, de a primi despăgubiri în fața unei instanțe competente, fie în țara în care este stabilită o Parte, fie în Bad Homburg, Germania, unde sunt stabilite FSE și FK AG, fie în țara în care persoana respectivă își are reședința obișnuită, și în fața autorităților de supraveghere, în special în țara de reședință obișnuită a persoanelor, locul de muncă sau locul presupusei încălcări, de exemplu, prin depunerea unei plângeri.

În cazul unor încălcări dovedite ale părților executorii ale BCR, astfel cum sunt prevăzute în secțiunea 4 de către părți stabilite în afara UE/SEE, FSE își asumă responsabilitatea și răspunderea pentru orice daune cauzate de o astfel de încălcare a BCR și se angajează

să ia orice măsură adecvată pentru a remedia actele părților stabilite în afara UE/SEE și să plătească despăgubiri pentru orice daune materiale sau morale cauzate unei persoane fizice ca urmare a unei astfel de încălcări. Înainte de a plăti orice despăgubire sau de a face orice declarație față de persoana vizată, FSE va notifica cu promptitudine Partea în cauză cu privire la cerere, pentru a permite părții în cauză să solicite un ordin de protecție sau o altă soluție adecvată. FSE are dreptul de a solicita singur un ordin de protecție sau o altă cale de atac adecvată împotriva presupusei încălcări.

În cazul în care persoanele fizice pot demonstra că au suferit prejudicii și prezintă în mod coerent fapte care arată că este probabil ca presupusele încălcări, respectiv că prejudiciul a avut loc din cauza presupusei încălcări a BCR, FSE trebuie să dovedească față de persoana fizică faptul că Partea care a cauzat prejudiciul nu a fost responsabilă pentru încălcarea BCR care a dat naștere acestor prejudicii sau că nu a avut loc o astfel de încălcare. Partea care a cauzat prejudiciul trebuie să ofere asistență rezonabilă FSE pentru a răspunde în timp util la astfel de plângeri sau cereri.

Orice Parte situată în afara UE/SEE va adera la orice solicitare sau ordin al unei autorități de supraveghere care ar fi obligatorie pentru Partea respectivă ca și cum aceasta ar fi stabilită în UE/SEE.

10.4 Cooperarea cu autoritățile de supraveghere

Fiecare Parte este obligată să (i) coopereze cu autoritățile de supraveghere în cauză, (ii) să se conformeze sfaturilor privind orice problemă de interpretare a prezentelor BCR (iii) să accepte să fie auditată de către autoritățile de supraveghere în cauză. La cererea unei Autorități de supraveghere vizate, responsabilul cu protecția datelor respectiv va furniza o copie a raportului de audit aplicabil creat în cadrul programului de audit descris la sec. 10.6.

10.5 Instruire

Fiecare Parte își va înscrie și își va obliga angajații implicați în prelucrarea datelor cu caracter personal sau în dezvoltarea de instrumente utilizate pentru prelucrarea datelor cu caracter personal să participe la o instruire privind BCR și legile aplicabile privind protecția datelor și să repete periodic această instruire. Instruirea generală este oferită cel puțin bianual tuturor Angajaților relevanți. În plus, se asigură o instruire specifică rolului (cum ar fi sesiuni de informare și coaching dedicate sau ateliere de lucru), ținând

cont de nevoile specifice ale anumitor roluri/persoane, de exemplu, membrii Organizației pentru protecția datelor din FSE și FK AG.

Instruirea este obligatorie pentru angajații în cauză. După ce este invitat prin e-mail să participe la o instruire, angajatului i se acordă un timp prestabilit pentru finalizarea acesteia. Angajații care nu au participat la un curs de formare la un anumit moment vor primi o atenționare. În plus, supervizorul Angajatului primește o notificare de reamintire care va fi trimisă din nou lunar până la finalizarea cursului. Un Angajat care nu participă la instruirea respectivă după două memento-uri poate fi supus unor consecințe (disciplinare) în conformitate cu legislația aplicabilă în materie de muncă.

