拘束力のある企業規則の概要（BCR）

本書は概要であり、BCR 文書の代用となるものではありません。いかなる場合も、BCR 文書が法的に適用可能な唯一の文書となります。

1 適切で統一されたレベルのデータ保護

Fresenius は、世界中の多くのデータ保護法に準拠する必要があります。拘束力のある企業規則（BCR）は、適切で統一されたレベルのデータ保護を設定します。これにより、適用範囲内の Fresenius 事業体間における、個人データの内部交換が可能になります。

2 世界中で適用可能

BCR は、以下の Fresenius 事業体に適用されます：

- Fresenius Kabi AG（全子会社/関連会社を含む）
- Fresenius Digital Technology (FDT)
- Fresenius SE & Co. KGaA

特定の活動に適用可能

BCR は、以下の個人データ処理活動に適用されます：

- ヨーロッパ事業体による全活動
- ヨーロッパ以外の事業体の全活動：
  - ヨーロッパFresenius事業体の代理で個人データを収集する場合、または
  - ヨーロッパFresenius事業体に協力する場合
  - ヨーロッパ事業体から個人データを受信する場合
  - 製品やサービスを提供するためにヨーロッパ在住の人からの個人データを収集する場合、またはモニタリング活動に関与する場合。

BCR は、紙ベースと IT ベースの両方のプロセスに適用されます。

BCR は、個人データを構造的に検索可能なすべてのプロセスに適用されます。

3 BCRは最低限のレベルを設定します

現地のデータ保護法が、個人データの処理においてより厳格な/追加規則を要求するような場合、これらを遵守する必要があります。

現地の法律が BCR と矛盾する場合、データ保護オフィサー（DPO）に報告する必要があります。データ保護オフィサー（DPO）はその影響を評価して、問題を解決します。

当局から BCR の要件に反するような個人データの開示命令を受けた場合、事業体はこれをデータ保護オフィサー（DPO）に通知する必要があります。データ保護オフィサー（DPO）は、ドイツの監督当局に通知します。

4 BCRは、組織とその従業員を拘束します。

BCR は義務付けられており、以下を拘束します：

- 全事業体：契約書に署名します

- 全従業員：雇用契約に基づく企業ポリシーに従う義務があります。

組織と人々の権利は、これらの義務の下で発生します。

BCR の施行と違反による制裁は、他のポリシー違反と同じです。

5 Fresenius はデータ保護組織を設立しました

Fresenius Group は、以下の役割と責任を担う内部データ保護組織を設立しました：

- データ保護オフィサー（DPO）は、データ処理がBCR、現地法、規則に準拠して行われているかどうかを確認・監督します。またデータ保護オフィサー（DPO）は、監査、レビュー、調査も行うことができます。データ保護オフィサー（DPO）は、ヨーロッパのデータ保護当局との窓口の役割も担当します。連絡先情報：

  データ保護担当者（DPO）：
  Else-Kröner-Str. 1
  61352 Bad Homburg v.d.H.
  ドイツ
  または電子メール：
  Fresenius SE and FDT： dataprotectionofficer@fresenius.com
  Fresenius Kabi 事業体： dataprotectionofficer@fresenius-kabi.com

- 現地データ保護アドバイザー（LDPA）は、データ保護に関連した質問や懸念について、いつでも現地従業員やデータ処理担当者の相談にのりアドバイスを与えます。現地データ保護アドバイザー（LDPA）は、たとえばモニタリング業務での言語の問題を解決するために、リクエストにより監督当局と連絡をとるなど、適宜データ保護アドバイザー（DPA）やデータ保護オフィサー（DPO）をサポートします。

- データ保護アドバイザー（DPA）は、現地データ保護アドバイザー（LDPA）へのサポートやコンサルティングを提供し、データ保護管理システムの管理を担当します。データ保護アドバイザー（DPA）は、たとえばモニタリング業務での言語の問題を解決するために、リクエストにより監督当局と連絡をとるなど、適宜データ保護オフィサー（DPO）をサポートします。

6 BCRの下で従うべき8つのデータ保護原則

個人データを処理する際は、BCR に従って、個人の基本的な権利と自由を保護するためにいくつかの原則に従います。各事業体は、個人データを処理する際は以下の原則に従う必要があります：

6.1 原則1：合法性

個人データを収集、使用、処理する際は、文書化された法的根拠があること。これらの法的根拠は、限定列挙されます。法的根拠の例：

- 雇用契約や販売契約などの個人との契約内容の実行に、処理が必要である
- 個人がデータ収集に同意した
- Fresenius の正当な利益が、個人へのマイナスの影響より大きい
- 税法、警戒要件、または GxP 要件などの他の法的根拠を満たす必要がある。

