Rezumat al regulilor obligatorii ale companiei (BCR)

Acest document reprezintă un rezumat și nu înlocuiește documentul BCR. Documentul BCR este singurul cu forță juridică în toate cazurile.

1 Un nivel adecvat și uniform pentru protecția datelor

Fresenius trebuie să respecte numeroase legi privind protecția datelor, din întreaga lume. Regulile obligatorii ale companiei (BCR) creează un cadru uniform și un nivel adecvat pentru protecția datelor. Aceste reguli fac posibil schimbul intern de date cu caracter personal între toate entitățile Fresenius implicate.

2 Aplicabilitate în întreaga lume

BCR sunt valabile pentru următoarele entități Fresenius:

- Fresenius Kabi AG, inclusiv toate filialele/entitățile afiliate
- Fresenius Digital Technology (FDT)
- Fresenius SE & Co. KGaA

Aplicabilitate pentru anumite activități

BCR se aplică următoarelor activități de prelucrare de date cu caracter personal:

- Toate activitățile realizate de către entități europene
- Activități ale entităților non-europene care sunt în legătură cu activitatea unei entități Fresenius din Europa::
  - în cazul în care în cadrul acestor activități se colectează date cu caracter personal în numele unei entități Fresenius europene sau
  - dacă ele colaborează cu o entitate Fresenius europeană sau
  - dacă primesc date cu caracter personal de la entități europene sau
  - Activități ale entităților non-europene cu persoane vizate care locuiesc în Uniunea Europeană, de exemplu, dacă ele colectează date cu caracter personal de la persoane cu reședința în Europa, pentru furnizarea de bunuri și servicii sau în scopuri de monitorizare a comportamentului.

BCR se aplică atât proceselor implementate în format fizic, pe hârtie, cât și celor IT.

BCR se aplică tuturor proceselor ce permit realizarea de căutări structurate prin date cu caracter personal.

3 BCR stabilesc nivelul minim

Dacă legislația locală privind protecția datelor cu caracter personal include prevederi mai stricte sau suplimentare cu privire la prelucrarea datelor cu caracter personal, acestea se vor respecta, pe lângă prevederile BCR.

Dacă legislația locală include prevederi în contradicție cu BCR, va trebui informat responsabilul cu protecția datelor (DPO). DPO va evalua impactul acestora și va remedia contradicția.

Dacă o entitate primește o dispoziție de la o autoritate pentru divulgarea de date cu caracter personal care nu respectă cerințele stipulate în BCR, este necesar să se informeze DPO. DPO va informa autoritatea de supraveghere din Germania.

4 BCR au caracter obligatoriu pentru organizația și angajații noștri

BCR au caracter obligatoriu și se vor respecta de către:

- Toate entitățile: ele semnează un contract
- Toți angajații: aceștia au obligația de a respecta în mod corect politicile companiei, conform contractului de angajare.

În cadrul acestor obligații, pot deriva drepturi pentru organizații și persoane (a se vedea, de exemplu, secțiunea 6, secțiunea 9 sau secțiunile 10-1-10.4).

Măsurile pentru punerea în aplicare a BCR și potențialele sancțiuni ca urmare a nerespectării BCR sunt aceleași ca și în cazul nerespectării altor politici.

5 Fresenius a înființat o organizație pentru protecția datelor

Fresenius Group a înființat o organizație internă de protecția datelor, în cadrul căreia s-au desemnat următoarele roluri și responsabilități:

- Responsabilul cu protecția datelor (DPO) monitorizează, adică verifică și supraveghează ca BCR, legislația locală și politicile și procedurile referitoare la protecția datelor să fie respectate. DPO poate efectua audituri, revizuiri și anchete. DPO este de asemenea persoana de contact pentru autoritățile pentru protecția datelor din Europa. Datele de contact sunt:

  Responsabil cu protecția datelor:
  Else-Kröner-Str. 1
  61352 Bad Homburg v.d.H.
  Germania
  Sau prin e-mail:
  Pentru Fresenius SE și FDT: dataprotectionofficer@fresenius.com
  Pentru entitățile Fresenius Kabi: dataprotectionofficer@fresenius-kabi.com

- Consultantul local cu privire la protecția datelor (CLPD) asistă și oferă consultanță angajaților la nivel local precum și responsabililor de proces, în caz de întrebări sau preocupări privind protecția datelor. La nevoie, CLPD oferă asistență Consultantului pentru protecția datelor și DPO, de exemplu, atunci când aceștia o solicită, ca parte a activității lor de monitorizare și de contact cu autoritățile de supraveghere, de exemplu datorită diferențelor lingvistice.

