

INFORMATIONEN ZUR DATENVERARBEITUNG FÜR MITARBEITENDE NACH ARTIKELN 13 und 14 DER DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Liebe Mitarbeiterinnen und Mitarbeiter,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach Artikeln 13 und 14 der EU-Datenschutz-Grundverordnung (DSGVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck und auf welcher Rechtsgrundlage wir Daten erheben, speichern oder weiterleiten und welche Datenschutzrechte gemäß den Artikeln 15 bis 22 der DSGVO Sie wahrnehmen können.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern im Folgenden die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Schutz Ihrer Daten

Beschäftigtendaten enthalten Privatgeheimnisse der betroffenen Mitarbeiter und unterliegen einer besonderen Vertraulichkeit nach den Bestimmungen des Datenschutzes. Ihre Vorgesetzten und alle Mitarbeiter der Personalabteilungen sind auf die Einhaltung der Datenschutzbestimmungen verpflichtet worden.

Zum Schutz Ihrer persönlichen Daten halten der DRK-Blutspendedienst Baden-Württemberg – Hessen gemeinnützige GmbH, Nord-Ost gGmbH und seine Tochtergesellschaften die Auflagen der EU-Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) strikt ein. Ihre persönlichen Daten werden nur für die Zwecke der Begründung, der Durchführung und der Beendigung des Beschäftigungsverhältnisses genutzt.

Keinesfalls werden Ihre Daten für Werbezwecke Dritter (kommerzielle Werbung, dies schließt auch die Werbung für sonstige Aufgaben des Deutschen Roten Kreuzes ein) genutzt oder weitergegeben. Zum Schutz der Anlagen der Informationstechnologie gegenüber einem

unberechtigten Zugriff Dritter sind Schutzmaßnahmen nach dem geltenden Stand der Technik eingeführt, der den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht.

Die folgenden Abschnitte dienen dazu, Sie über die mit dem Arbeitsverhältnis verbundene Verarbeitung personenbezogener Daten aufzuklären.

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

Die zentrale verantwortliche Stelle der Datenverarbeitung ist für die Institute und Tochtergesellschaften in Baden-Württemberg und Hessen der DRK-Blutspendedienst Baden-Württemberg – Hessen gGmbH mit Sitz in Mannheim. Die weiteren Institute und Tochtergesellschaften befinden sich in Frankfurt am Main, Kassel, Baden-Baden, Ulm, Heidelberg, Hamburg, Tübingen und Bad-Krozingen. Die Kontaktinformationen der Institute befinden sich in der Anlage A.

Die zentrale verantwortliche Stelle der Datenverarbeitung ist für die Institute und Tochtergesellschaften in Berlin, Brandenburg, Schleswig-Holstein und Sachsen der DRK-Blutspendedienst Nord-Ost gGmbH mit Sitz in Dresden. Die weiteren Institute befinden sich in Berlin, Chemnitz, Cottbus, Lütjensee, Plauen, Potsdam, Schleswig, Leipzig, Görlitz, Neuruppin und Zwickau. Die Kontaktinformationen der Institute befinden sich in der Anlage B.

Wenn Sie in einem der angeschlossenen Institute oder Tochtergesellschaften tätig sind, findet eine gemeinsam verantwortliche Datenverarbeitung des genannten Blutspendedienstes mit diesem Institut oder Tochtergesellschaft als ebenfalls verantwortliche Stelle statt.

Die Institute oder Tochtergesellschaften, die bei Ihrer dortigen Tätigkeit eine für Sie mit dem genannten Blutspendedienst gemeinsam verantwortliche Stelle sein können, finden Sie in der Anlage A für Baden-Württemberg – Hessen und in der Anlage B für Nord-Ost.

Die Datenverarbeitung der Beschäftigtendaten im DRK-Blutspendedienst Baden-Württemberg – Hessen gGmbH erfolgt zentral in der Personalabteilung in Baden-Baden. Die Datenverarbeitung der Beschäftigtendaten im DRK-Blutspendedienst Nord-Ost gGmbH erfolgt in der Personalabteilung an den Standorten Berlin und Dresden, mit zentraler Datenspeicherung auf den Servern am Standort Dresden. Wenn Sie in einer der angeschlossenen Institute oder Tochtergesellschaften tätig sind, erfolgt eine begrenzte

dezentrale Verarbeitung Ihrer personenbezogenen Beschäftigtendaten im Personalbüro dieses Institutes oder dieser Tochtergesellschaft.

Ihr Kontakt zum Datenschutzbeauftragten:

Externer Datenschutzbeauftragter der genannten verantwortlichen Stellen außer Klinik Dr. Becker und MVZ Dr. Becker ist Dr. Hartmut Voelskow. E-Mail Adressen, über die E-Mails an den Datenschutzbeauftragten (über das externe Netz) weitergeleitet werden:

Institute Baden-Württemberg – Hessen, IKT und MVZ Ulm, ZKT Tübingen, IKTZ Heidelberg und MVZ Frankfurt/M.: datenschutzbeauftragter@blutspende.de

Institute Nord-Ost: datenschutz-no@blutspende.de

ZIT Hamburg: Datenschutzbeauftragter-ZIT@blutspende.de

ZTB Berlin: datenschutz@ztb-charite.de

Antworten vom Datenschutzbeauftragten erhalten Sie über eine abweichende externe E-Mailadresse. Bei einer Kontaktaufnahme geben Sie bitte an, in welchem Institut Sie tätig sind.

Der Datenschutzbeauftragte der Klinik Dr. Becker und MVZ Dr. Becker ist Jörg M. Leuchtner, Rechtsanwalt, Freiburger Datenschutzgesellschaft mbH, Luisenstr. 5, D - 79098 Freiburg, E-Mail: info@freiburger-datenschutzgesellschaft.de

Schutz Ihrer elektronischen Kommunikation:

Für eine Kontaktaufnahme per E-Mail beachten Sie bitte, dass bei unverschlüsselter E-Mail-Kommunikation über die externe Leitung, also von Ihrer privaten E-Mailadresse aus und beim unverschlüsselten Senden an den Datenschutzbeauftragten, die Sicherheit Ihrer Mitteilungen auf dem Übertragungsweg nicht gewährleistet werden kann. Wenn Sie die E-Mailverschlüsselung nicht nutzen, erfolgt der externe E-Mailverkehr nur abschnittsweise transportverschlüsselt, also nicht durchgehend geschützt vom Sender bis zum Empfänger.