健康データなどの特殊カテゴリのデータは、追加の法的根拠が必要です。

現地法が追加または別の規定を求める場合は、これらに準拠する必要があります（たとえば、従業員データに関連する場合があります）。

6.2 原則2：透明性と公平性

公平で透明性のある手段で個人データを取り扱います。個人データを収集および使用する前/その時点で、以下を個人に通知します：

- 担当者とその連絡先情報
- 収集されるデータの種類
- データ収集の方法
- データを必要とする理由（目的）

- データが共有される組織
- データが他の国と共有されるかどうか
- データが保存される期間
- データの収集と使用についての法的根拠とその説明（原則１）
- 個人がプロファイルされる場合
- 自動化された手段で決定が下される場合
- 必須データが提供されない場合にどうなるか
- データ保護オフィサー（DPO）と当局の連絡先情報
- 個人の権利

このすべての情報は、包括的で簡単にアクセスできる形式で、明瞭でわかりやすい言葉を使って提供する必要があります。

6.3 原則3：目的の制限

個人データは、その収集目的が指定され、明示され、合法的である場合に限り使用できます。それ以上の使用は、それが本来の目的に沿ったものである場合、および/または追加措置が講じられている場合に限り許可されます。

一般に、本来の目的に沿っているとみなされる追加処理の目的：

- アーカイブ；
- 内部監査
- 調査

（現地）データ保護アドバイザー（L/DPA）は、目的変更の可否についてのガイダンスを提供することができます。目的変更が許可される場合は、そのような変更を個人に通知する必要があります。

6.4 原則4：データの最小化

個人に通知されている特定の目的のために必要とされる個人データだけを収集・使用します。つまりこれは、個人データがその目的に対して適切であり過剰ではないことを保証します。

6.5 原則5：正確性

個人データは正確で最新の状態に保ちます。不正確なデータを削除、修正または遅滞なく更新する手順を組み込む必要があります。

6.6 原則6：保存の制限

法律が求める場合を除き、収集される目的に必要とされる期間より長く個人データを保管しないでください。このような場合、個人データへのアクセスは制限される必要があります。法的根拠または目的がなくなった個人データは、削除または匿名化します。

6.7 原則7：セキュリティ、完全性、機密性

破壊、紛失、改ざん、開示、アクセスから個人データを保護するために、（たとえば、適切な役割と権利の概念、バックアップと復元、暗号化の使用などを通じた）適切な技術的および組織的対策を講じる必要があります。

そのような対策を実施する際には、個人へのリスクを考慮する必要があります。IT システムをインストールおよびメンテナンスする際には、このようなリスクを考慮して、IT システムのセキュリティを評価する必要があります。

関連する個人にリスクをもたらす可能性のあるセキュリティ違反を文書化して、データ保護組織に報告してください。状況に応じて、このような違反は、監督当局、個人または他の組織にも通知する必要があります。

6.8 原則8：説明責任

BCR への準拠を実証可能である必要があります。これは、次のような適切な文書の作成と保管によって行われます：

- 処理工程の記録
- データ保護原則を遵守し、リスクに対処するために講じられた技術的および組織的対策。
- データ保護のリスクと管理の評価

6.8.1 処理担当者の関与

処理方法が BCR および現地のデータ保護法の要件を満たし、適切な技術的・組織的対策を確実に実装できるような処理担当者のみが業務に従事します。

これは、それぞれの事業体と処理担当者間のデータ保護契約によって保証される必要があります。

6.8.2 （以降）個人データの転送

これらの BCR に準拠して、EEA 外に位置する他組織への個人データの転送を適切に保護するための対策を実施します。

これは、欧州委員会とその他の組織によって採択された、標準的な契約条項に合意することで実行できます。

7 データ保護リスク評価

各データ処理活動ごとに、データ保護リスク評価を実施する必要があります。

この評価は、関連各データ主体の権利と自由にこの活動が与える影響を評価するための正式なプロセスです。

特定された管理のギャップと潜在的なリスクを文書化して報告する必要があります。データ処理活動を開始する前に、技術的および組織的なリスク緩和対策を実施する必要があります。

8 データ保護影響評価

データ保護リスク評価の結果が高リスクである場合は、データ保護影響評価（DPIA）を実施する必要があります。データ保護オフィサー（DPO）のアドバイスを求めます。

データ保護影響評価（DPIA）で、特定のデータ処理活動でのリスクが高いと評価された場合、処理活動を開始する前に、そのようなリスクを緩和するための適切な措置を講じる必要があります。措置を講じた後も、データ保護影響評価（DPIA）が依然として高いリスクを示す場合は、データを処理する前に、関連監督当局に相談してください。

9 個人の権利

個人は、その権利（データ主体の権利）を行使できなければなりません：

- **個人データにアクセスする権利：**個人は、Fresenius によって処理された各個人データに関する情報へのアクセス/受信を要求することができます（処理の目的、関連する個人データのカテゴリ、受信者、保存期間、自動化された意思決定システムの存在など）。
- **個人データを修正する権利：**不正確/不完全な個人データは、修正を要求することができます。