- Consultantul pentru protecția datelor (CPD) realizează activități de asistență și consultanță pentru CLPD și este responsabil de sistemul de management al protecției datelor. Atunci când este necesar, CPD asistă DPO, ca parte a activității sale de monitorizare și de contact cu autoritățile de supraveghere, de exemplu datorită diferențelor lingvistice.

6 Opt principii de protecție a datelor care trebuie urmate, conform BCR

La prelucrarea datelor cu caracter personal vom respecta o serie de principii al căror scop este de a proteja drepturile și libertățile fundamentale ale persoanelor fizice, conform cu BCR. Fiecare entitate trebuie să respecte următoarele principii atunci când prelucrează date cu caracter personal:

6.1 Principiul 1: Legalitate

Colectarea, utilizarea și prelucrarea datelor cu caracter personal trebuie să se facă pe un temei juridic documentat. Aceste temeiuri juridice sunt enumerate limitativ. Exemple:

- persoana și-a acordat consimțământul
- prelucrarea este necesară în vederea executării unui contract cu persoana respectivă, de exemplu, contractele de angajare sau de vânzare

- necesitatea de a respecta alte obligații legale, cum ar fi cele de natură fiscală, de vigilență sau cerințe de calitate (de exemplu, legate de fabricație sau documentație) .
- interesul legitim al Fresenius depășește consecințele negative pentru persoanele fizice respective

Categorii speciale de date, cum ar fi cele despre sănătate, necesită o bază legală suplimentară.

Dacă legislația locală include prevederi suplimentare sau contradictorii, acestea trebuie de asemenea respectate (poate fi cazul datelor despre angajați).

6.2 Principiul 2: Transparență și echitate

Gestionați datele cu caracter personal într-o manieră echitabilă și transparentă. Înainte sau la momentul acestor operațiuni, informați persoanele cu privire la colectarea și utilizarea datelor cu caracter personal, despre:

- Cine este responsabil și cum poate fi respectivul responsabil contactat
- Care sunt datele colectate
- Cum se colectează datele
- De ce avem nevoie de date (scop)
- Care sunt organizațiile cu care datele sunt partajate
- Dacă datele sunt transmise în alte țări
- Care este perioada de stocare a datelor
- Temeiul juridic pentru colectarea și utilizarea datelor și explicarea acestuia (principiul 1)
- Dacă se realizează profiluri pentru persoanele respective
- Dacă luăm decizii printr-un proces decizional automatizat
- Dacă furnizarea datelor este obligatorie și ce se întâmplă dacă nu sunt furnizate
- Datele de contact ale DPO și ale autorității
- Drepturile pe care le au persoanele fizice.

Toate aceste informații trebuie furnizate într-o manieră cuprinzătoare și ușor de accesat, într-un limbaj clar și simplu.

6.3 Principiul 3: Limitare în funcție de scop

Datele cu caracter personal se vor utiliza doar pentru scopurile specificate, explicite și legitime, în care au fost colectate. Alte utilizări nu sunt permise decât în cazul în care această utilizare ulterioară respectă scopul inițial și/sau dacă se iau măsuri suplimentare.

Scopuri pentru prelucrare ulterioară care sunt considerate în general ca respectând scopul inițial sunt:

- arhivare;
- audituri interne
- investigații

C(L)PD va putea să vă indice dacă noul scop este în conformitate cu cel original și, dacă este necesar, trebuie luate măsuri suplimentare. Dacă schimbarea scopului este permisă, persoanele trebuie să fie informate de astfel de schimbări.

6.4 Principiul 4: Reducere la minimum a datelor

Se vor colecta și utiliza doar datele cu caracter personal necesare pentru scopul specificat, comunicat persoanei respective. Acest principiu presupune că datele cu caracter personal colectate sunt relevante și volumul nu este excesiv, raportat la scop.

6.5 Principiul 5: Exactitate

Datele cu caracter personal trebuie păstrate corecte și actualizate. Se vor implementa proceduri ce asigură că datele incorecte se șterg, corectează sau actualizează fără întârziere.

6.6 Principiul 6: Limitări legate de stocare

Nu se vor păstra datele cu caracter personal pentru mai mult decât este necesar conform scopului în care au fost colectate, cu excepția cazului în care păstrarea mai îndelungată este solicitată prin lege. Într-un astfel de caz este necesar să se restricționeze accesul la aceste date. Datele cu caracter personal se vor șterge sau anonimiza dacă nu există niciun motiv de natură juridică pentru păstrate sau dacă scopul nu mai este relevant

6.7 Principiul 7: Securitate, integritate și confidențialitate

Se vor lua măsuri tehnice și organizaționale adecvate pentru a proteja datele cu caracter personal de distrugere, pierdere, alterare, divulgare sau acces (de ex. printr-un concept adecvat de roluri și drepturi, prin creare de copii de rezervă și restaurare sau prin folosirea criptării).