În cele mai multe cazuri, instruirea va fi oferită prin intermediul unei platforme de e-Learning. În general, cursurile de formare se încheie cu o validare pentru a ajuta la consolidarea înțelegerii conținutului, de exemplu, prin utilizarea unui test cu alegere multiplă sau a unui test cu text liber.

10.6 Auditul

Părțile pun în aplicare și se angajează să mențină un program de audit care să acopere domeniile legate de protecția datelor la nivelul unei Părți, în special toate aspectele reglementate de BCR. Toate părțile se vor angaja să fie auditate în mod regulat pentru a evalua și a testa conformitatea cu BCR și pentru a pune în aplicare mecanisme adecvate și suficiente pentru a remedia nerespectarea de către o Parte a BCR. Se vor efectua audituri planificate, care vor fi completate de audituri ad-hoc, în cazul în care Organizația pentru protecția datelor sau conducerea părților solicită acest lucru.

Auditurile planificate acoperă, *printre altele,* următoarele domenii: (i) guvernanța în materie de protecție a datelor (de exemplu, măsura în care politicile și procedurile de protecție a datelor în vederea respectării BCR sunt instituite și în funcțiune etc.), (ii) securitatea datelor cu caracter personal (de exemplu, măsurile tehnice și organizatorice instituite pentru a asigura o securitate adecvată a datelor cu caracter personal prelucrate etc.), (iii) Instruire și conștientizare (de exemplu, furnizarea și participarea la cursuri de formare în domeniul protecției datelor etc.), (iv) Solicitări ale persoanelor fizice și ale autorităților de supraveghere (de exemplu, procedurile în vigoare pentru a răspunde la solicitările persoanelor fizice, precum și comunicarea cu autoritățile de supraveghere etc.), (v) Transferuri de date: Frecvența și succesiunea auditurilor planificate vor fi stabilite anual în cadrul unui plan de audit bazat pe riscurile asociate

transferurilor relevante, luând în considerare, *printre altele,* următoarele aspecte: (i) volumul de date cu caracter personal, (ii) sensibilitatea datelor cu caracter personal (inclusiv dacă sunt afectate categorii speciale de date cu caracter personal), (iii) tipurile de persoane, (iv) importanța critică pentru operațiunile interne, precum și (v) impactul potențial asupra persoanelor, în special pe baza evaluărilor de impact asupra protecției datelor efectuate (a se vedea secțiunea 8). Cu toate acestea, numărul de părți auditate în cursul unui an nu trebuie să fie mai mic de 5.

Domeniul de aplicare al auditurilor *ad-hoc* este stabilit de Organizația pentru protecția datelor sau de conducerea părților, de la caz la caz.

Rezultatul fiecărui audit va fi un raport de audit care va fi emis în mod oficial către toate entitățile auditate, către consiliul de administrație relevant sau către conducerea superioară a organizației care le controlează, către LDPA, către responsabilul respectiv cu protecția datelor și către responsabilul pentru conformitate al părților. Organizația pentru protecția datelor va urmări orice audit efectuat pentru a evalua dacă acțiunile corective propuse au fost puse în aplicare în mod corespunzător și va documenta orice rezultat în raportul de audit. Fiecare Parte va pune la dispoziția autorităților de supraveghere, la cerere, rapoartele de audit.

Auditurile vor fi efectuate fie de către responsabilii cu protecția datelor, fie de către departamentul de audit intern al Fresenius, fie de către auditori externi, în colaborare cu responsabilii cu protecția datelor din sectorul respectiv, luând în considerare orice conflict de interese prin excluderea faptului că auditorul își auditează propriul domeniu de activitate.

10.7 Actualizarea BCR

Legile privind protecția datelor, precum și mijloacele, domeniul de aplicare și scopurile prelucrării datelor în general, sunt supuse unor evoluții constante. Părțile le vor analiza pe măsură ce acestea apar și vor evalua dacă sunt necesare modificări ale BCR. Prin urmare, Fresenius își rezervă dreptul de a modifica BCR, inclusiv, fără a se limita la, adăugarea de noi părți la BCR sau eliminarea unor părți din BCR.