Verwenden Sie für die Kommunikation mit der Personalabteilung bitte wenn möglich Ihre interne E-Mailadresse. E-Mails an den Datenschutzbeauftragten mit vertraulichen Inhalten senden Sie bitte mit der im Unternehmen eingeführten E-Mailverschlüsselung. Wenn Sie aus wichtigen Gründen, z. B. im Krankheitsfall vom privaten Anschluss aus, wichtige Informationen senden müssen, dann bedenken Sie bitte, dass eine unverschlüsselte Übermittlung das Risiko birgt, dass Dritte Ihre Daten auf dem Übertragungsweg zur Kenntnis nehmen oder verfälschen können. Das Risiko dafür trägt jeweils der Absender einer E-Mail.

Ersatzweise können Sie, wenn keine E-Mailverschlüsselung zur Verfügung steht, auch verschlüsselte Dateianlagen senden. Mit geeigneter Software (z. B. dem kostenfreien PDF24) können Sie die Dateiverschlüsselung für PDF-Dateien einstellen oder (z. B. mit der Software 7-zip) Ihre Dateianlagen in eine verschlüsselte ZIP-Datei verpacken. (Bitte Umschalten auf 256-Bit, denn das voreingestellte Format zip-krypto ist nicht sicher). Das Passwort zum Öffnen teilen Sie uns dann bitte telefonisch an die folgende Telefonnummer mit: 0621/3706-8287.

2. Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?

Ihre persönlichen Daten werden nur für die Zwecke der Begründung eines Beschäftigungsverhältnisses im Rahmen des Einstellungsverfahrens und anschließend nach Abschluss des Arbeitsvertrages für den Zweck der Abwicklung des Beschäftigungsverhältnisses sowie damit verbundener rechtlicher Verpflichtungen genutzt.

Die Personaldaten umfassen folgende Angaben

Unterlagen, die bereits aus den Bewerberdaten übernommen wurden:

- Identifikation, Adresse, gegebenenfalls die Telefonnummer.
- Qualifikations- und Weiterbildungsdaten mit Kopien von Zeugnissen der schulischen Ausbildung und soweit bereits vorhanden der beruflichen Aus- und Weiterbildung.
- Angaben zur beruflichen Erfahrung und der wesentlichen Stationen des bisherigen beruflichen Werdeganges, soweit Sie diese bei Ihrer Bewerbung angegeben hatten.
- Alter, wenn es bereits im Bewerbungsverfahren erforderlich war oder freiwillig angegeben wurde.
- Angaben zur gesundheitlichen Eignung, wenn diese im Rahmen der Bewerbung für die zu besetzende Stelle angegeben werden mussten.
- Gegebenenfalls Daten aus beruflichen Netzwerken wie Xing oder LinkedIn.
- Gegebenenfalls Angaben des bisherigen oder eines früheren Arbeitgebers, wenn Sie diesen bei der Bewerbung als Referenz angegeben hatten.

Nach der Einstellung kommen Daten hinzu, die für die Entgeltabrechnung und die Abgaben an das Finanzamt sowie die Sozialversicherung erforderlich sind:

- Geburtsdatum, Religionszugehörigkeit, Familienstand.
- Krankenversicherungsnummern und Bankverbindung.

Unter den Beschäftigtendaten können im Laufe eines Arbeitslebens weitere Datenarten verschiedener Kategorien zusammenkommen.

Innerhalb der Personalabteilung verarbeitete Daten:

- Qualifikations- und Weiterbildungsdaten, die fortlaufend während des Beschäftigungsverhältnisses erfasst werden.
- Daten und Stationen des beruflichen Werdeganges im Unternehmen und Zwischen-Beurteilungen, Zielerfüllung.
- Daten der jeweiligen Eingruppierungen und Einstufungen und Gehaltshöhen, ggf. auch von Sonderzahlungen, Zulagen.
- Zeiterfassungsdaten, Summen der Arbeitszeiten, Abwesenheitsdaten sowohl von Urlaubszeiten als auch von Krankheitstagen.
- ggf. die Angabe einer Schwerbehinderung oder Gleichstellung und Grad der Behinderung.
- ggf. eine freiwillige Angabe zum Gesundheitszustand.
- Daten und Informationen über besondere Ereignisse wie zum Beispiel auch Abmahnungen.
- Pfändungen/ Abtretungen.
- Unterlagen zur betrieblichen Altersversorgung sowie Entgeltumwandlung.

Die Rechtsgrundlage für alle genannten Kategorien ergibt sich aus § 26 des Bundesdatenschutzgesetzes in der neuen Fassung (in Kraft ab 25.05.2018) zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses und zum Teil in Verbindung mit dem Steuerrecht und Sozialgesetzbuch, da alle diese Daten für die ordnungsgemäße Abwicklung des Beschäftigungsverhältnisses, für die nach Steuerrecht erforderlichen Meldungen an die Finanzämter und für die Zahlungen an die Sozial- und Krankenversicherungen erforderlich sind.

Die Herkunft der Daten ist bis auf folgende Ausnahmen 1.) und 2.) grundsätzlich direkt von Ihnen, 1.) bei ggf. aus beruflichen Netzwerken wie Xing oder LinkedIn erfassten Daten und 2.) ggf. bei Daten eines früheren Arbeitgebers, wenn Sie diesen im Bewerbungsverfahren als Referenz angegeben hatten.

Weitere Verwendungszwecke in besonderen Fällen

Betriebsratsarbeit, Betriebsratswahlen und Aufsichtsratswahlen:

Für die Betriebsratsarbeit können in Einzelfällen personenbezogene Daten an den Betriebsrat weitergegeben werden. Rechtsgrundlage sind die jeweiligen Pflichten zur Mitbestimmung nach dem Betriebsverfassungsgesetz. Details siehe unten unter „Datenübermittlungen an den Betriebsrat“.

Zur Vorbereitung von Betriebsratswahlen und für die Belegschaftsvertreter bei Aufsichtsratswahlen werden Namen und Kontaktdaten von Mitarbeitenden von der Personalabteilung an den Wahlvorstand weitergegeben. Die Rechtsgrundlage für Datenübermittlungen von der Personalabteilung an den Wahlvorstand von Betriebsratswahlen oder Aufsichtsratswahlen wird unten in den Abschnitten „Datenübermittlungen für die Vorbereitung von Wahlen“ und „Datenübermittlungen an den Betriebsrat“ angegeben.

