

FRAUNHOFER-INFORMATIONSSICHERHEITS- UND DATENSCHUTZ-POLICY



Im Interesse ihrer Kundschaft und Zuwendungsgeber sowie ihrer Mitarbeitenden ist für die Fraunhofer-Gesellschaft die Verfügbarkeit, Vertraulichkeit und Integrität ihrer Informationen sowie informationsverarbeitenden Verfahren sehr wichtig und definiert Maßnahmen, um deren Missbrauch zu verhindern. Sie wahrt die Persönlichkeitsrechte von Fraunhofer-Mitarbeitenden, von Kunden und Probanden und gewährleistet die Umsetzung der Betroffenenrechte. Die dazu erforderlichen Maßnahmen werden innerhalb eines Fraunhofer-weit vorgegebenen Rahmens durch die Fraunhofer-Institute lokal so festgelegt, dass die Informationssicherheits- und Datenschutz-Anforderungen der jeweiligen Forschungsfelder angemessen erfüllt werden.

1

Geschäftszweck

Die Fraunhofer-Gesellschaft betreibt anwendungsorientierte Forschung mit dem Ziel, ihren Kunden und Kundinnen system- und technologieorientierte Innovationen zu ermöglichen und die Wettbewerbsfähigkeit ihrer Regionen, Deutschlands und Europas zu stärken. Voraussetzung dafür ist, Know-how und die informationsverarbeitenden Verfahren gegen Spionage, Cyberangriffe, Fehler und Missbräuche zu schützen und die Anforderungen unserer Stakeholder, Industriestandards sowie Bestimmungen der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes zu beachten. Daher genießen die Informationssicherheit und der Datenschutz in der Fraunhofer-Gesellschaft und ihren Instituten einen hohen Stellenwert.

2

Geltungsbereich

Diese vorliegende Policy ist die zentrale Fraunhofer-weite Leitlinie zur Informationssicherheit und zum Datenschutz. Sie beschreibt grundlegende Ziele zum Schutz von Informationen und personenbezogenen Daten in der Fraunhofer-Gesellschaft. Sie gilt für alle papierlosen sowie papiergebundenen Verfahren der Informationsverarbeitung.

Sie ist verbindlich für alle Institute, aber auch für die Zentrale und sonstige Einrichtungen der Fraunhofer-Gesellschaft e.V. (im Folgenden sind all diese Fraunhofer-Einheiten gemeint, auch wenn nur Institute genannt werden). Zudem ist die Leitlinie verbindlich für alle Mitarbeitenden sowie für Externe, die als Dienstleister oder Nutzerinnen und Nutzer an informationsverarbeitenden Verfahren der Fraunhofer-Gesellschaft mitwirken.

Andere gesetzliche Anforderungen zum Schutz von Informationen bleiben unberührt.

3

Ziele

Die Fraunhofer-Gesellschaft verfolgt folgende grundlegende Informationssicherheits- und Datenschutz-Ziele:

- Schutz von Informationen und personenbezogenen Daten ihrer Kunden, Zuwendungsgeber und Beschäftigten im Hinblick auf Verfügbarkeit, Vertraulichkeit und Verfügbarkeit sowie Missbrauch.
- Schutz von eigenen Geschäftsgeheimnissen sowie denen unserer Kundschaft
- Sicherung Informationssystem-gestützter Geschäftsprozesse und Erhalt der Arbeitsfähigkeit u. a. bei Cyberangriffen (Cybersicherheit)
- Schutz jeglicher personenbezogenen Daten.
- Einhaltung der einschlägigen Gesetze und vertraglichen Regelungen mit Kunden/-innen und Partnern sowie anderer rechtlicher Bestimmungen zur Informationssicherheit und zum Datenschutz (insbesondere der Datenschutz-Grundverordnung – DSGVO).
- Förderung des Verantwortungsbewusstseins der Mitarbeitenden hinsichtlich Informationssicherheit und Datenschutz durch gezielte Sensibilisierungsmaßnahmen
- Wahrung der Rechte der Betroffenen von Datenverarbeitungen

