Tóm tắt Quy tắc Ràng buộc Doanh nghiệp (BCR)

Tài liệu này là một bản tóm tắt và không thay thế tài liệu BCR. Tài liệu BCR trong mọi trường hợp sẽ là tài liệu duy nhất được áp dụng hợp pháp.

1 Mức độ bảo vệ dữ liệu đầy đủ và thống nhất:

Fresenius cần tuân theo các luật bảo vệ dữ liệu trên thế giới. Quy tắc Ràng buộc Doanh nghiệp (BCR) đặt ra một mức độ bảo vệ dữ liệu thống nhất và đầy đủ. Điều này cho phép việc trao đổi nội bộ dữ liệu cá nhân giữa các tổ chức Fresenius.

2 Áp dụng trên toàn thế giới:

BCR áp dụng cho các tổ chức Fresenius sau:

- Fresenius Kabi AG bao gồm tất cả các công ty con/công ty liên kết
- Fresenius Digital Technology (FDT)
- Fresenius SE & Co. KgaA.

Áp dụng cho các hoạt động nhất định

BCR áp dụng cho các hoạt động xử lý dữ liệu cá nhân sau:

- Tất cả các hoạt động của các tổ chức Châu Âu
- Hoạt động của các tổ chức không thuộc Châu Âu có liên quan đến hoạt động kinh doanh của một tổ chức Fresenius tại Châu Âu
  - Khi họ thay mặt một tổ chức Fresenius ở Châu Âu thu thập dữ liệu cá nhân hoặc
  - khi họ cộng tác với một tổ chức Fresenius ở Châu Âu hoặc
  - khi họ nhận được dữ liệu cá nhân từ các tổ chức Châu Âu hoặc
- Hoạt động thu thập dữ liệu từ chủ thể dữ liệu đang hiện diện ở Châu Âu thuộc các tổ chức ngoài Châu Âu, ví dụ họ thu thập thông tin cá nhân của cá nhân đang ở Châu Âu để cung cấp hàng hóa dịch vụ, hay theo dõi hành vi.

BCR áp dụng cho cả quy trình thủ công và quy trình dưa trên ứng dụng CNTT.

BCR áp dụng cho tất cả các quy trình cho phép sự tìm kiếm theo cấu trúc đối với dữ liệu cá nhân.

3 BCR thiết lập mức tối thiểu:

Nếu bất kỳ luật bảo vệ dữ liệu địa phương nào yêu cầu các quy tắc chặt chẽ hơn hoặc bổ sung về xử lý dữ liệu cá nhân, thì các quy tắc này cũng cần phải được tuân thủ.

Nếu luật địa phương xung đột với BCR, cần thông báo cho Chuyên Viên Bảo vệ Dữ liệu (DPO). DPO sẽ đánh giá tác động và giải quyết các xung đột đó.

Nếu một tổ chức nhận được lệnh của cơ quan có thẩm quyền yêu cầu tiết lộ dữ liệu cá nhân không phù hợp với các yêu cầu BCR, DPO cần được thông báo. DPO sẽ thông báo cho cơ quan giám sát ở Đức.

4 BCR có tính ràng buộc đối với tổ chức và nhân viên của chúng ta:

BCR cần phải được tuân thủ và có tính ràng buộc đối với:

- Tất cả các tổ chức: các tổ chức có ký kết hợp đồng
- Tất cả nhân viên: có nhiệm vụ tuân theo các chính sách của công ty dựa trên hợp đồng lao động của họ.

Các tổ chức và cá nhân có thể thực thi các quyền theo các nghĩa vụ này (xem các mục 6, mục 9 hoặc mục từ 10.1 – 10.4)

Việc thực thi BCR và các biện pháp trừng phạt do vi phạm cũng sẽ giống như các biện pháp trừng phạt đối với bất kỳ hành vi vi phạm chính sách khác.

5 Fresenius đã thành lập một tổ chức bảo vệ dữ liệu

Tập đoàn Fresenius đã thành lập một tổ chức bảo vệ dữ liệu nội bộ và giao các vai trò và trách nhiệm sau:

- Chuyên viên Bảo vệ Dữ liệu (DPO) theo dõi, kiểm tra và giám sát xem liệu BCR, luật địa phương, quy tắc và quy trình có được tuân thủ hay không. DPO có thể thực hiện kiểm tra, đánh giá và điều tra. DPO cũng là đầu mối liên hệ của các cơ quan bảo vệ dữ liệu ở Châu Âu. Chi tiết liên hệ như sau:

