

Anlage zur Beitrittserklärung/Beteiligungserklärung

Vereinbarung zur Auftragsdatenverarbeitung

zwischen

dem in der anliegenden Beitrittserklärung genannten Mitglied
als Auftraggeber

und

der DATEV eG, Paumgartnerstraße 6 - 14, 90429 Nürnberg
als Auftragnehmer

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien. Sie findet Anwendung auf alle Tätigkeiten, die mit der Durchführung von Aufträgen in Zusammenhang stehen, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Subunternehmer mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Die vertraglichen Verpflichtungen ergeben sich im Übrigen aus den sonstigen Vereinbarungen auf der Grundlage der Geschäftsbedingungen der DATEV.

§ 1 Definitionen

(1) Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person.

(2) Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist die Erhebung, Verarbeitung und Nutzung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

Nach § 11 Abs. 5 Bundesdatenschutzgesetz gelten die Inhalte dieser Vereinbarung entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird, und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Weisung

Weisung ist die auf einen bestimmten datenschutzrelevanten Umgang (zum Beispiel Berichtigung, Sperrung und Löschung) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch die vertraglichen Vereinbarungen festgelegt und können vom Auftraggeber danach durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

Mündliche Weisungen sind umgehend schriftlich zu bestätigen. Weisungen, die sich auf Löschungen oder Übertragung von Daten beziehen, sind schriftlich zu erteilen.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in den vertraglichen Vereinbarungen festgelegt sind. Der Auftraggeber ist im Rahmen der Auftragsdatenverarbeitung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG).

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Auftrages die Herausgabe oder Löschung der Daten bzw. von überlassenen Datenträgern verlangen.

§ 3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.
- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen. Eine Auflistung dieser Maßnahmen ist dieser Vereinbarung als Anhang beigefügt.
- (3) An der Erstellung der Verfahrensverzeichnisse hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.
- (4) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes,

bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers oder bei Verstößen gegen die in diesem Auftrag getroffenen Festlegungen.

- (5) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gem. § 5 BDSG (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.
- (6) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte über seine Daten und Unterlagen zu erteilen.
- (7) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten im Sinne des § 4 f BDSG bestellt hat. Der Datenschutzbeauftragte des Auftragnehmers ist aus dem öffentlichen Verfahrensverzeichnis ersichtlich, welches unter www.datev.de/datenschutz einsehbar ist.

§ 4 Pflichten des Auftraggebers

- (1) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.
- (2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (3) Dem Auftraggeber obliegen die aus § 42a BDSG resultierenden Informationspflichten.
- (4) Der Auftraggeber ist verpflichtet, alle im Rahmen des Auftragsverhältnisses erlangte Kenntnisse von Datensicherungsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 5 Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen. Voraussetzung ist, dass der Auftraggeber den Auftragnehmer hierzu schriftlich auffordert und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet.

§ 6 Kontrollrecht

- (1) Der Auftraggeber kann sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen.
- (2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.
- (3) Der Auftragnehmer unterzieht sich regelmäßig auf freiwilliger Basis einem datenschutzrechtlichen Zertifizierungsverfahren (vgl. § 9a BDSG). Ein entsprechendes Testat der Auditierung kann dem Auftraggeber vorgelegt werden. Sollte es im Ausnahmefall dennoch erforderlich sein, kann sich der Auftraggeber nach Anmeldung während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufes in den Betriebsstätten des Auftragnehmers von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen persönlich überzeugen.
- (4) Das Ergebnis seiner Prüfung wird der Auftraggeber dokumentieren.

§ 7 Subunternehmer

- (1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen und, soweit für die Geschäftsabwicklung notwendig, Subunternehmer mit Leistungen unterbeauftragt.

- (2) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Auftrag dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Auftrages.

§ 8 Löschung von Auftragsdaten

- (1) Der Auftraggeber trägt die Verantwortung für das Löschen der nicht mehr benötigten Daten.
- (2) Der Auftragnehmer kann im Rahmen seines Leistungsangebots bereits bei Auftragserteilung eine Regelfrist für die Datenlöschung vorgeben.
- (3) In jedem Fall werden Auftragsdaten des Auftraggebers bei Auftragsbeendigung gelöscht bzw. nach § 35 III BDSG gesperrt.

§ 9 Informationspflichten, Schriftformklausel, Sonstiges

- (1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die

Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

- (2) Der Auftraggeber verzichtet auf die Erklärung der Annahme durch DATEV an ihn (§ 151 Satz 1 BGB).
- (3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der sonstigen Vereinbarungen im Übrigen nicht.
- (5) Im Übrigen gelten die Geschäftsbedingungen der DATEV.