Securitatea sistemelor IT trebuie evaluată cu privire la aceste riscuri, atunci când se instalează și se întreține sisteme IT.

Orice breșă de securitate susceptibilă de a cauza un risc pentru persoanele afectate va fi documentată și raportată către organizația de protecție a datelor. În funcție de situație, astfel de breșe vor fi comunicate autorității de supraveghere, persoanelor vizate sau altor organizații.

6.8 Principiul 8: Responsabilitate

Se va putea demonstra conformitatea cu BCR. Conformitatea se va demonstra prin crearea și menținerea documentației adecvate, care include:

- evidențe ale activităților de prelucrare (RoPA)
- măsuri tehnice și organizaționale implementate pentru a respecta principiile privind protecția datelor și pentru a gestiona riscurile.
- evaluări privind riscul cu privire la protecția datelor și control

6.8.1 Implicarea persoanelor împuternicite

Se vor implica doar persoane împuternicire care oferă suficiente garanții de implementare a măsurilor tehnice și organizatorice adecvate într-o manieră care să asigure că prelucrarea respectă cerințele BCR și legislația locală cu privire la protecția datelor. Acest aspect se va asigura prin încheierea unui contract de protecție a datelor între respectiva entitate și persoana împuternicită.

6.8.2 Transfer (în continuare) al datelor cu caracter personal

Se vor implementa măsuri pentru a proteja în mod adecvat transferul de date cu caracter personal către alte organizații din afara Europei, cu respectarea BCR. Protecția se poate implementa prin stabilirea unor clauze contractuale standard cu cealaltă organizație, așa cum au fost adoptate de către Comisia Europeană.

7 Evaluarea riscurilor pentru protecția datelor

Pentru fiecare activitate de prelucrare a datelor este necesar să se efectueze o evaluare a riscurilor. Această evaluare este un proces formal de evaluare a impactului activității asupra drepturilor și libertății persoanelor vizate respective.

Zonele deficitare din punct de vedere al controlului și potențialele riscuri identificate la analiză trebuie raportate și documentate. Atenuarea măsurilor tehnice și organizaționale trebuie implementată înainte de inițierea activității de prelucrare a datelor.

8 Evaluarea impactului pentru protecția datelor

Dacă la evaluarea riscului pentru protecția datelor a rezultat că acesta este ridicat, se va face o analiză a impactului asupra protecției datelor (AIPD). Se va solicita asistența DPO.

Dacă AIPD identifică un risc ridicat pentru o anumită activitate de prelucrare a datelor, se vor implementa măsuri adecvate pentru atenuarea acestor riscuri, înainte de a iniția activitatea

de procesare. Dacă după implementarea acestor măsuri, AIPD încă indică un risc ridicat, se va consulta autoritatea de supraveghere aferentă, înainte de a prelucra datele.

9 Drepturile persoanelor vizate

Persoanelor vizate trebuie să li se acorde posibilitatea de a-și exercita drepturile (drepturile persoanelor vizate):

- **Dreptul de acces la datele cu caracter personal**: Persoana vizată poate solicita să acceseze/primească informații despre datele sale cu caracter personal prelucrate de către Fresenius (de ex. scopul prelucrării, categoriile de date cu caracter personal vizate, destinatarii, perioadele de stocare, existența unui proces decizional automatizat).
- **Dreptul la rectificare a datelor cu caracter personal:** Persoana vizată poate solicita corectarea datelor cu caracter personal incorecte sau incomplete.
- **Dreptul la ștergere a datelor cu caracter personal:** Persoana vizată poate solicita ștergerea datelor sale cu caracter personal, cu excepția cazului în care acestea trebuie păstrate pe baza unor cerințe legale de păstrare.
- **Dreptul de a restricționa prelucrarea datelor cu caracter personal:** Persoana vizată poate solicita restricționarea prelucrării datelor sale cu caracter personal dacă acuratețea acestora este contestată sau dacă prelucrarea nu este legală (nu mai este necesară conform scopurilor urmărite).
- **Dreptul de a primi datele cu caracter personal într-un format portabil:** Persoana vizată poate solicita să primească datele sale cu caracter personal într-un format utilizat în mod curent și care poate fi citit automat, dacă sunt îndeplinite următoarele condiții:
    - Datele cu caracter personal au fost oferite de către persoana vizată
    - Prelucrarea are loc pe baza consimțământului persoanei vizate sau a unui contract cu persoana vizată
    - Prelucrarea se realizează prin mijloace automate.
- **Dreptul la opoziție față de prelucrarea datelor cu caracter personal:** Datorită situației sale personale, persoana vizată are dreptul de a se opune prelucrării datelor sale cu caracter personal, pe baza unui interes legitim sau public. Astfel de solicitări trebuie evaluate. Persoana vizată are de asemenea dreptul de a se opune marketingului direct și creării de profiluri. În acest caz prelucrarea trebuie oprită.
- **Dreptul de a nu fi supus unui proces decizional automatizat:** Persoana vizată are dreptul de a nu fi supusă unui proces decizional automatizat (incl. crearea de profiluri) care poate conduce la consecințe legale sau de o semnificație similară asupra sa, mai puțin atunci când:
    - Procesul este necesar pentru executarea sau participarea la un contract între persoana vizată și respectiva entitate
    - Are la bază consimțământul acordat explicit al persoanei

