Merkblatt zum Datenschutz beim Bundesverband Öffentlicher Banken Deutschlands, VÖB, e.V.

Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinen Persönlichkeitsrechten beeinträchtigt wird. Der Schutz von personenbezogenen Daten und die Wahrung der Privatsphäre unserer Mitarbeiter* und Geschäftspartner ist für den Bundesverband Öffentlicher Banken Deutschlands, VÖB, e.V. (nachfolgend: VÖB) von höchster Bedeutung. Wir erwarten daher von unseren Mitarbeitern einen verantwortungsvollen Umgang mit personenbezogenen Daten und die Einhaltung sämtlicher diesbezüglicher Vorschriften. Jeder Mitarbeiter, der regelmäßig im Rahmen seiner Tätigkeit mit personenbezogenen Daten in Verbindung kommt, wird deshalb vom VÖB verpflichtet, die datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG) einzuhalten. Im Folgenden geben wir Ihnen einen Überblick über die wesentlichen Prinzipien und Anforderungen des Datenschutzes.

1. Schutzgegenstand personenbezogene Daten

Schutzgegenstand der datenschutzrechtlichen Vorschriften sind nur **personenbezogene Daten** gemäß Art. 4 Nr. 1 der Datenschutz-Grundverordnung (DS-GVO). Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zur Anerkennung wie einem Namen, zu einer Kennnummer, Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen, die aus der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (z.B. Angaben wie Name, Anschrift, E-Mail-Adresse, Telefonnummer usw.), aber auch Geburtsdatum und -ort, Arbeitgeber, Beruf, Familienstand, Kinder, Grad der Behinderung, Gehalt, Vermögen, Steuerklasse, Krankenkasse, Schulabschluss, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse, Fotos, Hobbys, Interessen u.v.m. Auch Daten ohne unmittelbaren Personenbezug können personenbezogene Daten sein, wenn daraus auf eine bestimmte Person geschlossen werden kann (z.B. interne Personalnummer, PC-Login Daten, IP-Adressen oder ggf. KFZ-Kennzeichen). Betroffene sind insbesondere die Mitarbeiter und Geschäftspartner des VÖB.

Die Verarbeitung **besonderer Kategorien personenbezogener Daten,** aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, ist grundsätzlich untersagt, wenn nicht ein Ausnahmetatbestand nach Art. 9 Abs. 2 DS-GVO vorliegt. Solche Angaben sind besonders vertraulich zu behandeln.

2. Verarbeitung personenbezogener Daten

Die Vorschriften zum Datenschutz müssen bei jeder **Verarbeitung** von personenbezogenen Daten beachtet werden. Verarbeitung ist gem. Art. 4 Nr. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Erheben ist das Beschaffen von Daten über den Betroffenen. Es ist Voraussetzung für die nachfolgende Verarbeitung oder Nutzung. Bei jeder Erhebung ist der Verarbeitungs- oder Nutzungszweck festzulegen. Grundsätzlich sind die Daten beim Betroffenen zu erheben und eine Datenerhebung auf Vorrat, also für im Zeitpunkt der Erhebung noch nicht feststehende Zwecke, ist unzulässig gleichgültig, ob die Daten mündlich oder schriftlich beschafft werden, ob der Betroffene selbst befragt wird oder die Daten beibringen soll oder ob Dritte befragt oder Unterlagen von der speichernden Stelle eingesehen werden.

Ein **Speichern** liegt vor, wenn von dem VÖB als „Verantwortlicher" erhobene oder ihm sonst bekannte Informationen reproduzierbar fixiert werden oder wenn von anderer Seite, z. B. dem Betroffenen oder einem Dritten, der die Daten übermittelt hat, die Daten bereits auf einem Datenträger zur Verfügung gestellt wurden und nunmehr vom VÖB weiter vorrätig gehalten werden. **Verändern** von Daten ist jede inhaltliche Umgestaltung von gespeicherten Daten dergestalt, dass sich der Informationswert ändert. Dies kann auch durch das Verknüpfen von Daten aus verschiedenen Dateien geschehen, wenn durch den neuen Kontext ein neuer Informationsgehalt entsteht. **Übermitteln** ist das Bekanntgeben personenbezogener Daten an