  Chuyên viên Bảo vệ Dữ liệu:
  Else-Kröner-Str. 1
  61352 Bad Homburg v.d.H.
  Đức
  Hoặc thông qua thư điện tử:
  Đối với Fresenius SE và FDT: dataprotectionofficer@fresenius.com
  Đối với các tổ chức Fresenius Kabi: dataprotectionofficer@fresenius-kabi.com

- Cố vấn Bảo vệ Dữ liệu địa phương (LDPA) có trách nhiệm giúp đỡ và tư vấn cho nhân viên địa phương cũng người thực thi quy trình bất cứ khi nào họ có câu hỏi hoặc thắc mắc liên quan đến bảo vệ dữ liệu. Khi cần thiết, LDPA hỗ trợ DPA và DPO, ví dụ: theo yêu cầu trong chức năng giám sát của mình và liên hệ với các cơ quan giám sát, ví dụ, do các vấn đề về ngôn ngữ.

- Cố vấn Bảo vệ Dữ liệu (DPA) có nhiệm vụ hỗ trợ và tư vấn cho các LDPA và chịu trách nhiệm về hệ thống quản lý bảo vệ dữ liệu. Khi cần thiết, DPA hỗ trợ DPO theo yêu cầu trong chức năng giám sát của mình và liên hệ với Cơ quan giám sát, ví dụ: do các vấn đề về ngôn ngữ.

6 Tám (08) nguyên tắc bảo vệ dữ liệu cần tuân thủ theo BCR:

Khi xử lý dữ liệu cá nhân, chúng ta sẽ tuân thủ một số nguyên tắc để bảo vệ các quyền và sự tự do cơ bản của cá nhân theo BCR. Mỗi tổ chức phải tuân thủ các nguyên tắc sau khi xử lý dữ liệu cá nhân:

6.1 Nguyên tắc 1: Tính hợp pháp

Có cơ sở pháp lý được lập thành văn bản khi thu thập, sử dụng và xử lý dữ liệu cá nhân. Các cơ sở pháp lý này được liệt kê có giới hạn. Ví dụ như:

- Có sự đồng ý của cá nhân
- quá trình xử lý là cần thiết để thực hiện hợp đồng với cá nhân, chẳng hạn như hợp đồng nhân viên và hợp đồng mua bán
- nhu cầu thực hiện các nghĩa vụ pháp lý khác, chẳng hạn như luật thuế, yêu cầu cảnh giác hoặc yêu cầu về chất lượng (ví dụ như liên quan đến các vấn đề sản phẩm, hồ sơ, hay sản xuất)
- lợi ích hợp pháp của Fresenius lớn hơn những hậu quả tiêu cực đối với các cá nhân.

Các danh mục dữ liệu đặc biệt, chẳng hạn như dữ liệu sức khỏe, cần có thêm cơ sở pháp lý.

Nếu luật pháp địa phương yêu cầu các điều khoản bổ sung hoặc các điều khoản khác, thì những điều khoản này cũng phải được tuân thủ (ví dụ, điều này có thể liên quan đến dữ liệu nhân viên).

6.2 Nguyên tắc 2: Tính Minh bạch và Công bằng

Xử lý dữ liệu cá nhân một cách công bằng và minh bạch. Thông báo cho các cá nhân trước hoặc tại thời điểm thu thập và sử dụng dữ liệu cá nhân về:

- Người chịu trách nhiệm và làm cách nào để liên hệ với người thu thập
- Dữ liệu nào được thu thập

- Cách thu thập dữ liệu
- Tại sao cần dữ liệu (mục đích)
- Dữ liệu được chia sẻ với tổ chức nào
- Nếu dữ liệu được chia sẻ với các quốc gia khác
- Dữ liệu sẽ được lưu giữ trong bao lâu
- Cơ sở pháp lý để thu thập và sử dụng dữ liệu và giải thích về điều đó (nguyên tắc 1)
- Trường hợp thông tin cá nhân được lập thành hồ sơ
- Nếu các quyết định đưa ra bằng phương thức tự động
- Nếu dữ liệu phải được cung cấp và điều gì sẽ xảy ra nếu điều đó không được thực hiện
- Thông tin liên hệ DPO và cơ quan có thẩm quyền
- Quyền của các cá nhân được thu thập dữ liệu.

Tất cả thông tin này phải được cung cấp toàn diện và ở dạng dễ tiếp cận, sử dụng ngôn ngữ rõ ràng và đơn giản.