Anhang:

Technische und organisatorische Maßnahmen nach § 9 BDSG

Technische und organisatorische Maßnahmen gemäß Anlage zu § 9 BDSG

Nachstehend erfolgt eine Aufstellung und Beschreibung der wesentlichen Maßnahmen der DATEV in Nürnberg zur Einhaltung der Datensicherheitsvorschriften gemäß der Anlage zu § 9 BDSG (Kontrollziele Nr. 1 bis 8). Hierbei ist einschränkend darauf hinzuweisen, dass ein Rechenzentrum verständlicherweise nicht alle Sicherheitsvorkehrungen offenlegen kann; vielmehr ist gerade im Interesse des Datenschutzes und der Datensicherheit der Verzicht auf vertrauliche und detaillierte Beschreibungen unabdingbar. Durch freiwillige Datenschutzaudits gemäß § 9a BDSG wird auch der Nachweis erbracht, dass der Datenschutz bei DATEV nach den Vorgaben aus dem BDSG gesetzeskonform gestaltet und wirksam bei DATEV umgesetzt wird (Datenschutz-Zertifikat).

Zutrittskontrolle

Die Betriebsareale, die in mehrere Sicherheitsbereiche mit differenzierten Zugangsberechtigungen aufgeteilt sind, werden rund um die Uhr durch den Betriebsschutz überwacht. Der Zugang zu den baulich extrem abgeschotteten und elektronisch überwachten Sicherheitszonen des Rechenzentrums ist nur wenigen berechtigten Personen mit codierten Lichtbildausweisen möglich.

Zugangskontrolle

Der Zugang kann nur über ein Zugangskontrollsystem erfolgen. Beim elektronischen Datenaustausch zwischen dem DATEV-Rechenzentrum und den Mitgliedern bzw. Mandanten besteht das Sicherungssystem aus vielschichtigen und komplexen Prüfungen. Weitere technische Absicherungen erfolgen über Firewalls und Proxyserver.

Soweit technisch möglich und wirtschaftlich vertretbar, werden hierzu geeignete Verschlüsselungstechnologien eingesetzt.

Zugriffskontrolle

Eine Reihe von Hardware- und Software-Identifikationsmaßnahmen, die Verschlüsselung der Daten bei der Datenübertragung sowie ein mehrstufiges Zugriffs- und Nutzungskontrollverfahren schließen den unbefugten Zugriff auf die gespeicherten Datenbestände und die unberechtigte Kenntnisnahme aus.

Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen. Soweit technisch möglich und wirtschaftlich vertretbar, werden hierzu geeignete Verschlüsselungstechnologien eingesetzt.

Weitergabekontrolle

Beim elektronischen Datenaustausch besteht das Sicherungssystem aus vielschichtigen und komplexen Prüfungen.

Strenge Sicherheitsvorkehrungen im Rechenzentrum gewährleisten, dass ein unbefugtes Entfernen von Datenträgern aus den Sicherheitsbereichen verhindert wird. Entsorgungsgut mit schutzwürdigem Inhalt wird durch eine hausinterne Shredderanlage unter Beachtung des Vier-Augen-Prinzips nach einer hohen Sicherheitsstufe vernichtet.

Soweit technisch möglich und wirtschaftlich vertretbar, werden hierzu geeignete Verschlüsselungstechnologien eingesetzt.

Eingabekontrolle

Ein mehrstufiges Protokoll- und Auditingverfahren gewährleistet, dass keine Datenveränderungen unbemerkt vorgenommen werden können.

Auftragskontrolle

Die zur Verarbeitung eingereichten Daten werden entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen des jeweiligen Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben werden. Der Weisungsrahmen ist insbesondere durch den schriftlich geschlossenen Vertrag zur Datenverarbeitung im Auftrag unter Berücksichtigung der Pflichtinhalte gemäß § 11 Abs. 2 BDSG sowie ferner durch die Anwendungsbeschreibung der DATEV-Dienstleistungsprogramme eindeutig vorgegeben. Gleiches gilt für auftragsbezogene Auskünfte; sie werden ausschließlich an den Auftraggeber oder im Rahmen seiner Weisungen erteilt. Ausnahmen vom konkreten Weisungsrahmen gelten für technisch bedingte Verarbeitungen, z. B. für die interne Datensicherung.

Verfügbarkeitskontrolle

Zahlreiche Datensicherungsmaßnahmen gewährleisten, dass personenbezogene und andere schutzwürdige Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Besonders umfangreich sind die Brandschutz-, Verlustsicherungs- und Katastrophenschutz-Maßnahmen. Hierzu gehören unter anderem die Absicherung sämtlicher EDV-Räume und deren Umgebung durch Brandmelde- und stationäre Feuerlöschanlagen, die mehrfache maschinelle und gegen unbefugten Zugriff gesicherte Auslagerung von Datensicherungsbeständen, die Notstromversorgung zur unterbrechungsfreien Überbrückung von Stromausfällen sowie der 24-Stunden-Bereitschaftsdienst von Einsatz- und Evakuierungsleitung.

Trennungsgebot

In allen wichtigen Bereichen besteht das Prinzip der Funktionstrennung; das heißt, alle in die Datenverarbeitung eingebundenen Abteilungen sind funktionell, organisatorisch und räumlich getrennt. Das Prinzip der Funktionstrennung ist auch weitgehend innerhalb der Organisationseinheiten verwirklicht; schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist. Zur Sicherstellung werden definierte Rechteprofile für die verschiedenen Funktionsbereiche zugeteilt und zentral administriert.

Zahlreiche Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken und für unterschiedliche Ordnungsbegriffe (z. B. Mitglieds- und Mandantenummer) erhobene bzw. gespeicherte Daten getrennt verarbeitet werden können.