- **個人データを削除する権利：**個人は、法的保持要件による場合などを除き、保管する必要がない個人データの削除を要求できます。
- **個人データの処理を制限する権利：**個人データの正確性に異議がある場合、または処理が違法（目的のために必要ではなくなった場合）である場合に、個人はその個人データの処理の制限を要求することができます。
- **ポータブル形式で個人データを受け取る権利：**以下の条件が満たされる場合、個人は、一般に使用され機械で読み取り可能な形式で、自分の個人データの受信を要求することができます：
    - 個人データを提供した本人である場合
    - 個人の同意または個人との契約に基づきデータが処理されている場合
    - 自動化された手段で処理が行われる場合。
- **個人データの処理に異議を唱える権利：**個人は、その状況に応じて、正当性または公益に基づき個人データを処理することに異議を唱えることができます。このような要求には評価を行う必要があります。さらに、個人はダイレクトマーケティングとプロファイリングに異議を唱えることができます。処理はその後停止する必要があります
- **自動化された意思決定プロセスの対象とならない権利：**以下の場合を除き、個人は法的または類似の重要な影響を個人に及ぼす可能性のある、自動化された意思決定プロセス（プロファイリングを含む）の対象とならない権利を有します：
    - 個人と各事業体との間で契約を締結または履行するために必要である場合
    - 個人の明示的な同意に基づく場合

10 BCRへの準拠

10.1 BCRへのアクセス

BCR は、適切な手段で個人が使用できる状態を保つ必要があります。BCR は、インターネットとイントラネットで公開されます。

個人は、各データ保護オフィサー（DPO）またはデータ保護組織のメンバーに連絡して、BCR にアクセスすることも可能です。

10.2 BCR苦情処理

各個人は以下の権利を有します：

- BCR、現地のデータ保護法、監督当局による命令、内部ポリシーとガイドライン、またはデータ保護に関連する自主的な自己規定への違反を主張する権利
- 個人の権利への対処
- BCR の他の権利の行使。

このような苦情は、電話、電子メールや手紙、口頭で、各データ保護オフィサー（DPO）、各（現地）データ保護アドバイザー（L/DPA）、またはコンプライアンスホットラインに送信することができます。

苦情が正当であるとみなされた場合、事業体は苦情に対処するために適切な措置を講じ、1 か月以内に当該個人に通知を行います。

10.3 責任と執行

各個人データの処理の結果、影響を受けた、または損害を被った個人は、BCR のこれらの箇所を執行する権利があり、該当する場合管轄裁判所において補償を受ける権利があります。

EU/EEA 外で設立された当事者による違反が証明された場合、FSE は個人が被った任意の損害に対する社会的責任および賠償責任を負います。損害を生じさせた事業体は、このような苦情や要求にタイムリーに対処できるように、FSE に合理的な支援を提供するものとします。

10.4 監督当局との協力

各事業体は、監督当局と協力し、これらの BCR の解釈についてのアドバイスを遵守し、関係する監督当局による監査を受け入れる必要があります。

10.5 トレーニング

各事業体は、従業員に BCR やデータ保護に関するトレーニングへの登録と参加、そのようなトレーニングの定期的な反復を義務付けるものとします。

一般的なトレーニングについては、2 年に 1 回以上、関連する全従業員に提供する必要があります。さらに、特定の役割/担当者に特有のニーズを考慮して、職務専用のトレーニング（人事部門や調達部門など）を提供します。

10.6 監査

すべての当事者は、BCR へのコンプライアンスを評価およびテストし、事業体の BCR へのコンプライアンス違反を是正するための適切で有効なメカニズムを組み込むために、（計画監査または臨時監査を通じた）定期的な監査に積極的に協力します。

データ保護組織は、実施された監査のフォローアップを行い、提案された是正措置が適切に実施されているかどうかを評価して監査報告書にその結果を記録します。各事業体は、要求に応じて監督当局に監査報告書を提出します。

10.7 BCRの更新

当事者は、現地のデータ保護法を検討し、BCR に変更が必要かどうかを決定します。

Fresenius は、必要に応じて BCR を修正することができます。BCR への重大な変更は、各事業体および監督当局に迅速に報告します。BCR へのその他の重大でない修正は、実行可能な限り速やかに当事者に報告します。

11 組織の出口管理

事業体が BCR の遵守を停止した場合（つまり、それぞれのグループ内契約が終了した場合）、そのような事業体は、

- すべての個人データを、データの受信元である任意の当事者に返却、または
- 現地のデータ保持規則に準拠して、該当するすべての個人データを破棄、または
- そのような個人データに十分な保護手段（たとえば、標準的な契約条項を締結するなど）を提供します。