Aus der Anforderung nach Informationssicherheit und Datenschutz lassen sich folgende Anforderungen ableiten:

- **Risikobeurteilung:** Informationssicherheits- und Datenschutz-Risiken werden regelmäßig identifiziert, analysiert und bewertet – dezentral in den Instituten und zentral für Fraunhofer insgesamt.
- **Schutz von Informationen und personenbezogenen Daten:** Institute schützen Vertraulichkeit, Integrität und Verfügbarkeit erarbeiteter oder übergebener Informationen und der informationsverarbeitenden Systeme / Programme und wehren Missbrauchsversuche ab (zweckwidrige Nutzung, Nutzung durch Unbefugte).
- **Ausrichtung der Informationssicherheit und des Datenschutzes an Schutzerfordernis:** Maßnahmen zum Schutz von Informationen, Systemen, Anwendungen behandeln die Risiken am jeweiligen Institut sowie die Risiken betroffener Personen in angemessener Weise.
- **Nachweisbarkeit:** Durch die Orientierung ihrer Informationssicherheits- (ISMS) und Datenschutz-Managementsysteme (DSMS) an international anerkannten Standards können von Kunden geforderte Informationssicherheits- und Datenschutz-Nachweise überzeugend gestaltet werden.

4 Prinzipien

Zur Erreichung der grundlegenden Informationssicherheits- und Datenschutz-Ziele werden folgende allgemeine Prinzipien definiert:

- Fraunhofer orientiert sich an internationalen Informationssicherheits- und Datenschutz-Standards, insbesondere an ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27701. Bei deren Umsetzung wird den unterschiedlichen Sicherheits- und Datenschutzerfordernissen verschiedener Arbeits-/ Forschungsfelder der Institute Rechnung getragen.
- Informationssicherheit und Datenschutz sind von Fraunhofer sicherzustellen, unabhängig davon, ob Fraunhofer Informationen elektronisch oder auf Papier, auf Fraunhofer-eigenen oder Systemen Dritter verarbeitet werden.
- Zentral vorgegeben werden in Fraunhofer Informationssicherheits- und Datenschutz-Mindestmaßnahmen (Richtlinien), die zum Schutz institutsübergreifender Infrastrukturen oder betroffener Personen, der Reputation der Fraunhofer-Gesellschaft insgesamt, der internen Kooperation oder aus Gründen der Wirtschaftlichkeit erforderlich sind.
- Im Rahmen der zentralen Vorgaben erarbeiten die Institute eigene Sicherheits- und Datenschutzkonzepte, die für die Sicherheits- und Datenschutzerfordernissen der jeweiligen Tätigkeitsfelder angemessen sind. Die Angemessenheit lokaler Maßnahmen und die Einhaltung zentraler Mindestvorgaben werden durch regelmäßige Audits sichergestellt.
- Von allen Instituten genutzte Fraunhofer-weite IT-Services werden so ausgestaltet, dass sie den individuellen Informationssicherheits- und Datenschutzerfordernissen der Institute gerecht werden.
- Maßnahmen zur Informationssicherheit und technisch-organisatorische Maßnahmen zum Datenschutz sind aufeinander abgestimmt, um Widersprüche und Mehrfachaufwände für die Institute zu vermeiden. Aus diesem Grund sind die Informationssicherheits- und Datenschutz-Koordination organisatorisch miteinander verzahnt.
- In der Forschung lässt sich Informationssicherheit und Datenschutz nicht allein durch technische Einschränkungen und Überwachung erreichen, sondern erfordert verantwortungsbewusste Mitarbeitende. Die Fraunhofer-Gesellschaft legt daher besonderes Gewicht auf die Sensibilisierung, Motivation und Befähigung ihrer Mitarbeitenden zum sachgerechten Umgang mit Informationssicherheits- und Datenschutzerisiken.
- Gesetzesbrüche / Regelverletzungen werden bei Fraunhofer nicht toleriert und daher geahndet.