Revisionsprüfungen:

Im Rahmen von Revisionsprüfungen können in Einzelfällen personenbezogene Daten an die Firma Tasco weitergegeben werden. Der Zweck sind die an die Tasco ausgelagerten Prüfungen der Internen Revision. Die Information der Mitarbeitenden erfolgt über die vorherigen Ankündigungen der Revisionsprüfungen. Die Rechtsgrundlage wird unten im Abschnitt „Datenübermittlungen im Rahmen von Revisionsprüfungen“ angegeben.

Außerhalb der Personalabteilung erfasste und verarbeitete Daten:

- Speicherung von E-Mails im E-Mail-Dokumentationssystem.
Zweck und Rechtsgrundlage: Einhaltung der Archivierungspflichten nach Abgabenordnung und Handelsgesetzbuch. Wichtiger Hinweis: Ihre Korrespondenz mit der Personalabteilung wird nicht in das Dokumentationssystem aufgenommen.
- Benutzerdaten und Berechtigungsdaten in der Verwaltung der Systeme zur Datenverarbeitung
Zweck und Rechtsgrundlage: Abwicklung des Beschäftigungsverhältnisses sowie Schutzvorschriften in Bezug auf die Datenverfügbarkeit nach dem Datenschutzrecht, AMG und TFG.
- Mitarbeiterbezogene Datensatzkennungen bei allen Tätigkeiten in GMP-konformen Systemen zur Datenverarbeitung
Zweck und Rechtsgrundlage: Gesetzliche Forderung nach dem AMG und TFG, die Datenverarbeitung GMP-konform zu gestalten. Nach diesen Regeln ist für die Rückverfolgbarkeit der Bearbeitung die Speicherung erforderlich, wer einen Datensatz angelegt und wer ihn zuletzt geändert hat.
- Zutrittsdaten im Transponderchip-basierten Zutrittskontrollsystem
Zweck und Rechtsgrundlage: Einerseits die Abwicklung des Beschäftigungsverhältnisses, um die notwendigen Zutritte für die Erledigung der

dienstlichen Aufgaben zu ermöglichen und andererseits die Schutzvorschriften in Bezug auf die Zutrittsbegrenzungen nach dem Datenschutzrecht, AMG und TFG.

- Arbeitszeitdaten in Systemen, mit denen für Abrechnungszwecke oder Zwecke der Geräteüberwachung der Arbeitsaufwand bestimmter Vorgänge erfasst wird (System für die Verwaltung von technischem Anlagengut und Facility Management)
Zweck und Rechtsgrundlage: Einhaltung aller notwendigen gesetzlichen Vorgaben für Anlagen und Geräte, z.B. Betriebssicherheitsverordnung § 4 Abs. 1-4, TRBS spezifische Regeln für Arbeitsmittel überwachungsbedürftiger Anlagen, ASR Technische Regeln für Arbeitsstätten, AMWHV §12GMP, Laborrichtlinie.
- Installationsdaten in persönlich zugeordneten mobilen elektronischen Geräten (Mobile Device Management)
Zweck: Zur Sicherstellung, dass nur geprüfte sichere Anwendungen laufen und Gewährleistung einer sicheren Kommunikation.
Rechtsgrundlage: Abwicklung des Beschäftigungsverhältnisses: Soweit die Mitarbeiter mobile Endgeräte für ihre berufliche Tätigkeit vom DRK-BSD bekommen, ist die Kontrolle und Verwaltung der installierten Anwendungen gemäß Zweckbestimmung zur Sicherstellung der Einhaltung vertraglicher Pflichten erforderlich.
- Dateieigenschaften von Office-Dateien: Diese sind zwar auch zu beachten, stehen aber unter alleiniger Kontrolle der Mitarbeiter. Personenbezogene Daten werden in Dateieigenschaften von Office-Dateien automatisiert abgelegt.
Außer der Angabe „zuletzt gespeichert von“ können vor einer Weitergabe einer Datei die personenbezogenen Angaben der Dateieigenschaften von jedem Mitarbeiter selbst gelöscht werden.
Zweck: Vom Hersteller der Office-Programme wird damit eine Rückverfolgbarkeit beabsichtigt, wer der Ersteller ist, auf welcher Vorlage das Dokument basiert, in welcher Organisation es erstellt wurde und wer es zuletzt geändert hat. Eine Rechtsgrundlage für die Notwendigkeit der Speicherung wird seitens des Arbeitgebers nicht festgelegt. Es besteht daher keine Verpflichtung, diese Daten vor Weiterleitung von Dateien gespeichert zu lassen.
Bei übernommenen und anschließend selbst weiterbearbeiteten Dateien sollen in eigener Verantwortung der Mitarbeiter nicht mehr korrekte Vorgängerangaben aus den Dateieigenschaften entfernt werden.

3. Wer bekommt meine Daten? (Kategorien von Empfängern der personenbezogenen Daten)

Die genannten Daten innerhalb der Personalabteilung:

Die Daten werden intern im Konzernverbund von den einzelnen Instituten an die zentrale Personalabteilung in Baden-Baden bzw. Dresden übermittelt und soweit lokal der Bedarf zur Einsicht oder Bearbeitung der Daten besteht auch zurück zum Personalbüro im jeweils verantwortlichen Institut (funktionell durch die gegenseitige Einrichtung der Zugriffsrechte). Die Einsichtnahme der Vorgesetzten in die Daten ist bei begründetem Anlass möglich. Ein Anlass mit klarem Bezug zur Zweckbestimmung, nämlich der Abwicklung des Beschäftigungsverhältnisses, muss dazu vom anfragenden direkten Vorgesetzten der Personalabteilung angegeben werden.

Dies gilt gleichermaßen auch für die Tochtergesellschaften BSD Nord-Ost, IKT Ulm, IKTZ Heidelberg, ZKT Tübingen, MVZ Frankfurt, MVZ Ulm, ZIT Hamburg und ZTB Berlin, deren Mitarbeiterdaten ebenso an die zentrale Abteilung der Muttergesellschaft zur Verwaltung und Verarbeitung übermittelt werden und zur Einsicht oder Bearbeitung der Daten parallel dazu lokal im Personalbüro der einzelnen Tochtergesellschaft zur Verfügung stehen.

