FVB-Datenschutzrichtlinie

- beschlossen vom Vorstand am 6. November 2019 -

1. Die Datenschutzorganisation des FVB

1.1 FVB-Verantwortliche

Die Verantwortlichen für den Datenschutz im Forschungsverbund Berlin e.V. sind die jeweiligen Institutsleiter*innen gemeinsam mit der Geschäftsführung des FVB. Hierbei sind die einzelnen Institutsleiter*innen nur für die datenschutzrelevanten Vorgänge in ihrem jeweiligen Institut verantwortlich. Bei mehreren Institutsleiter*innen in einem Institut sind diese gemeinsam verantwortlich.

Aufgaben der Verantwortlichen

Die Verantwortlichen entscheiden über Zwecke und Mittel der Verarbeitung. Sie legen Zuständigkeiten in Ihren Instituten bzw. im FVB fest und stellen die Einhaltung der europäischen Datenschutzgrundverordnung (DSGVO) sicher. Hierüber sind sie gegenüber der Aufsichtsbehörde nachweispflichtig (Art. 5.2 i.V.m. Art. 58 DSGVO). Darüber hinaus sind sie zur Sorgfalt gem. §§ 93 AktG, 43 GmbHG und 130 OWiG verpflichtet. Die Namen der jeweils Verantwortlichen finden sich in der Anlage.

1.2 FVB-Datenschutzbeauftragte

Die Verantwortlichen des FVB bestellen gemäß Art. 36 ff. DSGVO eine*n gemeinsame*n Beauftragte*n für den Datenschutz (DSB).

Aufgaben der/des FVB-Datenschutzbeauftragten

Die Aufgaben der/des DSB ergeben sich aus Art. 38 und 39 DSGVO sowie § 38 BDSG (neu). In erster Linie ist dies: die Überwachung der Einhaltung der Datenschutzvorschriften (Art. 39.1 DSGVO). Diese Überwachungsfunktion schließt auch entsprechende Prüfungen ein. Darüber hinaus überwacht die/der DSB die Sensibilisierung und Schulung der Mitarbeiter, berät Verantwortliche in Datenschutzfragen und ist Ansprechpartner*in für alle datenschutzrelevanten Fragestellungen - auch vertraulicher Art - sowohl von Mitarbeitern als auch von außerhalb des FVB. Sie/er ist die „Anwaltschaft der Betroffenen“. Schließlich begleitet die/der DSB Datenschutzfolgeabschätzungen der initiierenden Institute und Bereiche. Die/der DSB wird der zuständigen Aufsichtsbehörde (Berliner Landesbeauftragte*r für Datenschutz und Informationsfreiheit) gegenüber benannt und zusammen mit den jeweiligen Kontaktdaten auf der Website des Forschungsverbunds und in der Anlage dieser Richtlinien veröffentlicht.

1.3 FVB-Datenschutzkoordinatoren

Jedes Institut benennt eine*n eigene*n Datenschutzkoordinator*in (DSK). Sie/er wirkt in erster Line als Koordinierungsstelle zwischen DSB und den Mitarbeitern des Institutes. Die/der DSK verwaltet, aktualisiert und pflegt die Datenschutz-Dokumentation des Institutes. Hierzu zählen:

- Das Instituts-Verzeichnis der Verarbeitungstätigkeiten (vgl. Punkt 3).
- Die Aufstellung der Auftragsverarbeitungen des Instituts (vgl. Punkt 4).
- Risikobeurteilungen, etwa bei Datenschutzfolgeabschätzungen (vgl. Punkt 5).

Die/der DSK wird durch die jeweilige Institutsleitung berufen, unterstützt das Institut durch die Umsetzung von Standardprozessen, ist Erst-Ansprechpartner*in der Mitarbeiter für Datenschutzfragen - auch vertraulicher Art - und Erst-Anlaufstelle im Fall von Datenschutzverletzungen.[1] Sie/er stimmt sich regelmäßig mit der/dem DSB und den DSK der anderen FVB-Institute ab. Die Institutsleitung trägt Sorge für die fachliche Weiterbildung der jeweiligen DSK und stellt ihr/ihm ausreichend Zeit für die o.a. Tätigkeiten zur Verfügung. Die Namen der jeweiligen DSK findet sich in der Anlage.