6.3 Nguyên tắc 3: Giới hạn mục đích

Chỉ sử dụng dữ liệu cá nhân cho các mục đích cụ thể, rõ ràng và hợp pháp mà dữ liệu đó được thu thập. Không được phép sử dụng cho các mục đích khác, trừ khi việc sử dụng cho các mục đích khác là phù hợp với mục đích ban đầu và/hoặc các biện pháp bổ sung được thực hiện.

Các mục đích xử lý tiếp theo thường được coi là phù hợp với mục đích ban đầu là:

- Lưu trữ;
- Kiểm toán nội bộ;
- Điều tra.

Cố vấn Bảo vệ dữ liệu (địa phương) có thể cung cấp hướng dẫn về việc thay đổi mục đích và các biện pháp cần thiết bổ sung.Trong trường hợp được phép thay đổi mục đích, cá nhân phải được thông báo về bất kỳ thay đổi nào như vậy.

6.4 Nguyên tắc 4: Giảm thiểu dữ liệu

Chỉ thu thập và sử dụng dữ liệu cá nhân cần thiết cho mục đích xác định như đã thông báo cho cá nhân. Có nghĩa là đảm bảo dữ liệu cá nhân có liên quan và không quá mức theo mục đích.

6.5 Nguyên tắc 5: Tính chính xác

Giữ cho dữ liệu cá nhân luôn chính xác và cập nhật. Các thủ tục phải được thực hiện ngay để đảm bảo dữ liệu không chính xác sẽ được xóa, sửa hoặc được cập nhật.

6.6 Nguyên tắc 6: Giới hạn lưu trữ

Không lưu giữ dữ liệu cá nhân lâu hơn cần thiết cho mục đích mà dữ liệu cá nhân đã được thu thập, trừ khi luật pháp yêu cầu. Trong trường hợp đó, quyền truy cập vào dữ liệu cá nhân phải bị hạn chế. Xóa hoặc ẩn danh dữ liệu cá nhân nếu không có lý do hoặc mục đích pháp lý nào nữa.

6.7 Nguyên tắc 7: Tính an toàn, toàn vẹn và bảo mật

Thực hiện các biện pháp kỹ thuật và có tổ chức để bảo vệ dữ liệu cá nhân khỏi bị phá hủy, mất mát, thay đổi, bị tiết lộ hoặc truy cập trái phép (ví dụ: thông qua các khái niệm về vai trò và quyền hạn, sao lưu, khôi phục hoặc bằng cách sử dụng mã hóa).

Phải xem xét đánh giá mức độ rủi ro cá nhân khi cài đặt và bảo trì hệ thống công nghệ thông tin.

Lập hồ sơ và báo cáo cho tổ chức bảo vệ dữ liệu bất kỳ vi phạm bảo mật nào có khả năng dẫn đến rủi ro cho các cá nhân. Tùy từng trường hợp, những vi phạm đó cũng phải được thông báo cho cơ quan giám sát, cá nhân hoặc tổ chức khác.

6.8 Nguyên tắc 8: Trách nhiệm giải trình

Có thể chứng minh sự tuân thủ BCR. Điều này được thực hiện bằng cách tạo và duy trì tài liệu một cách thích hợp như:

- hồ sơ về các hoạt động xử lý

- các biện pháp kỹ thuật và có tổ chức được thực hiện để tuân thủ các nguyên tắc bảo vệ dữ liệu và đánh giá các rủi ro.
- thực hiện đánh giá rủi ro và các biện pháp kiểm soát trong việc bảo vệ dữ liệu.

6.8.1 Hợp tác với các bên xử lý:

Chỉ hợp tác với các bên xử lý đảm bảo được các biện pháp mang kỹ thuật và có tổ chức nhằm đáp ứng các yêu cầu của BCR và luật bảo vệ dữ liệu địa phương. Điều này phải được đảm bảo bằng hợp đồng bảo vệ dữ liệu giữa đơn vị tương ứng và bên xử lý.

6.8.2 Chuyển (gửi đi) dữ liệu cá nhân:

Thực hiện các biện pháp để bảo vệ đầy đủ việc chuyển dữ liệu cá nhân cho các tổ chức khác nằm ngoài EEA theo BCR. Điều này có thể được thực hiện bằng cách đồng ý các điều khoản hợp đồng tiêu chuẩn đã được Ủy ban Châu Âu thông qua với tổ chức khác.

7 Đánh giá rủi ro bảo vệ dữ liệu:

Đối với mọi hoạt động xử lý dữ liệu, phải thực hiện việc đánh giá rủi ro bảo vệ dữ liệu. Đánh giá này là một quá trình chính thức để đánh giá tác động của hoạt động đối với quyền và tự do của các đối tượng dữ liệu có liên quan.