Orice modificare a BCR care va afecta în mod semnificativ nivelul de protecție a datelor oferit de BCR sau de BCR în sine, inclusiv modificările administrative, dacă acestea au un impact asupra BCR, va fi raportată cu promptitudine fiecărei părți și autorității de supraveghere din Hesse, Germania (responsabilul BCR). Orice alte modificări

nesubstanțiale ale BCR vor fi raportate anual Autorității de supraveghere din Hesse, Germania, inclusiv o scurtă explicație a motivelor care justifică modificarea; părțile vor fi notificate cu privire la astfel de modificări cât mai curând posibil, în orice caz în termen de două (2) luni înainte de intrarea în vigoare a modificării sau variației BCR. Toate modificările și variațiile BCR vor fi publicate anual. Pentru evitarea oricărui dubiu: Autoritatea de Supraveghere din Hesse, Germania, are libertatea de a împărtăși oricare dintre aceste rapoarte cu alte autorități de supraveghere.

Responsabilii cu protecția datelor din cadrul FSE și FK AG, în colaborare, țin un registru actualizat care include (i) detaliile tuturor părților obligate să respecte BCR și (ii) o evidență a tuturor actualizărilor BCR. Aceștia vor permite, de asemenea, autorităților de supraveghere sau persoanelor fizice să acceseze informațiile din registru la cerere.

11 Managementul ieșirii

În cazul în care o Parte încetează să adere la BCR (de exemplu, prin rezilierea acordului intragrup respectiv), Partea respectivă fie (i) va returna imediat și, respectiv, va returna toate datele cu caracter personal tuturor părților care au transferat date cu caracter personal către Partea care părăsește grupul pe durata participării acesteia din urmă la BCR, fie (ii) va distruge, în conformitate cu normele locale de păstrare a datelor, toate aceste date cu caracter personal și va certifica în scris părților care transferă datele cu caracter personal că aceste date cu caracter personal au fost distruse, fie (iii) va asigura în alt mod garanții suficiente cu privire la aceste date cu caracter personal în sensul Artt. 44 și următoarele GDPR (de exemplu, prin încheierea unor clauze contractuale standard adoptate de Comisia UE). În cazul în care Partea care părăsește acordul nu poate oferi astfel de garanții suficiente, Partea care părăsește acordul poate continua să prelucreze astfel de date cu caracter personal numai în viitor și în măsura în care se acordă o derogare în temeiul art. 49 din GDPR (adică doar în scopurile acoperite de derogarea aplicabilă).

12 Referințe

Global-ANNEX-LE-000067672	Natura datelor cu caracter personal transferate
Global-ANNEX-LE-000067674	Lista părților obligate prin BCR

13 Istoricul modificărilor documentului

Versiunea	Motivul modificării și descrierea modificării

1.0 FDPB versiunea finală

Anexa 1: Lista Părților obligate prin BCR

No.	Numele și descrierea entității Fresenius	Țara
1	Fresenius Kabi S.A.	Argentina
2	Nutri Home S.A.	Argentina
3	Fresenius Kabi Australia Pty Ltd.	Australia
4	Fresenius Kabi Austria GmbH	Austria
5	Fresenius Kabi N.V.	Belgia
6	Gan Rio Apoio Nutricional - Ganutre Ltda.	Brazilia
7	Fresenius Kabi Brasil Ltda.	Brazilia
8	Fresenius HemoCare Brasil Ltda.	Brazilia
9	Fresenius Kabi Bulgaria EOOD	Bulgaria
10	Fresenius Kabi Canada Ltd.	Canada
11	Calea Ltd.	Canada
12	Calea Vancouver Inc.	Canada
13	Calea Pharmacy Ltd.	Canada
14	Fenwal International Inc., Cayman Islands	Grand Cayman
15	Fenwal International Inc., Domenican Republic branch	Republica Dominicană
16	Fenwal International Inc., Puerto Rico branch	Puerto Rico
17	Fresenius Kabi Chile Ltda.	Chile
18	Recetario Magistral Endovenoso S. A.	Chile
19	Laboratorio Sanderson S. A.	Chile
20	Beijing Fresenius Kabi Pharmaceutical Co., Ltd.	China
21	Fresenius Kabi (Beijing) Pharmaceutical Distribution Co. Ltd.	China
22	Fresenius Kabi (China) Co. Ltd.	China
23	Fresenius Kabi (Guangzhou) Co. Ltd.	China
24	Fresenius Kabi (Nanchang) Co., Ltd.	China
25	Fresenius Kabi Sino-Swed Pharmaceutical Corp. Ltd.	China
26	Fresenius Kabi Colombia S.A.S.	Columbia
27	Fresenius Kabi d.o.o.	Croația
28	Fresenius Kabi Horatev CZ s.r.o.	Republica Cehă
29	Fresenius Kabi s.r.o.	Republica Cehă
30	Fresenius Kabi S.A.	Ecuador
31	Fresenius Kabi Scientific Office - Egypt	Egipt
32	Fenwal France S.A.S.	Franța
33	Fresenius Kabi France S.A.S.	Franța