1.4 Definitionen und Anwendungsbereich

Diese Datenschutzrichtlinie gilt für alle Mitarbeiter*innen des FVB. Sie gilt für jede Verarbeitung personenbezogener Daten (zu den Begriffen siehe unten), wenn diese

- ganz oder teilweise automatisiert erfolgt (z.B. mittels Computern)
- die Daten in einem Dateisystem (Art. 4 Nr. 6 DSGVO) gespeichert sind oder gespeichert werden sollen (z.B. auf einer Festplatte oder in Handakten), oder
- Daten über Mitarbeiter betrifft (z.B. Notizen aus einem Bewerbungsgespräch).

Art. 4 DSGVO definiert insgesamt 26 Begriffe. Im Folgenden sind die Definitionen der drei wichtigsten kurz zusammengefasst:

- *Personenbezogene Daten*
  sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. [Auf die Sensibilität kommt es nicht an, auch Kontaktdaten fallen darunter oder Angaben wie einer Benutzerkennung, die einer Person problemlos zugeordnet werden kann.]

- *Verarbeitung*
  ist jeder Umgang mit personenbezogenen Daten, insbesondere das Erheben, Erfassen [z.B. per Formular, Software oder auch einer Kamera], Speichern, Ändern, Übermitteln, Abgleichen, Verknüpfen, das Sperren oder Löschen.

- *Betroffener*
  ist die natürliche Person, auf die sich die personenbezogenen Daten beziehen [z.B. Mitarbeiter, Bewerber oder Lieferanten]

2. Einbindung der/des Datenschutzbeauftragten

Sollten sich Fragen mit Datenschutzhintergrund ergeben die von den direkt betroffenen Mitarbeitern oder Verantwortlichen nicht sicher geklärt werden können, ist die/der DSB einzubinden, in jedem Fall ist die/der DSB aber in den folgenden Fällen einzubinden:

- Eingang von Anfragen oder Beschwerden von Betroffenen (gegenwärtige oder ehemalige Mitarbeiter, Nutzer des FVB-Online-Angebots, Geschäftspartner).
- Einführung eines neuen Systems/Tools, das mit personenbezogenen Daten arbeitet.
- Einsatz eines neuen Dienstleisters im Bereich Auftragsverarbeitung.
- Installation von Kameras oder Videoüberwachung.
- Einbindung oder Nutzung von Online-Tools dritter Anbieter für die Internetpräsenz des FVB oder seiner Institute (Beispiel: Google Analytics).

[1] Die Dienststellung der DSK hinsichtlich Qualifikation, Reporting und Weisungen durch den DSB ist im FVB institutsindividuell geregelt.

- Betreiben von Fan-Pages in sozialen Medien (z.B. FVB-Facebook-Auftritt).
- Einführung neuer Prozesse mit Übermittlung von Daten in Drittländer außerhalb der EU.
- Initiierung von Projekten oder Veranstaltungen mit eigener Internetpräsenz.

3. Verzeichnis der Verarbeitungstätigkeiten

Für einen ordnungsgemäßen Schutz personenbezogener Daten im FVB ist es erforderlich festzustellen, wo und wie personenbezogene Daten erhoben und verarbeitet werden. Hierfür wird eine Aufstellung aller Systeme und Tools benötigt, mit denen personenbezogene Daten erhoben, gespeichert und/oder verarbeitet werden. Das Ergebnis ist das „Verzeichnis der Verarbeitungstätigkeiten“. In diesem Verzeichnis sind die wesentlichen Informationen zu Datenverarbeitungstätigkeiten zusammengefasst, speziell:

- Angaben zum Zweck der Verarbeitung
- Beschreibung der Kategorien der personenbezogenen Daten
- Beschreibung der Kategorien betroffener Personen
- Empfänger der verarbeiteten Daten
- Angaben zur Systemeignerschaft.

Diese Aufgabe ist eine Rechtspflicht der Verantwortlichen und leitet sich aus Art. 30 DSGVO ab.

3.1 Umsetzung der Erfassung

Die Aufgabe der Erfassung wird in den Instituten von den DSK übernommen. Sie können sich hierfür auf die jeweiligen Fachabteilungen, insbesondere die IT stützen. Die DSK der Institute verfügen über Formblätter zur Erfassung und Beschreibung der Verarbeitungstätigkeiten. Sie leiten die Ergebnisse an die/den DSB weiter.

