Leitlinie Datenschutz und Informationssicherheit

Leitlinie zum Schutz personenbezogener Daten und zur Informationssicherheit

Fassung vom 14.12.2021

Präambel

Der Verein zur Förderung eines Deutschen Forschungsnetzes - DFN-Verein e. V. - ist die zentrale Einrichtung der Wissenschaft in Deutschland für Entwicklung und Betrieb einer ihr eigenen Kommunikationsinfrastruktur, dem Deutschen Forschungsnetz.

Der DFN-Verein verwirklicht seinen satzungsgemäßen Zweck insbesondere durch Organisation von Dienstleistungen zur Nutzung des Deutschen Forschungsnetzes (DFN-Dienste). Dabei ist davon auszugehen, dass auch personenbezogene Daten erhoben und verarbeitet werden müssen sowie zur Sicherstellung der notwendigen Verfügbarkeit, Vertraulichkeit und Integrität der DFN-Dienste ein angemessenes Informationssicherheitsniveau gewährleistet sein muss.

1 Grundlagen

Gemäß Artikel 3 Ziffer 1 der EU-Datenschutz-Grundverordnung (EU-DSGVO) sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der besondere Schutz personenbezogener Daten ist bereits seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15.Dezember 1983 verfassungsrechtlich verankert: Aus dem allgemeinen Persönlichkeitsrecht ergibt sich ein Recht auf informationelle Selbstbestimmung. Der Datenschutz bezweckt somit den Schutz des Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht durch den angemessenen Umgang mit seinen personenbezogenen Daten.

Der Umgang mit personenbezogenen Daten in Umsetzung völkerrechtlicher Verpflichtungen ist ab dem 25. Mai 2018 in der EU-DSGV0 geregelt, die in den europäischen Staaten und damit auch für den DFN-Verein ohne weitere Umsetzung gilt. Damit obliegt es ihm die technischen und organisatorischen Maßnahmen zu treffen die erforderlich sind, um die Ausführung der EU-DSGVO zu gewährleisten.

Der Schutz sensitiver betrieblicher Daten, Informationen und Systeme ist ebenfalls eine zwingende Anforderung, obwohl dieser Bereich gesetzlich weniger explizit als der Datenschutz geregelt ist. Diese Anforderung ergibt sich vielfach aus vertraglichen und rechtlichen Verpflichtungen, darüber hinaus aber auch aus dem Eigeninteresse, die Ziele des DFN-Vereins nicht durch ein zu niedriges Sicherheitsniveau zu gefährden.

2 Ziele

Mit dieser Leitlinie zum Datenschutz und zur Informationssicherheit gibt sich der DFN-Verein den Rahmen für den Umgang mit personenbezogenen Daten und den sicheren Betrieb der informationstechnischen Infrastrukturen, die für die Erfüllung des satzungsgemäßen Vereinszwecks benötigt werden.

3 Selbstverpflichtung und Leitbild

Die Geschäftsführung und die Mitarbeiter der Geschäftsstelle des DFN-Vereins sind sich ihrer Verantwortung bei der Erbringung der DFN-Dienste und im Umgang mit den dafür eingesetzten informationstechnischen Infrastrukturen bewusst. Die Umsetzung von Datenschutz und Informationssicherheit hat einen hohen Stellenwert. Es werden alle notwendigen geeigneten und angemessenen Maßnahmen getroffen, um negative materielle und immaterielle Folgen für Betroffene und den DFN-Verein auszuschließen.

Als Gemeinschaftseinrichtung der Wissenschaft in Deutschland sieht sich der DFN-Verein verpflichtet, ergänzend zur Umsetzung des Datenschutzes und der Informationssicherheit in seinen eigenen Arbeitsabläufen auch eine befördernde Wirkung in Richtung der wissenschaftlichen Einrichtungen in Deutschland zu entfalten. Dabei hat er als Leitbild eine wirkungsvolle Umsetzung unter Berücksichtigung der besonderen Eigenschaften der Arbeitsabläufe in Forschung und Lehre vor Augen.