Externe Lohn- und Gehaltsabrechnung

Eine externe Datenübermittlung findet zum Zweck der Abwicklung der Lohn- und Gehaltszahlungen, sowie Verrechnung und Abführung der Lohnsteuer- Sozialversicherungsbeiträge statt. Auftragnehmer für diese Abwicklung ist die Firma P&I Personal & Informatik AG, Kreuzberger Ring 56, 65205 Wiesbaden. Mit der Firma P&I wurde ein Vertrag zur Auftragsdatenverarbeitung nach den gesetzlichen Vorgaben abgeschlossen und die Firma sowie deren Mitarbeiter auf die Einhaltung der Vertraulichkeit und Privatgeheimnisse der Mitarbeiterdaten und auf die Einhaltung der notwendigen Sicherheitsmaßnahmen nach dem geltenden Stand der Technik verpflichtet.

Kontaktdaten des Datenschutzbeauftragten der Firma P&I:

E-Mail: Datenschutzbeauftragter@pi-ag.com

Weitere externe Datenübermittlungen finden nur auf der Grundlage geltender Gesetze statt. Das sind in der Regel die Übermittlungen an Finanzämter, die Sozialversicherung und gesetzliche Krankenversicherungen. An diese werden im Rahmen der Abrechnungen, auch über den Auftragnehmer, die Firma P&I Daten, übermittelt. Weitere Datenübermittlungen können bei gegebenem Anlass an die Berufsgenossenschaft erfolgen und in anonymisierter Form an statistische Landesämter.

Nur in Ausnahmefällen können Übermittlungen an Ermittlungs- und Strafverfolgungsbehörden erforderlich werden, wenn diese mit hinreichender Begründung auf der Basis der entsprechenden gesetzlichen Grundlagen Daten anfordern.

Datenübermittlungen für die Vorbereitung von Wahlen

Zur Vorbereitung der Betriebsratswahlen und der Arbeitnehmervertretung im Aufsichtsrat ist der Arbeitgeber gemäß § 24 Abs. 1 und 2 WahlO BetrVG verpflichtet, die privaten Adressen aller wahlberechtigten Mitarbeiterinnen und Mitarbeitern dem Wahlvorstand der Betriebsratswahlen zu übermitteln. Auch die privaten Adressen von Mitarbeiterinnen und Mitarbeitern sind personenbezogene Daten und unterliegen den Bestimmungen des Datenschutzes. Der Zweck dieser Datenverarbeitung beim Wahlvorstand ist die Schaffung der Möglichkeit, bei Anfragen zur Ausübung der Briefwahl umgehend die Unterlagen verschicken zu können.

Das Geschlecht ist aufgrund § 15 Abs. 2 Betriebsverfassungsgesetz (BetrVG) zu übermitteln. Danach muss das Geschlecht, das in der Belegschaft in der Minderheit ist, entsprechend seines zahlenmäßigen Verhältnisses im Betriebsrat vertreten sein, wenn dieser aus mindestens drei Mitgliedern besteht. Die Wählerliste muss nach § 2 Abs.1 der oben genannten Wahlordnung auch das Geburtsdatum enthalten. Eintrittsdatum und Austrittsdatum sind zusätzlich zur Feststellung der Wahlberechtigung erforderlich. Alle diese Angaben der Rechtsgrundlage nach dem BetrVG gelten in Verbindung mit dem § 26 des Bundesdatenschutzgesetzes.

Eine Einwilligung der Mitarbeiter in die Übermittlung dieser Daten an den Wahlvorstand ist aufgrund der genannten gesetzlichen Verpflichtungen nicht einzuholen. Die Herkunft der Daten, die der Wahlvorstand verarbeitet, ist von der für Sie zuständigen Personalabteilung. Dort sind die Daten gespeichert, die Sie dem Arbeitgeber selbst zur Verfügung gestellt hatten. Der Wahlvorstand verarbeitet die Daten nach der Übermittlung durch die Personalabteilung.

Mit den genannten gesetzlichen Grundlagen fällt diese Übermittlung auch unter den Zweck der Durchführung Ihres Beschäftigungsverhältnisses. Zugriffsrechte für die Daten werden nur den Mitgliedern des Wahlvorstandes eingeräumt, die für den Versand der Betriebsrats-Wahlunterlagen im Falle Ihres entsprechenden Antrags zuständig sind. Eine anderweitige Weitergabe durch den Wahlvorstand erfolgt nicht. Die ausschließliche Verwendung für die genannten Zwecke wird Ihnen bei jeder Betriebsratswahl vom Wahlvorstand zugesichert.

Die übermittelten Daten umfassen folgende Angaben

- Name, Vorname, Titel
- Geschlecht
- Geburtsdatum
- Private Postadresse
- Eintrittsdatum in das Unternehmen
- Ggf. Austrittsdatum aus dem Unternehmen

Zusätzlich für die Wahlberechtigten, denen der Wahlvorstand nach § 3 Abs. 4 WO i.V.m. § 24 Abs. 2 WO das Wahlausschreiben zusenden muss:

- Namen und Kontaktdaten der Wahlberechtigten, die aufgrund der Eigenart ihres Beschäftigungsverhältnisses (z. B. Außendienst) voraussichtlich nicht am Wahltag im Betrieb sein werden
- Namen und Kontaktdaten der Wahlberechtigten, die aus sonstigen Gründen (z. B. längerer Arbeitsunfähigkeit, Elternzeit...) vom Zeitpunkt des Erlasses des Wahlausschreibens bis zum Wahltag voraussichtlich nicht im Betrieb sein werden.

Datenübermittlungen an den Betriebsrat

Weitere personenbezogene Daten werden in Einzelfällen an den Betriebsrat übermittelt, bei denen der Betriebsrat ein Mitbestimmungsrecht oder Anhörungsrecht hat. Diese Übermittlungen erfolgen auf der rechtlichen Grundlage des Betriebsverfassungsgesetzes. Dazu zählen zum Beispiel die Planung von internen Versetzungen, Arbeitseinsätze mit besonderen Anforderungen, die vorübergehend zu einer Ansammlung von Überstunden führen und dazu zählen die Aufgaben der speziellen Arbeitsgruppen mit Beteiligung des Betriebsrates wie Behindertenvertretung und Jugendvertretung, soweit jeweils im Institut vorhanden. Zugriffe auf Daten dieser Vertretungen sind grundsätzlich genau auf die zugehörigen Mitglieder begrenzt. Andere Betriebsratsmitglieder bekommen keinen Zugriff auf Daten dieser Vertretungen.