4. Auftragsdatenverarbeitung

Nicht alle Leistungen, die der FVB erbringt, können im eigenen Haus erbracht werden. Für bestimmte Tätigkeiten, etwa die Gehaltsabrechnung, werden Dienstleister herangezogen. Hierbei ist sicherzustellen, dass die Dienstleister die Ihnen im Rahmen ihrer Tätigkeit bekannt gewordenen Daten des FVB sorgfältig schützen. Verantwortung und Haftung für die ordnungsgemäße Verarbeitung von FVB-Daten durch Externe („Auftragsdatenverarbeitung“) verbleiben im FVB.

Mit dem Dienstleister wird daher zusätzlich zum Leistungsvertrag eine Datenschutzvereinbarung getroffen, die die Verpflichtungen der Vertragsparteien zum Datenschutz konkretisiert. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Erfassung der Auftragsverarbeitungen erfolgt analog zu Punkt 3.1. Der FVB hat jederzeit einen Überblick über die Auftragsdatenverarbeitungen in seinem Verantwortungsbereich.

5. Datenschutz-Folgenabschätzung

Der FVB ist in bestimmten Fällen verpflichtet, eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen. Dies ist der Fall, wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko für personenbezogene Daten verursacht, insbesondere bei neuen Technologien oder aufgrund ihres Wesens, ihres Umfangs, ihres Kontexts oder ihrer Zwecke.
Hierbei ist die/der DSB von den initiierenden Instituten oder Fachbereichen rechtzeitig einzubinden.

6. Wahrnehmung von Betroffenenrechten

Mit der DSGVO erwachsen den Verantwortlichen neue Pflichten in Bezug auf die Information von Betroffenen. Die Betroffenen sollen wissen, wer welche Daten zu welchem Zweck über sie erhebt und

in die Lage versetzt werden, die hiermit verbundene Datenerhebung, Datenverarbeitung und Datennutzung zu prüfen.

6.1 Umfang der Mitteilungspflichten

Werden personenbezogene Daten erhoben, muss der Verantwortliche den Betroffenen nach Art. 13 und Art. 14 DSGVO folgende Informationen mitteilen:

- Identität des Verantwortlichen
- Kontaktdaten des DSB
- Verarbeitungszwecke und Rechtsgrundlage
- Berechtigtes Interesse
- Empfänger
- Übermittlung in Drittstaaten
- Dauer der Speicherung

6.2 Rechte der Betroffenen

Die Betroffenen einer Datenverarbeitung haben folgende Rechte:

- Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO)
- Auskunft (Art. 15 DSGVO)
- Berichtigung (Art. 16 DSGVO)
- Löschung (Art. 17 Abs. 1 DSGVO)
- Einschränkung der Verarbeitung (Art 18 DSGVO)
- Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruch gegen die Verarbeitung (Art. 21 DSGVO)
- Beschwerde bei der Aufsichtsbehörde (Art. 77 DSGVO).

Diese Anforderung kann nur dann erfüllt werden, wenn der FVB die Betroffenen ausreichend über die Datenverarbeitungsvorgänge informiert. Um die Betroffenen informieren zu können, muss im FVB und seinen Instituten wiederum bekannt sein, wo Informationspflichten bestehen (beispielsweise Teilnahme an FVB-Veranstaltung, Anmeldung zum Newsletter, etc.). Wenn Verantwortliche ihren Informationspflichten nicht nachkommen, droht gemäß Art. 83 Abs. 5 b DSGVO ein Bußgeld.

6.3 FVB-Datenschutzhinweise im Internet

Mit den Datenschutzhinweisen auf der jeweiligen Internetpräsenz kommen der FVB und seine Institute den oben beschriebenen Pflichten gegenüber Nutzern des Webangebotes nach. Die Datenschutzhinweise befinden sich unter dem Stichwort „Datenschutz“ prominent platziert auf der Einstiegsseite. Die Datenschutzhinweise benennen den jeweilig Verantwortlichen, die/den DSB des FVB und geben allgemeine Informationen zur Datenverarbeitung der jeweiligen Organisationseinheit. Darüber hinaus werden die Nutzer der Website über die von ihm erhobenen Daten in Logfiles und Cookies informiert und – wo vorhanden – auf Einbindungen von Web-Applikationen von Internetdienstleistern inklusive einer möglichen Anonymitätsoption hingewiesen. Schließlich werden die Nutzer über Ihre Rechte aufgeklärt.