* Soweit in diesem Merkblatt Begriffe – insbesondere Mitarbeiter etc. – in ihrem männlichen Genus verwendet werden, geschieht dies nur zum Zwecke der leichteren Lesbarkeit dieses Merkblatts und erfasst alle Geschlechter.

einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Dabei ist die intensivste Form der Übermittlung die Veröffentlichung. Keine Übermittlung liegt aber vor, wenn Daten nicht an einen Dritten, sondern an den Betroffenen, einen Auftragsdatenverarbeiter oder andere Mitarbeiter innerhalb des Verantwortlichen weitergegeben werden. Unter **Löschung** ist jede Form der Unkenntlichmachung der Daten zu verstehen. Dies ist in der Regel die physische Vernichtung. In jedem Fall müssen die Daten unlesbar geworden sein. Die Information darf dem Verantwortlichen nicht mehr zur Verfügung stehen.

Verwenden bzw. Nutzen ist als datenschutzrechtlicher Auffangtatbestand jeder Gebrauch des Informationsgehalts personenbezogener Daten für bestimmte Zwecke.

3. Grundsätze der Datenverarbeitung

Bei der Verarbeitung personenbezogener Daten sind die folgenden sechs Grundsätze zu beachten:

a) Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

b) Grundsatz der Zweckbindung
Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

c) Grundsatz der Datenminimierung
Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

d) Grundsatz der Richtigkeit
Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

e) Grundsatz der Speicherbegrenzung
Personenbezogene Daten müssen grundsätzlich in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

f) Grundsatz der Integrität und Vertraulichkeit
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

4. Rechtliche Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist gem. Art. 6 Abs. 1 S. 1 DS-GVO nur zulässig, wenn die DS-GVO, das BDSG oder eine andere Rechtsvorschrift (z.B. § 39b EStG, § 79 BetrVG, §§ 8 Abs. 1 Satz 2 ASiG, 203 Abs. 1 Nr. 1 StGB, die dem BDSG gem. § 1 Abs. 2 BDSG vorgehen) **dies erlaubt oder anordnet oder der Betroffene freiwillig und für den Einzelfall eingewilligt hat.** Die Einwilligung muss sich aber ausdrücklich auf diese Daten beziehen, also in besonderem Maße bestimmt sein. Für die Verarbeitung besonderer Kategorien von personenbezogenen Arten (s.o.) gelten besondere Erlaubnisnormen, die die Datenverarbeitung auch ohne Einwilligung erlauben (Art. 9 Abs. 2 DS-GVO).

Die DS-GVO, das BDSG und andere Rechtsvorschriften enthalten Erlaubnistatbestände, **bei deren Eingreifen eine Einwilligung des Betroffenen nicht erforderlich** ist, z.B. bei der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (§ 26 BDSG, gilt auch für die Verarbeitung besonderer Kategorien von personenbezogenen Arten). Soweit dies für die Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist, dürfen daher personenbezogene Daten von Beschäftigten (auch besonderer Kategorien) ohne vorherige Einwilligung der Beschäftigten verarbeitet werden. Diese Erlaubnistatbestände sind als Ausnahmevorschriften grundsätzlich eng auszulegen.

Eine **Einwilligung des Betroffenen** ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht (freiwillige Einwilligung). Der Betroffene ist hierzu auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung seiner Daten, sowie auf die Folgen einer Verweigerung der Einwilligung

hinzuweisen (informierte Einwilligung). Die Einwilligung ist eine vorherige Einverständniserklärung. Die datenschutzrechtliche Einwilligung muss als solche deutlich zu erkennen sein und bedarf daher einer besonderen Hervorhebung.