No.	Numele și descrierea entității Fresenius	Țara
34	Fresenius Kabi Groupe France S.A.S.	Franța
35	Fresenius Vial S.A.S.	Franța
36	Fresenius HemoCare GmbH	Germania
37	Fresenius Kabi AG	Germania
38	Fresenius Kabi Deutschland GmbH	Germania
39	Fresenius Kabi Logistik GmbH	Germania
40	medi1one Medical GmbH	Germania
41	MC Medizintechnik GmbH	Germania
42	Fresenius Kabi Ltd.	Marea Britanie
43	Calea U.K. Ltd.	Marea Britanie
44	Fresenius Kabi Hellas AEE	Grecia
45	Fresenius Kabi Asia Pacific Ltd.	Hong Kong
46	Fresenius Kabi Hongkong Ltd.	Hong Kong
47	Fresenius Kabi Hungary Kft.	Ungaria
48	Fresenius Kabi India Pvt. Ltd.	India
49	Fresenius Kabi Oncology Limited	India
50	PT. Fresenius Kabi Indonesia	Indonezia
51	PT. Fresenius Kabi Combiphar	Indonezia
52	Fresenius Kabi Ltd, Ireland branch.	Irlanda
53	Fresenius HemoCare Italia S.r.l.	Italia
54	Fresenius Kabi Italia S.r.l.	Italia
55	Fresenius Kabi iPSUM S.r.l.	Italia
56	Fresenius Kabi Japan K.K.	Japonia
57	Fresenius Kabi Korea Ltd.	Corea de Sud
58	Fresenius Kabi Baltics UAB	Lituania
59	Fresenius Kabi Malaysia Sdn Bhd	Malaezia
60	Fresenius Kabi México, S.A. de C.V.	Mexic
61	Fresenius Kabi Nederland B.V.	Olanda
62	Fresenius HemoCare Netherlands B.V.	Olanda
63	EnzyPep B.V.	Olanda
64	Fresenius Kabi NZ Ltd.	Noua Zeelandă
65	Fresenius Kabi Norge A/S	Norvegia
66	Fresenius Kabi Pakistan (Private) Limited	Pakistan
67	Fresenius Kabi Peru SA	Peru
68	Fresenius Kabi Philippines Inc.	Filipine
69	Fresenius Kabi Polska Sp. z o.o.	Polonia
70	Fresenius Kabi Business Services Sp.z.o.o.	Polonia
71	DOM Medica Sp. z o.o.	Polonia
72	Clinico Medical Sp. z o.o.	Polonia
73	Fresenius Kabi Pharma Portugal Lda.	Portugalia
74	Labesfal - Laboratórios Almiro, S.A.	Portugalia
75	Fresenius Kabi Romania S.R.L.	România