Es wird auch eine Version in englischer Sprache zur Verfügung gestellt.

6.4 Umgang mit Anfragen und Beschwerden von Betroffenen

Für den Fall des Eingangs einer Anfrage oder Beschwerde ist sicherzustellen, dass der Anfragende oder Beschwerdeführer unverzüglich, also unmittelbar nach dem Eingang der Information, an die/den DSB des FVB weitergeleitet wird. Die/der DSB ist die offizielle Anlaufadresse für alle datenschutzbezogenen Anfragen von außen. Sollte die/der DSB nicht erreichbar sein ist ihr*e/sein*e Stellvertreter*in (vgl. Anlage) zu kontaktieren.

Die/der DSB nimmt das Anliegen entgegen, prüft und wird - gegebenenfalls nach Rücksprache mit eventuell betroffenen Fachbereichen - antworten bzw. eine Maßnahme veranlassen.

7. Verpflichtung auf das Datengeheimnis

Alle Beschäftigten des FVB werden mit der Aufnahme ihrer Beschäftigung auf das Datengeheimnis verpflichtet. Eine entsprechende Unterlage liegt den Einstellungsunterlagen bei. Sie ist vom Mitarbeiter zur Kenntnis zu nehmen, zu unterzeichnen und wird Teil der Personalakte. Eine Erfassung der Verpflichtungserklärungen erfolgt analog zu Punkt 3; alternativ ist eine Beauftragung der Erfassung durch den Personalbereich des jeweiligen Instituts möglich.
Die Verpflichtung ist als erste Sensibilisierungsmaßnahme zu werten, muss aber durch Schulungsmaßnahmen ergänzt werden.

8. Datenschutz-Schulungen

Im Rahmen der Datenschutzschulungen hat die/der DSB die ordnungsgemäße Durchführung zu überwachen. Dies gehört zu seinen Tätigkeitsaufgaben gemäß Art. 39 Abs. 1 DSGVO. Die Datenschutz-Schulung und die Verpflichtung auf das Datengeheimnis sind beide als Teil der organisatorischen Maßnahmen anzusehen, die dem Schutz der personenbezogenen Daten dienen.
Im FVB besteht die Möglichkeit, die/den DSB über die Überwachungsfunktion hinaus mit der Organisation und/oder Durchführung von Schulungen zu beauftragen. Die Verantwortlichen stellen hierfür entsprechende Ressourcen bereit.

9. Meldung von Datenschutzverstößen

Nach Art. 33 Abs. 1 DSGVO muss im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich – d.h. möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde – diese Verletzung bei der zuständigen Aufsichtsbehörde gemeldet werden. Von einer Meldung kann abgesehen werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen führt. Nach Art. 34 DSGVO sind bei einem hohen Risiko für die persönlichen Rechte und Freiheiten zusätzlich die Betroffenen zu informieren.

Um diesen Melde- und Informationspflichten nachkommen zu können, ist im FVB ein Prozess zum „Umgang mit Datenschutzverletzungen“ implementiert, mit dessen Hilfe die Verletzung des Schutzes personenbezogener Daten erkannt, der Sachverhalt an die/den DSB weitergeleitet und anschließend von diesem bewertet wird. Die/der DSB prüft dabei, ob ein Risiko für die Rechte und Freiheiten von Betroffenen vorliegt und wenn ja, wie dieses einzustufen ist.

10. Technisch-organisatorische Maßnahmen

Nach Art. 24. Abs. 1 und 32 DSGVO sind Verantwortliche und Auftragsverarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen (kurz: TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Verantwortliche muss nach Art. 5 Abs. 2 DSGVO die Einhaltung der Datensicherheit gewährleisten und nachweisen.

Die Maßnahmen sind unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu bestimmen.

10.1 Schutzziele bei der Verarbeitung personenbezogener Daten

Nach Art. 32 Abs. 1 lit. b) ergeben sich als Schutzziele:

- **Vertraulichkeit**, d.h. Daten sind für unberechtigte Dritte nicht zugänglich.
- **Integrität**, d.h. Daten können nicht verfälscht werden.
- **Verfügbarkeit**, d.h. Daten stehen zur Verfügung, wenn sie gebraucht werden.

Ein zusätzliches neues Schutzziel ist die „Belastbarkeit", also die „Resilienz" bzw. Widerstandsfähigkeit der Systeme und Dienste.