4 Prinzipien

Der Umgang mit personenbezogenen Daten ist in der EU-DSGVO als **Verbot mit Erlaubnisvorbehalt** geregelt. Damit ist das Verarbeiten von personenbezogenen Daten grundsätzlich verboten. Ausnahmen bestehen nur, wenn ein Gesetz dies erlaubt oder der Betroffene einwilligt. Hieraus leitet der DFN-Verein vier Prinzipien zur Umsetzung des Datenschutzes ab. Diese sind:

1. Der DFN-Verein strebt bei allen seinen Arbeitsvorgängen an, die Verarbeitung von personenbezogenen Daten zu vermeiden (Prinzip der **Datenvermeidung**).
2. Soweit bei Arbeitsvorgängen die Verarbeitung von personenbezogenen Daten nicht vermieden werden kann, wählt der DFN-Verein im Rahmen des technisch und organisatorisch Vertretbaren jeweils den Arbeitsvorgang, bei dem so wenig personenbezogene Daten wie möglich verarbeitet werden müssen (Prinzip der **Erforderlichkeit**).
3. Eine Verwendung von personenbezogenen Daten für einen anderen als den vorab festgelegten oder einem diesem besonders nahen Zweck ist ausgeschlossen. Ausnahmen ergeben sich nur, wenn ein Gesetz dies erlaubt oder der Betroffene einwilligt (Prinzip der **Zweckbindung**).
4. Bei allen Arbeitsvorgängen werden die gesetzlichen Löschfristen beachtet. Werden personenbezogene Daten nicht mehr benötigt, werden sie auch ohne Ausschöpfung der Löschfristen gelöscht (Prinzip der **Datenminimierung)**.

Eine wirksame Umsetzung des Datenschutzes ist nur mit einer wirkungsvollen Informationssicherheit zu erreichen. Zudem folgen für den DFN-Verein auch aus grundsätzlichen Erwägungen Anforderungen an die Informationssicherheit. Darum formuliert der DFN-Verein neben den vier Prinzipien zur Umsetzung des Datenschutzes auch drei Prinzipien zur Umsetzung der Informationssicherheit und des Notfallmanagements. Diese sind:

1. Die Vermeidung von Unterbrechungen und Inkonsistenzen der für einen DFN-Dienst eingesetzten informationstechnischen Infrastrukturen spielt eine maßgebliche Rolle bei der Durchführung der Arbeitsvorgänge der betreffenden DFN-Dienste. Deswegen werden die für die Erbringung von DFN-Diensten eingesetzten informationstechnischen Infrastrukturen so betrieben, dass Ausfälle einzelner Komponenten im Rahmen des Notfallmanagements toleriert werden können (Prinzip der **Verfügbarkeit und Fehlerfreiheit**).

2. Technische und organisatorische Maßnahmen stellen sicher, dass die Auswirkungen von Unregelmäßigkeiten in Daten oder Fehlfunktionen in informationstechnischen Infrastrukturen vermieden werden, nicht unbemerkt bleiben und zeitlich begrenzt werden (Prinzip der **Integrität**).
3. Der Schutz sensibler Daten und informationstechnischer Infrastrukturen wird dadurch gewährleistet, dass diese ausschließlich Berechtigten zugänglich gemacht werden (Prinzip der **Vertraulichkeit**).

Der DFN-Verein erbringt ausschließlich Dienste, deren Informationssicherheits- und Datenschutzniveau entsprechend dieser sieben Prinzipien umgesetzt werden kann. Bei der Umsetzung der Prinzipien berücksichtigt er ein wirtschaftlich vertretbares Verhältnis im Vergleich zum Wert der betreffenden Informationen und IT-Systeme.

5 Umsetzung

Die Umsetzung der Prinzipien zum Datenschutz und zur Informationssicherheit in den Arbeitsabläufen des DFN-Vereins erfordert technische und organisatorische Maßnahmen. Diese werden in den Richtlinien zum Management der Informationssicherheit und zum Datenschutzmanagement, den dort verankerten Prozessbeschreibungen und anderen Vorgaben geregelt. Die Aufteilung in unterschiedliche Dokumente ist in der Organisations- und Dienstleistungsstruktur für die Geschäftsstelle des DFN-Vereins begründet.