Các lỗ hổng kiểm soát và rủi ro tiềm tàng sau khi xác định phải được báo cáo và lập thành văn bản. Các biện pháp về kỹ thuật và có tính tổ chức nhằm giảm thiểu rủi ro phải được thực hiện trước khi bắt đầu hoạt động xử lý dữ liệu.

8 Đánh giá tác động bảo vệ dữ liệu:

Nếu kết quả của đánh giá rủi ro bảo vệ dữ liệu cho thấy rủi ro cao, thì cần phải thực hiện đánh giá tác động bảo vệ dữ liệu (DPIA- Data Protection Impact Assessment). Cần tham vấn từ DPO.

Khi DPIA xác định có rủi ro cao đối với một hoạt động xử lý dữ liệu cụ thể, phải thực hiện các biện pháp thích hợp để giảm thiểu những rủi ro trước khi bắt đầu hoạt động xử lý. Nếu DPIA vẫn cho thấy rủi ro cao sau khi thực hiện các biện pháp, thì phải tham vấn đến cơ quan giám sát liên quan, trước khi xử lý dữ liệu.

9 Quyền của các cá nhân:

Các cá nhân phải được thực hiện các quyền của họ (quyền của chủ thể dữ liệu):

- **Quyền truy cập dữ liệu cá nhân**: Cá nhân có thể yêu cầu truy cập/nhận thông tin về dữ liệu cá nhân do Fresenius xử lý (ví dụ: mục đích xử lý, các loại dữ liệu cá nhân liên quan, người nhận, thời gian lưu trữ, sự tồn tại của các quyết định tự động).
- **Quyền chỉnh sửa dữ liệu cá nhân:** Cá nhân có thể yêu cầu sửa dữ liệu cá nhân không chính xác hoặc không đầy đủ.
- **Quyền xóa dữ liệu cá nhân:** Cá nhân có thể yêu cầu xóa dữ liệu cá nhân của mình trừ khi nó phải được duy trì, ví dụ: do các yêu cầu lưu giữ theo pháp luật.
- **Quyền hạn chế xử lý dữ liệu Cá nhân:** Cá nhân có thể yêu cầu hạn chế việc xử lý dữ liệu cá nhân của mình nếu tính chính xác của dữ liệu cá nhân bị tranh chấp hoặc việc xử lý là bất hợp pháp (không còn cần thiết cho các mục đích theo đuổi).
- **Quyền nhận dữ liệu cá nhân ở định dạng di động:** Cá nhân có thể yêu cầu nhận dữ liệu cá nhân của họ ở định dạng được phổ biến và định dạng có thể đọc bằng máy, nếu đáp ứng được các điều kiện sau đây:
  - Dữ liệu cá nhân được cung cấp bởi cá nhân
  - Việc xử lý dựa trên sự đồng ý của cá nhân hoặc trên hợp đồng với cá nhân đó
  - Quá trình xử lý được thực hiện bằng các phương thức tự động.
- **Quyền phản đối việc xử lý dữ liệu cá nhân:** Cá nhân có thể, do tình hình cá nhân của mình, phản đối việc xử lý dữ liệu cá nhân của mình dựa trên lợi ích hợp pháp hoặc công cộng. Yêu cầu này phải được xem xét . Hơn nữa, cá nhân có thể phản đối việc được tiếp thị trực tiếp và thu thập hồ sơ. Do vậy, quá trình xử lý này phải dừng lại.

- **<u>Quyền không phụ thuộc vào quyết định tự động:</u>** Cá nhân có quyền không phụ thuộc vào quyết định tự động (bao gồm lập hồ sơ) có thể dẫn đến những ảnh hưởng đáng kể về mặt pháp lý hoặc tương tự đối với cá nhân đó, trừ khi:
    - Cần phải giao kết hoặc thực hiện hợp đồng giữa cá nhân và tổ chức tương ứng
    - Nó dựa trên sự đồng ý rõ ràng của cá nhân.

10 Tuân thủ BCR

10.1 Truy cập vào BCR

BCR phải có sẵn cho các cá nhân theo phương thức thích hợp. BCR sẽ được công bố trên internet và mạng nội bộ.

Cá nhân cũng có thể truy cập BCR bằng cách liên hệ với DPO tương ứng hoặc bất kỳ thành viên nào của tổ chức bảo vệ dữ liệu.