10.2 Mögliche Kontrollmaßnahmen

Die DSGVO erwähnt keine Einzelmaßnahmen. Aber im Rückgriff auf § 9 des Bundesdatenschutzgesetzes (BDSG) sind Kontrollmaßnahmen aus dem im Folgenden aufgeführten Spektrum zu ergreifen:

- **Zutrittskontrolle**

  Kein Zutritt von Unbefugten zu Räumen mit Datenverarbeitungsanlagen, mit welchen personenbezogene Daten verarbeitet werden. Beispiele für Einzelmaßnahmen: Alarmanlage, Pförtner.

- **Zugangskontrolle**
  Maßnahmen um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können. Beispiele: Passwortverfahren, Verschlüsselung.

- **Zugriffskontrolle**

  Sicherstellung, dass die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können für welche sie berechtigt sind **und** das personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können. Beispiele: Berechtigungskonzept, Datenträger-Kopierrichtlinie.

- **Weitergabekontrolle**

  Es muss verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und dass die Übermittlungspunkte dieser Daten im DV-System bekannt sind. Beispiele: Festplattencodierung, VPN.

- **Eingabekontrolle**

  Eine nachträgliche Überprüfung, ob, wann und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind. Beispiele: Protokollierung, Protokollauswertungssysteme.

- **Auftragskontrolle**

  Es muss sichergestellt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden (vgl. Punkt 4 dieser Richtlinie), gemäß den Weisungen des Auftraggebers verarbeitet werden. Beispiele: Vertragsgestaltung bei Auftragsdatenverarbeitung, Kontrollen.

- **Verfügbarkeitskontrolle**
  Sicherstellung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Beispiele: Firewall, Datensicherung.

- **Trennungsgebot**

  Maßnahmen um zu gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können. Beispiele: Mandanten, separate Produktiv- und Testsysteme.

Neben den oben aufgeführten Maßnahmen sind Verschlüsselungsverfahren nach aktuellem Stand der Technik zu berücksichtigen.

Prinzip der Verhältnismäßigkeit

Für TOM gilt ein Verhältnismäßigkeitsprinzip. Demnach müssen personenbezogene Daten nicht unendlich stark geschützt werden, wenn die Maßnahmen dafür wirtschaftlich unangemessen hoch ausfallen würden. Daraus lässt sich ableiten, dass etwa bei einer Auftragsdatenverarbeitung (ADV) der Dienstleister, welcher nur einen Teil der Daten zur Bearbeitung erhält, nicht zwingend die gleichen Schutzmaßnahmen treffen muss, wie sie etwa die verantwortliche Stelle ausführt.

Anlage

Stand 04.12.2019

Die Verantwortlichen i.S.d. DSGVO sind

FBH: Hr. Prof. Dr. G. Tränkle
FMP: Fr. Prof. Dr. D. Fiedler/Hr. Prof. Dr. V. Haucke
IGB: Hr. Prof. Dr. M. Gessner (kommissarisch)
IKZ: Hr. Prof. Dr. T. Schröder
IZW: Hr. Prof. Dr. H. Hofer
MBI: Hr. Prof. Dr. S. Eisebitt/Hr. Prof. Dr. T. Elsässer/Hr. Prof. Dr. M. Vrakking
PDI: Hr. Prof. Dr. H. Riechert
WIAS: Hr. Prof. Dr. M. Hintermüller
GV: Fr. Dr. M. Urban

Datenschutzbeauftragter des FVB ist

Hr. Johannes Höper
Rudower Chaussee 17
12489 Berlin
Tel: +49-30-6392-3311
E-Mail: datenschutz@fv-berlin.de

Stellvertretender Datenschutzbeauftragter des FVB ist

Hr. Frank Schilling
Robert-Roessle-Str. 10
13125 Berlin
Tel: +49 30 94793-401
E-Mail: schilling@fmp-berlin.de

Die Datenschutzkoordinatoren sind

FBH: Hr. V. Bentlage
FMP: Hr. F. Schilling
IGB: Hr. E. Willenbuecher
IKZ: Hr. T. Remmele
IZW: Hr. I. Heckmann
MBI: Hr. Dr. A. Grimm
PDI: Hr. Dr. B. Pakulat
WIAS: Hr. Dr. A. Rathsfeld
GV: N.N.; Hr. J. Höper ohne gesonderte Beauftragung