Durch die Etablierung eines Datenschutzmanagementsystems (DSMS), eines Informationssicherheitsmanagementsystems (ISMS) und eines Notfallmanagementsystems (Business Continuity Management Systems) werden kontinuierliche Revisionen dieser Regelungen und deren konsequente Einhaltung für das angestrebte Datenschutz- und Informationssicherheitsniveau sichergestellt. Abweichungen werden unmittelbar mit dem Ziel analysiert, den Datenschutz, die Informationssicherheit und das Notfallmanagement zu verbessern und auf dem aktuellen Stand der Technik zu halten.

Für die Umsetzung der Prinzipien zum Datenschutz, der Informationssicherheit und des Notfallmanagements hat der DFN-Verein einen Datenschutzbeauftragten, einen Beauftragten für Informationssicherheit und einen Notfallbeauftragten benannt.

Der Datenschutzbeauftragte überwacht die Einhaltung der gesetzlichen Vorgaben zum Datenschutz und berät die Geschäftsführung auf Anfrage zur Umsetzung des Datenschutzes. Er ist darüber hinaus Ansprechpartner für betroffene Personen und für die zuständige Datenschutzaufsichtsbehörde.

Der Beauftragte für Informationssicherheit berät die Geschäftsführung bei allen Fragen zur Informationssicherheit der ihm zugeordneten Informationsverbünde. Er tauscht sich regelmäßig und darüber hinaus anlassbezogen mit dem Datenschutzbeauftragten zu Maßnahmen der Informationssicherheit und zu datenschutzrelevanten Sicherheitsvorfällen aus.

Der Notfallbeauftragte berät die Geschäftsführung zum Thema Notfallmanagement und koordiniert die entsprechenden Tätigkeiten. Er kooperiert diesbezüglich mit den Beauftragten für Datenschutz und Informationssicherheit. Zu seinen Kerntätigkeiten gehören die Identifikation kritischer Geschäftsprozesse, die Festlegung der jeweiligen Kritikalität und der daraus abzuleitenden notwendigen Vorsorgemaßnahmen. Der Notfallbeauftragte steuert und kontrolliert die Durchführung angemessener Notfallübungen.

Datenschutz und Informationssicherheit sind ein integraler Bestandteil der entsprechenden Fachaufgabe. In die Zuständigkeit der jeweiligen Fachverantwortlichen fallen somit auch Maßnahmen, um den Datenschutz und die Informationssicherheit in Ihrem Bereich umzusetzen, aufrecht zu erhalten und bei Bedarf an neue rechtliche, technische und organisatorische Gegebenheiten anzupassen. Die hierfür erforderlichen technischen, organisatorischen und personellen Voraussetzungen werden von der Geschäftsführung in Abstimmung mit dem Datenschutzbeauftragten und dem Beauftragten für Informationssicherheit geschaffen.

Zur Abwehr und zur Minderung der Folgen von Angriffsversuchen auf die informationstechnischen Infrastrukturen der DFN-Dienste ergreift der DFN-Verein sowohl proaktive als auch zeitnahe reaktive Maßnahmen. Die Maßnahmen werden durch ein Computer Emergency Response Team (CERT) maßgeblich unterstützt. Das CERT übernimmt auch die organisationsübergreifende Koordination mit externen Experten, Herstellern sowie im Verbund mit anderen CERTs.

Eine befördernde Wirkung in Richtung der wissenschaftlichen Einrichtungen entfaltet der DFN-Verein durch die Organisation eines kontinuierlichen Wissensaustausches zum

Datenschutz und zur Informationssicherheit, mit dem eine breite Sensibilisierung initiiert und eine zielgerichtete Diskussion über geeignete Maßnahmen befördert werden soll.

6 Geltungsbereich

Diese Leitlinie gilt für die Rechtsperson DFN-Verein.

7 Geltungsdauer

Diese Leitlinie tritt mit Beschluss des Vorstandes vom 14. Dezember 2021 in Kraft und ersetzt die Fassung vom 18. April 2018. Sie gilt, bis sie außer Kraft gesetzt oder durch eine jüngere Fassung ersetzt wird.