So wie alle Mitarbeiter des Unternehmens sind auch die Mitglieder des Betriebsrates und des Wahlvorstandes auf die Einhaltung der Datenschutzbestimmungen verpflichtet worden. Sie unterliegen zusätzlich einer gesetzlichen Verschwiegenheitspflicht.

Die Aufbewahrung der personenbezogenen Daten erfolgt beim Betriebsrat in Akten auf Papier. Diese werden mit geregelten Zugriffsrechten unter sicherem Verschluss gelagert. Darüber hinaus liegen Daten in Office-Dokumenten (E-Mail, Word-Dateien und Dateien im Tabellenformat) gespeichert vor. Die Dateiverzeichnisse der Betriebsräte aller Institute

unterliegen den begrenzten Zugriffsrechten ausschließlich für die Betriebsratsmitglieder. Die eingeführten Sicherheitsmaßnahmen des Unternehmens für die IT-Infrastruktur wirken sich voll auch auf die Sicherheit der Speicherbereiche der Betriebsräte aus.

Datenübermittlungen im Rahmen von Revisionsprüfungen

Rechtsgrundlage der Übermittlungen ist der Vertrag von TASCO mit dem DRK Blutspendedienst über die revisorische Betreuung abgeschlossen. TASCO nimmt die ausgelagerten Revisionsaufgaben für den BSD wahr. Rechtsgrundlage für die Einbeziehung personenbezogener Daten von Mitarbeitenden daher Art. 6 Abs. 1 lit. b DSGVO in Bezug auf den Arbeitsvertrag. Die Auslagerung erfolgt im Rahmen einer Beauftragung, bei der die Verantwortung für die Datenverarbeitung beim DRK Blutspendedienst verbleibt.

Die Revision übernimmt klassischerweise Kontroll- und Überwachungstätigkeiten im Unternehmen. Rechtsgrundlage hierfür ist auch die Wahrung berechtigter Interessen des BSD nach Art. 6 Abs. 1 lit. f DSGVO. Unterliegen nun Beschäftigtendaten einer Prüfung gilt als Rechtsgrundlage für die Kontroll- und Überwachungstätigkeit der Internen Revision Art. 6 Abs. 1 lit. f DSGVO i.V.m. § 26 BDSG.

Falls der Verdacht einer dolosen Handlung festgestellt wird, müssen personenbezogene Daten zur Sachverhaltsaufklärung genutzt und als Prüfungsergebnis personenbezogene Aussagen getroffen werden. Die Rechtsgrundlage bei internen Sachverhaltsaufklärungen bzw. internen Ermittlungen ergeben sich vor allem aus der DSGVO, dem BDSG (§ 26 Abs. 1 Satz 2) und der Rechtsprechung des Bundesarbeitsgerichts.

Aufbewahrungsfristen bei der Firma Tasco: Revisionsunterlagen (Arbeitspapiere etc.) werden gemäß dem Handbuch der Tasco für sechs Jahre archiviert und anschließend ordnungsgemäß vernichtet. Diese Regelung gilt für Papier und digitale Unterlagen.

Die genannten Daten, die außerhalb der Personalabteilung erfasst werden:

Diese werden ausschließlich in der jeweiligen Fachabteilung gespeichert und verarbeitet. Genaue Angaben dazu finden Sie zu jedem einzelnen Verfahren im Datenschutz-Verzeichnis der Verarbeitungstätigkeiten. Dieses Verzeichnis steht den Mitarbeitern im Intranet zur Verfügung.

Letzterer Absatz zuvor in Bezug auf Übermittlungen an Ermittlungs- und Strafverfolgungsbehörden gilt in Ausnahmefällen auch für Bewegungsdaten des Zutrittskontrollsystems und im Falle eines Diebstahls eines mobilen Gerätes für Daten des Mobile Device Managementsystems.

Benutzerdaten, Berechtigungsdaten und mitarbeiterbezogene Datensatzkennungen können gegebenenfalls bei behördlichen Prüfungen der Arzneimittelüberwachung und bei Auditierungen vor Ort eingesehen werden.

Daten im Rahmen von Meldungen nach dem Hinweisgeberschutzgesetz (HinSchG):

Personenbezogene Daten, die im Rahmen einer Meldung gemäß HinSchG an die externe Meldestelle gegeben werden, müssen nach Prüfung, außer bei Ablehnung einer Meldung durch die externe Stelle, an den Arbeitgeber zur weiteren Bearbeitung übermittelt werden.

- **Daten der meldenden Person:**
Meldungen können anonym erfolgen, sie können mit Angabe des Namens erfolgen, aber mit dem Wunsch, dass der Name dem Arbeitgeber nicht offenbart wird, oder auf freiwilliger Basis kann der Weiterleitung an den Arbeitgeber zugestimmt werden. Im letzteren Fall werden nur Personen des Arbeitgebers die Identität des Meldenden erfahren, die mit der Aufarbeitung des Falls betraut werden und für die es wichtig ist, die Identität zu erfahren, um mit der meldenden Person selbst ein Gespräch führen zu können. Die gemeldete Person erfährt nicht die Identität des Meldenden. Die beteiligten Personen werden sensibilisiert, auch darauf zu achten, auf welchen Informationen Rückschlüsse auf die meldende Person möglich sind.
- **Daten der gemeldeten Person:**
Die Identität der gemeldeten Person muss dem Arbeitgeber preisgegeben werden, da eine berechtigte Meldung nur dann von der externen Meldestelle weitergegeben wird, wenn ein Gesetzesverstoß im Unternehmen gemeldet wird. Der Personenkreis, der die Identität erfährt, wird so klein wie möglich gehalten und auf das notwendige Minimum begrenzt, um den Fall bearbeiten bzw. ein Ermittlungsverfahren einleiten zu können. Eine Weiterleitung an Ermittlungsbehörden wird erfolgen, wenn klare Nachweise für einen Gesetzesverstoß vorliegen. Die gemeldete Person wird sobald wie möglich über die Meldung des Falls und den Vorwurf ihr gegenüber in Kenntnis gesetzt. Wenn durch diese Information das Ermittlungsverfahren beeinträchtigt werden könnte, erfolgt sie vorübergehend jedoch noch nicht, solange bis diese Beeinträchtigung nicht mehr zu befürchten ist.
- Es handelt sich bei Meldungen nach dem HinSchG niemals um einen Routinevorgang, sondern immer um Einzelfälle. Deshalb kann kein Standardablauf in allen Punkten festgelegt werden. Eine datenschutzgerechte Vorgehensweise im Einzelfall wird durch entsprechende Sensibilisierung der jeweils eingebundenen Personen erreicht.

4. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Datenübermittlungen von Beschäftigendaten in andere Staaten finden nicht statt.

5. Wie lange werden meine Daten gespeichert?

Die Beschäftigendaten von Mitarbeitern werden über die Dauer des Beschäftigungsverhältnisses aufbewahrt. Bei bestimmten Sonderfällen wie Abmahnungen, bestehen kürzere Löschrufen, sofern der Zweck der Erhebung entfällt. Sollten Sie davon betroffen sein, wenden sie sich bitte an Ihre zuständige Personalabteilung. Für bestimmte Daten ist anschließend im Rahmen bestimmter Gesetze noch eine weitere Archivierung erforderlich:

- Die steuerrelevanten Daten werden bis zum Ende des 10. Jahres nach Beendigung des Beschäftigungsverhältnisses aufbewahrt.
- Bei Daten zu eventuellen gesundheitlichen Belastungen am Arbeitsplatz, gelten längere Aufbewahrungsvorschriften nach den jeweiligen einzelnen relevanten Rechtsvorschriften.

Personalakten in Papierform werden, soweit sie nicht zum Nachweis für Steuer- und Sozialversicherungsbehörden bzw. der betrieblichen Altersversorgung benötigt werden, bis zu 5 Jahre nach Beendigung des Arbeitsverhältnisses, längstens bis zur Beendigung eventueller Rechtsstreitigkeiten aus Anlass der Beendigung des Arbeitsverhältnisses aufbewahrt und danach vernichtet.

Die Daten, die nicht zu den Personaldaten zählen (oben genannte Datenarten Außerhalb der Personalabteilung) werden nach den jeweils zugrundeliegenden Rechtsvorschriften aufbewahrt und die detaillierten Angaben dazu werden im Datenschutz-Verzeichnis der Verarbeitungstätigkeiten zu den einzelnen Verfahren dokumentiert. Dieses Verzeichnis steht den Mitarbeitern im Intranet zur Verfügung.

Dauer der Datenspeicherung für Wahlen:

Die Daten werden zu Beginn der Planung der Betriebsratswahl oder der Arbeitnehmervertretung im Aufsichtsrat an den Wahlvorstand übermittelt und bei diesem über die gesamte Dauer der Abwicklung der Wahl gespeichert.

Nach Beendigung der Frist zur Anfechtung der Betriebsratswahl erfolgt die Löschung der Privatadressen auf den Verzeichnissen des Wahlvorstandes bzw. des Betriebsrates soweit die Daten auf diesen übergegangen sind. Diese Frist beträgt zwei Wochen, beginnend mit dem Tag nach Veröffentlichung des Wahlergebnisses.

Alle anderen Angaben auf den Wählerlisten werden mit den Wahlunterlagen für die Dauer des Bestehens des gewählten Gremiums (Betriebsrat, Aufsichtsrat) aufbewahrt. Das sind für den Betriebsrat vier Jahre bis zur nächsten Betriebsratswahl und mind. für die Dauer von fünf Jahren bei Aufsichtsratswahlen. Diese Aufbewahrung erfolgt in schriftlichen Unterlagen, nicht digital.

Im Falle der Übermittlung von Dateien von der Personalabteilung per interner E-Mail wird die Dateianlage in der E-Mail unmittelbar nach der Übernahme aus der E-Mail auf dem Netzwerkverzeichnis des Betriebsrates gelöscht.

Dauer der Datenspeicherung für andere Daten beim Betriebsrat:

Soweit keine kürzere Aufbewahrungsdauer vorgeschrieben ist, archiviert der Betriebsrat alle Daten über die Dauer bis zur nächsten Betriebsratswahl. Eine kürzere Dauer gilt einzelfallbezogen für Daten, die zu einem bestimmten Zweck über einzelne Mitarbeitende an den Betriebsrat übermittelt werden. Diese werden gelöscht, wenn der jeweilige Vorgang beendet ist.

6. Welche Datenschutzrechte habe ich?

Sie haben jederzeit ein Recht auf Auskunft über die bei uns über Sie gespeicherten personenbezogenen Daten. Sie können auf Antrag eine Kopie der personenbezogenen Daten über Ihre Person bekommen, die aktuell Gegenstand der Verarbeitung sind.

Eine solche Auskunftsanfrage sollten Sie jedoch nicht häufiger als höchstens einmal pro Jahr stellen, da auch die DS-GVO die Erteilung einer kostenfreien Auskunft auf Anfrage nur einmal pro Jahr vorschreibt.

Archivierte Unterlagen, die nicht mehr in den aktiven Datensätzen oder Personalakten vorliegen, können für die Auskunftserteilung nicht berücksichtigt werden, sind allerdings auch dem normalen Zugriff der Personalabteilung entzogen.

Für die Datenarten, die oben als „Innerhalb der Personalabteilung“ gekennzeichnet sind, richten Sie bitte Ihr Auskunftersuchen entweder an die Personalabteilung ihres Institutes oder Ihrer Tochtergesellschaft oder an die Personalabteilung des DRK-Blutspendedienstes gemäß Angaben im Kapitel 1.

Für die Datenarten, die oben als „Außerhalb der Personalabteilung“ gekennzeichnet sind, wenden Sie sich bitte möglichst direkt an die zuständige Fachabteilung. Bei Unklarheit in Bezug auf die Zuständigkeit können Sie sich auch dafür an die Personalabteilung wenden.

Für Daten, die beim Betriebsrat gespeichert oder in Aktenordnern abgelegt sind, wenden Sie sich bitte an das Betriebsratsbüro Ihres Institutes oder die intern kommunizierte E-Mailadresse Ihres Betriebsrates.

7. Umfang Ihres Widerspruchsrechts gegen die Verarbeitung personenbezogener Daten und Ihres Rechts auf Berichtigung oder Löschung

Das Widerspruchsrecht und das Recht auf Berichtigung oder Löschung gelten im Allgemeinen für gespeicherte personenbezogene Daten, aber mit der Ausnahme, wenn ein Gesetz die Speicherung und Aufbewahrung vorschreibt und solange die Speicherung im Rahmen eines Vertragsverhältnisses erforderlich ist.