No.	Numele și descrierea entității Fresenius	Țara
76	Fresenius Kabi LLC	Federația Rusă
77	Fresenius Kabi d.o.o. Beograd	Serbia
78	Fresenius Kabi (Singapore) Pte Ltd.	Singapore
79	Fresenius Kabi South Africa (Pty) Ltd.	Africa de Sud
80	Fresenius Kabi Manufacturing SA (Pty) Ltd.	Africa de Sud
81	Fresenius Kabi Grupo España S.L.	Spania
82	Fresenius Kabi España S.A.U.	Spania
83	Quantium Medical S.L.U.	Spania
84	Fresenius Kabi AB , Sweden	Suedia
85	Fresenius Kabi AB, Finish branch	Finlanda
86	Fresenius Kabi AB, Denmark branch	Danemarca
87	Fresenius Kabi (Schweiz) AG	Elveția
88	Fresenius Kabi SwissBioSim GmbH	Elveția
89	FresuCare AG	Elveția
90	Fresenius Kabi Taiwan Ltd.	Taiwan
91	Fresenius Kabi (Thailand) Ltd.	Tailanda
92	Fresenius Kabi Tunisia S.a.r.l.	Tunisia
93	Fresenius Kabi İlaç San. ve Tic. Ltd. Şti.	Turcia
94	Fresenius Kabi Middle East FZ-LLC	Emiratele Arabe Unite
95	Fresenius Kabi Latin America Exports S.A	Uruguay
96	Fresenius Kabi, LLC	Statele Unite ale Americii
97	Fresenius Kabi USA, LLC	Statele Unite ale Americii
98	Fenwal Inc.	Statele Unite ale Americii
99	Fresenius Kabi Vietnam Joint Stock Company	Vietnam
100	Representative office of Fresenius Kabi Asia Pacific Limited	Vietnam
101	Fresenius SE & Co. KGaA	Germania
102	Fresenius Digital Technology GmbH	Germania
103	Fresenius Versicherungsvermittlungsgesellschaft mbH	Germania
104	Fresenius Management SE	Germania
105	Hyginus Publisher GmbH	Germania
106	Fresenius Digital Technology Polska sp. z o.o	Polonia
107	Fresenius Netcare Beijing Consulting Co.,Ltd	China
108	Fresenius Digital Technology India Private Limited	India
109	Fresenius Immobilien-Verwaltungs-GmbH	Germania
110	FPS Immobilien Verwaltungs GmbH	Germania
111	Fresenius ProServe GmbH	Germania
112	Fresenius Finance Ireland PLC	Irlanda
113	Fresenius Finance Ireland II PLC	Irlanda
114	Fresenius Finance Holdings Ltd	Irlanda
115	Fresenius Kabi Business Services Manila Inc	Filipine
116	GH Genhelix, S.A. (Unipersonal),	Spania

No.	Numele și descrierea entității Fresenius	Țara
117	Mabxience Research, S.L. (Unipersonal),	Spania
118	Mabxience, S.A.U.	Argentina
119	Mabxience, S.A	Elveția
120	Mabxience Holding, S.L.,	Spania

Anexa 2: Natura datelor cu caracter personal transferate

Următoarele date cu caracter personal fac obiectul unor transferuri în temeiul BCR în următoarele scopuri

Resurse umane

Următoarele date cu caracter personal ale managerilor, angajaților și candidaților unei părți pot fi transferate către alte părți în scopurile descrise în prezentul document:

Scop	Categorii de date
• Administrarea relațiilor de muncă • Administrarea și funcționarea IT și a comunicațiilor pentru angajați • Comunicări externă și site web • Gestionarea fluxului de lucru și a performanței, sancțiuni • Gestionarea cunoștințelor și a învățării • Gestionarea salariilor/plății salariilor/beneficii/pensii • Planificarea personalului și a resurselor • Recrutare, dezvoltarea carierei și angajare de personal • Comunicări internă, intranet • Fuziuni și achiziții • Conformitate, cerințe de reglementare	• Date de identificare și caracteristici personale (nume, vârstă, gen, cetățenie, număr național de identificare, imagine și date de contact) • Condiții de angajare, calificări, fișa postului • Date financiare (salarii, asigurări, impozite, pensii și beneficii) • Planificarea și performanța muncii (flux de lucru, proiecte și sarcini; ore lucrate; evaluare; sancțiuni) • Activitate în sindicate sau comitete de întreprindere • Condiții de sănătate • Comunicarea și utilizarea IT • Investigații privind conformitatea • Informații privind litigiile juridice • Certificate emise de poliție (cu condiția ca acestea să nu aibă mențiuni)