Die Daten müssen für die Zwecke, für die sie erhoben und verarbeitet werden, erforderlich sein und dürfen nur so lange gespeichert werden, wie es der Zweck, zu dem sie erhoben oder verarbeitet wurden, erfordert. Nicht mehr erforderliche Daten sind zu löschen, unrichtige Daten zu berichtigen. Nur in gesetzlich bestimmten Fällen oder mit Einwilligung des Betroffenen ist eine Verarbeitung zu anderen Zwecken zulässig.

Wenn weder eine Einwilligung vorliegt, noch ein Erlaubnistatbestand greift, ist die Verarbeitung personenbezogener Daten rechtswidrig und kann die Folgen nach sich ziehen, die unter Nr. 7 dargestellt sind!

5. Besondere Anforderungen an den Datenschutz und konkrete Verhaltensweisen für bestimmte Arbeitsplätze

Den Mitarbeitern ist es grundsätzlich untersagt, unbefugt personenbezogene Daten zu verarbeiten. Unbefugt handelt ein Mitarbeiter bereits, wenn die Verarbeitung zwar für den VÖB als „Verantwortlicher" zulässig ist, der Mitarbeiter persönlich aber die ihm intern zugewiesenen Zugriffsberechtigungen überschreitet. Mitarbeiter dürfen personenbezogene Daten nur im Einklang mit den Vorschriften der DS-GVO, des BDSG oder sonstigen Rechtsvorschriften zu dem zu ihrer jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck erheben, verarbeiten oder sonst nutzen. Die Verpflichtung, das Datengeheimnis zu wahren, besteht auch nach Beendigung der Tätigkeit fort.

Den **Personalsachbearbeitern** obliegen besondere Pflichten im Umgang mit den personenbezogenen Daten unserer Mitarbeiter (Mitarbeiterdaten). **Mitarbeiterdaten** sind teilweise besondere Kategorien personenbezogener Daten, für die wie beschrieben noch strengere Maßstäbe gelten als für sonstige personenbezogene Daten. Mitarbeiterdaten dürfen in aller Regel nicht an Dritte bekanntgegeben oder übertragen werden. Auch betriebsintern dürfen Mitarbeiterdaten ausschließlich an dazu berechtigten Mitarbeitern und in einem Umfang bekannt gegeben werden, der für die Erfüllung der konkreten Aufgaben notwendig ist. Mitarbeiterdaten sind besonders schutzbedürftig. Es ist deshalb erforderlich, dass Personalsachbearbeiter die Personalakten grundsätzlich verschlossen aufbewahren und nicht offen liegen lassen. Beim Verlassen des Arbeitsplatzes (auch kurzzeitig) sind Personalakten stets wieder zu verschließen und der benutzte Computer gegen Einsichtnahme durch andere zu sichern (Sperrfunktion von Microsoft Windows, Win+L). Elektronisch erfasste Mitarbeiterdaten sind ausschließlich in den dafür vorgesehenen, gesonderten Speicherplätzen zu speichern. Weiteres regeln die Anweisungen des VÖB zu den technischen und organisatorischen Maßnahmen für die interne Datenverarbeitung.

Insbesondere den **Mitarbeitern der Administration** aber auch den übrigen Mitarbeitern obliegen besondere Pflichten im Umgang mit den **personenbezogenen Daten unserer Geschäftspartner**. Diese dürfen lediglich anderen Mitarbeitern des VÖB bekannt gegeben werden, für deren Aufgaben diese relevant sind. Eine Bekanntgabe oder Übermittlung an Dritte ist grundsätzlich untersagt und bedarf der Prüfung im Einzelfall. Bei personenbezogenen Daten unserer Geschäftspartner ist insbesondere der jeweilige Zweck der Datenerhebung für die weitere Verarbeitung und Nutzung zu beachten. Der Zweck der Erhebung personenbezogener Daten unserer Geschäftspartner ist diesen jeweils zuvor bekannt zu geben. Der Grundsatz der Datenvermeidung und -sparsamkeit ist besonders gründlich zu bedenken. Ein rechtswidriger Umgang mit personenbezogenen Daten unserer Geschäftspartner kann zu einem besonderen Image-Schaden für den VÖB führen und erhebliche finanzielle Verluste nach sich ziehen, weshalb er in jedem Fall zu vermeiden ist.