Das Recht auf Berichtigung gilt grundsätzlich für Fehler in Adressdaten, Namen oder Daten der absolvierten Aus- und Weiterbildung. Sie haben auch das Recht, Ergänzungen zu verlangen, wenn Ihre Namens- oder Adressangaben unvollständig sind. Die Richtigkeit der verlangten Änderungen muss vom Betroffenen nachgewiesen werden.

Sie können die Löschung von Teilen der gespeicherten Daten verlangen, wenn Sie der Ansicht sind, dass diese nicht mehr für die Abwicklung des Beschäftigungsverhältnisses erforderlich sind. Wenn der Arbeitgeber der Ansicht ist, dass diese Daten weiterhin gespeichert bleiben müssen, wird er Ihnen dann die Rechtsgrundlage erläutern, aufgrund derer er die Fortführung der Speicherung dieser Daten anstrebt. Das kann zum Beispiel ein berechtigtes Interesse des Arbeitgebers sein, wenn er darlegen kann, dass dadurch und durch den guten Schutz Ihrer Daten Ihre Persönlichkeitsrechte nicht beeinträchtigt werden. Für eine Einigung ist im Zweifelsfall der Betriebsrat in das Gespräch einzubeziehen.

8. Recht auf Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit zu einem anderen Arbeitgeber kann Ihnen durch Übergabe einer Datei mit Ihren bei uns gespeicherten Identifikations-, Kontakt- sowie Aus- und Weiterbildungsdaten (soweit diese elektronisch gespeichert sind) in Form einer pdf-Datei, einer Textdatei oder in einem gängigen Office-Dateiformat gewährt werden.

9. Einwilligung und Widerrufsrecht

Sollte eine Datenerfassung oder Datenverwendung auf der Basis Ihrer Einwilligung erforderlich werden, zum Beispiel zur Veröffentlichung Ihres Bildes im Internet, dann ist diese Einwilligung grundsätzlich freiwillig. Für Bilder gilt Letzteres jedoch nicht, wenn die Veröffentlichung, zum Beispiel für Tätigkeiten im Außendienst, bereits im Arbeitsvertrag vereinbart wurde. Die Ablehnung einer freiwilligen Einwilligung hat für Sie keine Nachteile. Sie werden im Einzelfall vor Einholung der Einwilligung darüber aufgeklärt.

Wenn Sie zur Erfassung oder Verwendung bestimmter Daten oder von Bildern eine Einwilligung erteilt haben, dann gilt ein uneingeschränktes Widerrufsrecht. Dieses richtet sich gegen jede weitere Verwendung der Daten oder Bilder in einem neuen Vorgang. Unter der Voraussetzung, dass die Löschung keinen unangemessenen Aufwand verursacht, werden nach Eingang Ihres Widerrufs die betroffenen Daten oder Bilder auch in der bereits bestehenden Speicherung oder Anwendung gelöscht.

Die Neuauflage einer bereits bestehenden Druckschrift wäre zum Beispiel mit einem unangemessenen Mehraufwand verbunden. In diesem Fall kann sich der Widerruf nur gegen die erneute Verwendung für die nächste Auflage auswirken.

10. Beschwerderecht bei der Aufsichtsbehörde

Sollten Sie sich trotz aller unserer Bemühungen um eine gute Information und die vertrauliche Behandlung aller Ihrer personenbezogenen Daten bei der Datenschutzaufsichtsbehörde beschweren wollen, dann ist das Ihr gutes Recht und Sie können sich direkt an die zuständige Datenschutzaufsichtsbehörde des Bundeslandes des Unternehmenssitzes Ihres Arbeitgebers wenden.

Die Adressen der Aufsichtsbehörden der Bundesländer finden Sie unter:

<https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html>

Zuständig sind die Behörden der folgenden Bundesländer:

Für die Institute, Blutspendezentralen und Tochtergesellschaften:	Unternehmenssitz und zuständige Aufsichtsbehörde in:
Mannheim, Baden-Baden, Frankfurt am Main, Kassel, Mannheim und Ulm	Baden-Württemberg
Medizinisches Versorgungszentrum in Frankfurt am Main	Hessen
Zentralinstitut für Transfusionsmedizin in Hamburg	Hamburg
Dresden, Berlin, Chemnitz, Cottbus, Dresden, Görlitz, Leipzig, Lütjensee, Neuruppin, Plauen, Schleswig, Potsdam und Zwickau	Sachsen
ZTB Zentrum für Transfusionsmedizin und Zelltherapie Berlin	Berlin

11. Besteht für mich eine Pflicht zur Bereitstellung von Daten?

Bereits im Bewerbungsverfahren war es erforderlich, uns alle die personenbezogenen Daten zur Verfügung zu stellen, die wir für die Begründung des Beschäftigungsverhältnisses benötigten. Diese wurden in die Personaldaten übernommen und deren Verfügbarkeit ist dort weiterhin erforderlich. Bei der Einstellung als Mitarbeiter bei uns sind Sie vertraglich und

gesetzlich verpflichtet weitere Daten anzugeben, die für die Abwicklung des Beschäftigungsverhältnisses sowie die steuerrechtlichen und sozialversicherungsrechtlichen Belange vorliegen müssen. Zusätzlich können für spezielle Tätigkeiten bestimmte Eignungsangaben erforderlich sein, bevor solche Tätigkeiten ausgeführt werden dürfen. Die Information dazu erhalten Sie dann im Einzelfall.

Während des Beschäftigungsverhältnisses besteht für Sie die vertragliche Verpflichtung, uns jede Änderung Ihrer Kontaktdaten, Namensangaben, Kontoverbindung und des Familienstandes mitzuteilen. Eine Nichtbereitstellung kann die Abwicklung des Beschäftigungsverhältnisses erheblich behindern und zu Fehlern in steuerlichen sowie sozialversicherungsrechtlichen Mitteilungen und Berechnungen führen.

Sie sind weiterhin verpflichtet, uns die Teilnahmebescheinigungen oder Zertifikate von Weiterbildungen vorzulegen, die für Ihre Tätigkeit bei uns von Relevanz sind. Eine Nichtvorlage kann Nachteile für Ihren weiteren beruflichen Werdegang haben.