Client

Următoarele date cu caracter personal ale clienților și ale persoanelor de contact ale clienților unei părți pot fi transferate către alte părți în scopurile descrise mai jos:

Scop	Categorii de date
• Executarea contractelor/fabricarea, furnizarea și livrarea de produse și servicii/gestionarea reclamațiilor • Administrarea relațiilor cu clienții	• Nume, funcție, post și date de contact • Activitatea clientului • Tranzacții comerciale și relația cu clientul

Scop	Categorii de date
• Finanțe/facturare/încasarea plăților/ contabilitate • Marketing/relații cu clienții și gestionarea conturilor • Fuziuni și achiziții • Îndeplinirea cerințelor de conformitate și reglementare, cum ar fi verificarea prealabilă a partenerilor de afaceri, verificarea listei de sancțiuni, combaterea spălării banilor, securitatea lanțului de aprovizionare, legislația vamală și de export, urmărirea produselor, evaluarea riscului de credit	• Date financiare (bancare și de facturare) • Comunicarea și utilizarea IT • Detalii referitoare la înregistrările publice, registrele comerțului și consiliile profesionale

Pacienți

Următoarele date cu caracter personal ale pacienților și ale persoanelor asistate (de exemplu, îngrijitori) ale unei părți pot fi transferate către alte părți în scopurile descrise mai jos:

Scop	Categorii de date
• Executarea contractelor/fabricarea, furnizarea și livrarea de produse și servicii/gestionarea reclamațiilor • Administrarea relațiilor pacienților • Marketing/relații cu pacienții și gestionarea conturilor • Finanțe/facturare/încasarea plăților/contabilitate • Conformitatea și cerințele de reglementare • Fuziuni și achiziții • Studii clinice, cercetare și dezvoltare • Gestionarea situațiilor de urgență/evenimente adverse și vigilență	• Date de identificare și caracteristici personale (nume, vârstă, gen, naționalitate și date de contact) • Dosare medicale și condiții de sănătate • Tratamentul și relația cu pacientul • Date financiare (bancare și de facturare) • Comunicarea și utilizarea IT

Furnizor

Următoarele date cu caracter personal ale furnizorului și ale persoanelor de contact ale furnizorilor unei părți pot fi transferate către alte părți în scopurile descrise mai jos:

Scop	Categorii de date
• Marketing/gestionarea relațiilor cu furnizorii • Administrarea relațiilor cu furnizorii • Executarea contractelor/fabricarea, furnizarea și livrarea de produse și servicii/gestionarea reclamațiilor • Finanțe/facturare/contabilitate • Fuziuni și achiziții • Îndeplinirea cerințelor de conformitate și reglementare, cum ar fi verificarea prealabilă a partenerilor de afaceri, verificarea listei de sancțiuni, combaterea spălării banilor, siguranța lanțului de aprovizionare, legislația vamală și de export, urmărirea produselor, evaluarea riscului de credit	• Nume, funcție, post și date de contact • Activitatea furnizorului • Tranzacții comerciale și relația cu furnizorul • Date financiare (bancare și de facturare) • Comunicarea și utilizarea IT • Detalii referitoare la înregistrările publice, registrele comerțului și consiliile profesionale

Alte scopuri

Următoarele date cu caracter personal ale altor persoane fizice (de exemplu, contacte de urgență, contacte de presă) pot fi transferate către alte părți în scopurile descrise mai jos:

Scop	Categorii de date
• Gestionarea în caz de urgență, • IT • Securitate • Administrarea periodică a corespondenței, monitorizarea	• Nume și date de contact • Legătură cu Fresenius sau cu o persoană din grupul Fresenius • Alte informații necesare în acest scop.