10 Respectarea BCR

10.1 Acces la BCR

BCR trebuie să fie disponibile persoanelor, într-o manieră adecvată. BCR vor fi publicate pe internet și intranet.

Persoanele pot accesa BCR și prin contactarea respectivului responsabil cu protecția datelor sau a oricărui membru al organizației de protecție a datelor.

10.2 Gestionarea reclamațiilor cu privire la BCR

Orice persoană are dreptul de a:

- reclama încălcarea BCR, a legilor locale de protecția datelor, a ordinelor autorităților de supraveghere, a politicilor și directivelor interne sau a propriilor angajamente voluntare cu privire la protecția datelor
- adresa drepturile sale individuale
- exercita orice alt drept conform cu BCR.

Toate aceste reclamații pot fi înaintate, de exemplu, prin telefon, e-mail sau poștă, verbal prin adresarea către respectivul responsabil cu protecția datelor, către C(L)PD sau la linia de asistență telefonică pentru conformitate.

Dacă reclamația este considerată justificată, entitatea va lua măsura(măsurile) necesare pentru a o gestiona și va informa respectiva persoană în decurs de o lună.

10.3 Răspundere și aplicare

Persoanele care au fost afectate de către sau au suferit prejudicii ca urmare a procesării datelor cu caracter personal respective au dreptul de a solicita aplicarea acestei secțiuni din BCR și, dacă este cazul, să primească compensații conform deciziei unei instanțe competente.

Dacă se demonstrează încălcări de către entități din afara Europei, Fresenius SE &Co. KGaA acceptă răspunderea și responsabilitatea pentru eventualele prejudicii cauzate persoanelor fizice. Entitatea care a provocat prejudiciile va oferi Fresenius SE &Co. KGaA asistență, într-o măsură rezonabilă, pentru a răspunde la astfel de reclamații sau solicitări, într-un interval de timp rezonabil.

10.4 Cooperarea cu autoritățile de supraveghere

Fiecărei entități i se solicită să coopereze cu autoritățile de supraveghere, să respecte recomandările privind interpretarea acestor BCR și să accepte audituri efectuate de către autoritățile de supraveghere aferente.

10.5 Instruire

Fiecare entitate își va înscrie și obliga angajații să participe la un instructaj privind BCR și protecția datelor și să repete astfel de instructaje la intervale regulate. Un instructaj general trebuie să fie oferit cel puțin semestrial, pentru toți angajații. Instructaje specifice în funcție de rol (de exemplu pentru departamentele de relații umane sau de achiziții) trebuie să fie de asemenea oferite, luând în considerare nevoile specifice pentru anumite roluri/persoane.

10.6 Auditare

Toate părțile se vor angaja să se supună în mod regulat la audituri (planificate sau ad hoc), pentru a evalua și verifica respectarea BCR și pentru a implementa mecanisme adecvate și suficiente pentru remedierea cazurilor de neconformitate cu BCR a unei entități. Organizația de protecție a datelor va urmări auditurile efectuate pentru a evalua dacă acțiunile corective propuse au fost implementate corespunzător și va documenta rezultatele în raportul de audit. La cerere, toate entitățile vor pune rapoartele de audit la dispoziția autorităților de supraveghere.

10.7 Actualizare BCR

Părțile vor examina legislația locală de protecția datelor și vor semnala dacă sunt necesare modificări ale BCR. Fresenius poate modifica BCR dacă este necesar. Orice modificări semnificative ale BCR se vor anunța fără întârziere fiecărei entități și autorității de supraveghere. Modificările BCR care nu sunt de fond vor fi comunicate părților de îndată ce este fezabil.

11 Gestionarea retragerilor

Dacă o entitate încetează să mai adere la BCR (adică prin încetarea respectivului acord din interiorul grupului), ea fie va

- returna toate datele cu caracter personal părților de la care acestea au fost primite, fie
- în conformitate cu regulamentele locale de păstrare a datelor, va distruge orice astfel de date cu caracter personal, fie

- va oferi suficiente măsuri de salvgardare în ceea ce privește datele cu caracter personal (de exemplu, prin definirea unor clauze contractuale standard).