12. Inwieweit werden meine Daten für die Profilbildung (Scoring) genutzt?

Automatisierte Entscheidungen gemäß Art. 22 DSGVO oder andere Profiling-Maßnahmen nach Art. 4 Nr. DSGVO finden nicht statt.

Anlage A - DRK-Blutspendedienst Baden- Württemberg – Hessen gGmbH

Institut für Transfusionsmedizin und Immunologie Mannheim

Adresse: Friedrich-Ebert-Straße 107, 68167 Mannheim
Telefonnummer: +49 621 3706-8944
E-Mailadresse: karriere-man@blutspende.de

Institut für Transfusionsmedizin und Immunhämatologie Frankfurt am Main

Adresse: Sandhofstraße 1, 60528 Frankfurt
Telefonnummer: +49 69 6782 107
E-Mailadresse: karriere-ffm@blutspende.de

Institut für Transfusionsmedizin und Immunologie Kassel

Adresse: Mönchebergstraße 57, 34125 Kassel
Telefonnummer: +49 561 8793 101
E-Mailadresse: karriere-kas@blutspende.de

Institut für Transfusionsmedizin und Immunhämatologie Baden-Baden

Adresse: Gunzenbachstraße 35, 76530 Baden-Baden
Telefonnummer: +49 72 2121 4218
E-Mailadresse: karriere-bad@blutspende.de

Institut für Klinische Transfusionsmedizin und Immungenetik Ulm (IKT) gGmbH

Adresse: Helmholtzstraße 10, 89081 Ulm
Telefonnummer: +49 731 150-554
E-Mailadresse: karriere-ulm@blutspende.de

Institut für Klinische Transfusionsmedizin und Zelltherapie Heidelberg (IKTZ) gGmbH

Adresse: Im Neuenheimer Feld 583, 69120 Heidelberg
Telefonnummer: +49 621 3706 8944
E-Mailadresse: karriere-man@blutspende.de

Zentralinstitut für Transfusionsmedizin Hamburg (ZIT) gGmbH

Adresse: Eilbektal 111, 22089 Hamburg
Telefonnummer: +49 72 2121 4218
E-Mailadresse: karriere-bad@blutspende.de

Zentrum für Klinische Transfusionsmedizin Tübingen (ZKT) gGmbH

Adresse: Otfried-Müller-Straße 4/1, 72076 Tübingen
Telefonnummer: +49 707 1298 1632
E-Mailadresse: karriere-zkt@blutspende.de

Medizinisches Versorgungszentrum, DRK Blutspendedienst Frankfurt am Main gGmbH

Adresse: Sandhofstraße 1, 60528 Frankfurt
Telefonnummer: +49 69 6782 107
E-Mailadresse: karriere-ffm@blutspende.de

Medizinisches Versorgungszentrum, DRK Blutspendedienst Ulm gGmbH

Adresse: Helmholtzstraße 10, 89081 Ulm
Telefonnummer: +49 731 150-554
E-Mailadresse: karriere-ulm@blutspende.de

Medizinisches Versorgungszentrum Dr. Becker gGmbH

Adresse: Staufener Str. 18, 79189 Bad-Krozingen
Telefonnummer: +49 72 2121 4218
E-Mailadresse: karriere@becker-klinik.de

Klinik Dr. Becker gGmbH

Adresse: Staufener Straße 18, 79189 Bad-Krozingen
Telefonnummer: +49 72 2121 4218
E-Mailadresse: karriere@becker-klinik.de

Anlage B – DRK-Blutspendedienst Nord-Ost gGmbH

Institut für Transfusionsmedizin Dresden

Adresse: Blasewitzer Straße 68 / 70, 01307 Dresden
Telefonnummer: +49 351 4450 800
E-Mailadresse: personal@blutspende.de

Institut für Transfusionsmedizin Berlin

Adresse: Hindenburgdamm 30 A 12203 Berlin
Telefonnummer: +49 30 8068 10
E-Mailadresse: personal@blutspende.de

Institut für Transfusionsmedizin Chemnitz

Adresse: Zeisigwaldstraße 103, 09130 Chemnitz
Telefonnummer: +49 371 4322 00
E-Mailadresse: personal@blutspende.de

Institut für Transfusionsmedizin Cottbus

Adresse: Thiemstraße 105, 03050 Cottbus
Telefonnummer: +49 355 4995 0
E-Mailadresse: personal@blutspende.de

Institut für Transfusionsmedizin Lütjensee

Adresse: Hamburger Str. 24, 22952 Lütjensee
Telefonnummer: +49 4154 8073 0
E-Mailadresse: personal@blutspende.de

Institut für Transfusionsmedizin Plauen

Adresse: Röntgenstraße 2a, 08529 Plauen
Telefonnummer: +49 3741 4070
E-Mailadresse: personal@blutspende.de

Institut für Transfusionsmedizin Potsdam

Adresse: Charlottenstr. 72, Haus I, 14467 Potsdam
Telefonnummer: +49 331 2846 0
E-Mailadresse: personal@blutspende.de

Institut für Transfusionsmedizin Schleswig

Adresse: Rote-Kreuz-Weg 5, 24837 Schleswig
Telefonnummer: +49 4621 9674 0
E-Mailadresse: personal@blutspende.de

Blutspendezentrum Leipzig

Adresse: Prager Str. 13, 04103 Leipzig
Telefonnummer: +49 341 2535 4410
E-Mailadresse: personal@blutspende.de

Blutspendezentrum Görlitz

Adresse: Zeppelinstraße 43, 02828 Görlitz
Telefonnummer: +49 3581 32115 0
E-Mailadresse: personal@blutspende.de

Blutspendezentrum Neuruppin

Adresse: Fehrbelliner Straße 38, 16816 Neuruppin
Telefonnummer: +49 30 8068 10
E-Mailadresse: personal@blutspende.de

Plasmaspendezentrum Zwickau

Adresse: Äußere Schneeberger Str. 100, 08056 Zwickau
Telefonnummer: +49 375 2769 2622 0
E-Mailadresse: personal@blutspende.de

ZTB Zentrum für Transfusionsmedizin und Zelltherapie Berlin gGmbH

Adresse: Hindenburgdamm 30 A, 12203 Berlin
Telefonnummer: +49 30 8068 10
E-Mailadresse: personal@blutspende.de