6. Datensicherheit

Gemäß Art. 32 Abs. 1 lit. a) bis d) DS-GVO hat der Verantwortliche (hier: der VÖB) geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau (Datensicherheit) zu gewährleisten (Art. 32 Abs. 1 DS-GVO). Die Regelungen des Arbeitsvertrages, die jeweiligen Arbeitsanweisungen und der Richtlinien sind für die Gewährleistung der Datensicherheit unabdingbare Voraussetzung und daher jederzeit zu beachten.

7. Rechtsfolgen von Verstößen

Verstöße gegen datenschutzrechtliche Vorschriften können als **Ordnungswidrigkeit** oder **Straftat** verfolgt werden (z.B. Art. 83 Abs. 4 DS-GVO, §§ 42, 43 BDSG). Daneben können Sie als Mitarbeiter des VÖB bei einer unbefugten Verarbeitung von personenbezogenen Daten zum **Schadensersatz**, zur **Unterlassung**

und/oder zur **Beseitigung** verpflichtet sein. In der Verletzung datenschutzrechtlicher Pflichten (insbesondere der oben unter 5. genannten besonderen Pflichten) kann zudem eine Verletzung arbeitsvertraglicher Pflichten liegen, die **arbeitsrechtliche Sanktionen bis hin zur außerordentlichen fristlosen Kündigung** nach sich ziehen kann.

8. Betroffenenrechte

Jeder Betroffene, dessen personenbezogene Daten von dem VÖB verarbeitet werden, hat das Recht auf **Auskunft** (Art. 15 DS-GVO) hinsichtlich der über ihn gespeicherten Daten, des Zwecks und Orts der Speicherung sowie der Herkunft und etwaiger Empfänger der Daten . Bei fehlerhaften Daten besteht ein Anspruch auf **Berichtigung** (Art. 16 DS-GVO) oder **Einschränkung der Verarbeitung** (Art. 18 DS-GVO), bei unzulässig gespeicherten oder nicht mehr erforderlichen Daten ein Anspruch auf **Löschung** (Art. 17 DS-GVO) der Daten. Gemäß Art. 20 DS-GVO darf jeder Betroffene verlangen, seine personenbezogenen Daten, die er uns bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesebaren Format zu erhalten oder diese an einen anderen Verantwortlichen zu übermitteln.

Gemäß Art. 7 Abs. 3 DS-GVO kann jeder Betroffene seine einmal zu einer konkreten Datenverarbeitung erteilte Einwilligung jederzeit dem VÖB gegenüber widerrufen. Dies hat zur Folge, dass der VÖB die Datenverarbeitung, die auf dieser Einwilligung beruhte, für die Zukunft nicht mehr fortführen darf.

Fügt der VÖB als „Verantwortlicher" dem Betroffenen durch eine nach der DS-GVO, dem BDSG oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist der VÖB dem Betroffenen zum Schadensersatz verpflichtet, es sei denn er hat die nach den Umständen des Falles gebotene Sorgfalt beachtet.

Jeder von einer Datenerhebung, -verarbeitung oder -nutzung Betroffene hat das Recht, sich unmittelbar an den Datenschutzbeauftragten des VÖB zu wenden und sich bei einer Datenschutzaufsichtsbehörde zu **beschweren** (Art. 77 DS-GVO), wenn er meint, durch den Umgang mit seinen personenbezogenen Daten in seinen Rechten verletzt worden zu sein.

9. Weitere Informationen

Für Rückfragen und weiterführende Informationen stehen den Mitarbeitern der jeweilige Vorgesetzte sowie unser Datenschutzbeauftragter (derzeit: Herr Thomas Ihering, Tel.: 030 81 92-296, E-Mail: thomas.ihering@voeb.de) zur Verfügung.

Berlin, den 03.01.2022

Iris Bethge-Krauß
Hauptgeschäftsführerin