10.2 Xử lý khiếu nại BCR:

Mỗi cá nhân có quyền:

- Công bố sự vi phạm BCR, các luật bảo vệ dữ liệu địa phương, điều lệnh của cơ quan giám sát, các chính sách và hướng dẫn nội bộ hoặc các cam kết tự nguyện liên quan đến việc bảo vệ dữ liệu
- Thể hiện các quyền cá nhân của mình
- Thực thi bất kỳ quyền nào khác của BCR.

Có thể gửi bất kỳ khiếu nại nào ví dụ: qua điện thoại, qua email hoặc thư, bằng miệng hay bằng cách liên hệ với DPO tương ứng, (L) DPA tương ứng hoặc đường dây nóng tuân thủ.

Trong trường hợp khiếu nại được coi là chính đáng, đơn vị sẽ thực hiện (các) hành động thích hợp để giải quyết khiếu nại và thông báo cho cá nhân có khiếu nại trong vòng một tháng.

10.3 Trách nhiệm pháp lý và thực thi:

Các cá nhân bị ảnh hưởng hoặc bị thiệt hại do quá trình xử lý Dữ liệu Cá nhân của họ, có quyền thực thi các phần của BCR và nếu có sẽ được bồi thường trước tòa án có thẩm quyền.

Trong trường hợp các tổ chức bên ngoài EU/EEA đã được chứng minh được hành vi vi phạm, Fresenius SE & Co. KGaA chấp nhận trách nhiệm và trách nhiệm pháp lý đối với bất kỳ thiệt hại nào đối với cá nhân. Tổ chức, người gây ra thiệt hại, sẽ cung cấp hỗ trợ hợp lý cho Fresenius SE & Co. KGaA để phản hồi các khiếu nại hoặc các yêu cầu một cách kịp thời.

10.4 Hợp tác với các cơ quan giám sát:

Mỗi tổ chức được yêu cầu hợp tác với các cơ quan giám sát, tuân thủ sự tư vấn liên quan đến sự diễn dịch BCR này và chấp nhận việc kiểm tra bởi các cơ quan giám sát có liên quan.

10.5 Đào tạo:

Mỗi tổ chức sẽ đăng ký và bắt buộc nhân viên của họ tham gia khóa đào tạo về BCR, bảo vệ dữ liệu và thường xuyên lặp lại khóa đào tạo đó. Đào tạo chung phải được cung cấp ít nhất hai năm một lần cho tất cả các nhân viên có liên quan. Hơn nữa, các khóa đào tạo cho các vị trí đặc thù (ví dụ: bộ phận Nhân sự hoặc Mua sắm) sẽ được cung cấp theo nhu cầu cụ thể của một số vị trí /nhân sự nhất định.

10.6 Kiểm tra:

Tất cả các bên cam kết về việc được kiểm toán thường xuyên (theo kế hoạch hoặc đột xuất) để đánh giá và kiểm tra việc tuân thủ BCR và thực hiện các cơ chế thích hợp, đầy đủ để khắc phục sự không tuân thủ của một tổ chức với BCR. Tổ chức bảo vệ dữ liệu sẽ theo dõi các cuộc kiểm toán đã thực hiện để đánh giá liệu các hành động khắc phục được đề xuất có được thực hiện một cách thích hợp và kết quả trong báo cáo kiểm toán có được ghi lại hay không. Mỗi tổ chức sẽ cung cấp báo cáo kiểm toán cho cơ quan giám sát khi có yêu cầu.

10.7 Cập nhật BCR:

Các bên sẽ xem xét luật bảo vệ dữ liệu địa phương và cho biết liệu có cần thiết cho việc thay đổi đối với BCR. Fresenius có thể sửa đổi BCR nếu cần thiết. Bất kỳ thay đổi quan trọng nào đối với BCR sẽ được báo cáo ngay cho từng tổ chức và cơ quan giám sát. Bất kỳ sửa đổi không quan trọng nào khác đối với BCR sẽ được báo cáo cho các bên trong thời gian sớm nhất có thể.

11 Ra khỏi BCR:

Trong trường hợp một tổ chức không còn tuân thủ BCR (tức là thông qua việc chấm dứt thỏa thuận nội bộ tương ứng), tổ chức đó phải:

- trả lại tất cả dữ liệu cá nhân cho bất kỳ Bên nào mà từ đó dữ liệu đã được nhận, hoặc
- tuân thủ các quy tắc lưu giữ dữ liệu địa phương, hủy tất cả dữ liệu cá nhân đó hoặc
- sẽ cung cấp đủ các biện pháp bảo vệ liên quan đến dữ liệu cá nhân đó (ví dụ: bằng cách ký kết các điều khoản hợp đồng tiêu chuẩn).