5 Verantwortlichkeiten und Rollen

Aufgrund der zentral/dezentralen Organisation der Fraunhofer-Gesellschaft sind für Informationssicherheit und Datenschutz eine Reihe von zentralen und Instituts-lokalen Funktionsträger und -trägerinnen verantwortlich:

- Der Vorstand trägt die Gesamtverantwortung für Informationssicherheit in der Fraunhofer-Gesellschaft und bewertet in regelmäßigen Abständen sowie anlassbezogen die fortdauernde Eignung, Angemessenheit und Wirksamkeit des Fraunhofer ISMS. Er ernennt eine/n Informationssicherheitskoordinator/in sowie die Vertretungen und stellt die notwendigen zentralen Ressourcen zur Erreichung der Fraunhofer-Informationssicherheits-Ziele zur Verfügung.
- Der Gesamtvorstand trägt die Gesamtverantwortung für die Umsetzung von Datenschutzmaßnahmen bei Fraunhofer. Der Vorstand Personal, Unternehmenskultur und Recht übt die Funktion des Verantwortlichen i.S.d. DSGVO bzw. des BDSG aus. Er ernennt eine/n Datenschutz-Koordinator/in, eine/n betrieblichen Datenschutzbeauftragten sowie die Vertretungen und stellt die notwendigen zentralen Ressourcen zur Erreichung der Fraunhofer-Datenschutz-Ziele zur Verfügung.
- Die / Der betriebliche Datenschutzbeauftragte ist im Auftrag der Vorständin / des Vorstands an der Schnittstelle zwischen der Fraunhofer-Gesellschaft, den Datenschutzbehörden und betroffenen Personen tätig.
- Im Auftrag des Gesamtvorstands ist der / die Informationssicherheits-Koordinator/in für Planung, Umsetzung, Überwachung, Überprüfung und kontinuierliche Verbesserung des Fraunhofer-ISMS und der / die Datenschutz-Koordinator/in für Planung, Umsetzung, Überwachung, Überprüfung und kontinuierliche Verbesserung des Fraunhofer-DSMS verantwortlich.
- Der / die Informationssicherheits-Koordinator/in stimmt zusammen mit dem / der Datenschutz-Koordinator/in Mindestanforderungen an die Informationssicherheit und den Datenschutz mit dem Gesamtvorstand ab, erarbeitet Organisationsanweisungen und Richtlinien zur Informationssicherheit und Datenschutz, überprüft die Umsetzung der geplanten Maßnahmen und berichtet dem Gesamtvorstand über den aktuellen Stand der Informationssicherheit und des Datenschutzes sowie über aufgetretene Vorfälle und Schwachstellen.
- Die Institutsleitenden sind für die Informationssicherheit und den Datenschutz in ihren Instituten verantwortlich und bewerten in regelmäßigen Abständen sowie anlassbezogen die fortdauernde Eignung, Angemessenheit und Wirksamkeit des lokalen ISMS und DSMS. Sie ernennen für ihr Institut Informationssicherheits-Beauftragte und Datenschutz-Ansprechpersonen sowie deren Vertretungen, entscheiden über lokal gültige Informationssicherheits- und Datenschutz-Ziele sowie -Maßnahmen, beschließen ein Sicherheits- und ein Datenschutzkonzept für ihr Institut und stellen die notwendigen Ressourcen zur Erreichung der Ziele in ihren Instituten zur Verfügung.
- Im Auftrag der Institutsleitung sind die Informationssicherheits-Beauftragten für die Umsetzung, Überwachung, Überprüfung sowie kontinuierlichen Verbesserung des institutsspezifischen ISMS verantwortlich und, sofern im Datenschutz-Konzept einer Einheit nicht explizit eine andere Regelung festgelegt wurde, unterstützen die Datenschutz-Ansprechpersonen bei der Umsetzung, Überwachung, Überprüfung sowie kontinuierlichen Verbesserung des institutsspezifischen DSMS. Sie koordinieren die Erstellung lokaler Sicherheits- und Datenschutzkonzepte, legen institutsspezifische Informationssicherheits- und Datenschutz-Maßnahmen fest, überprüfen deren Umsetzung und berichten sowohl der Institutsleitung als auch der Informationssicherheits- und Datenschutz-Koordination über den aktuellen Stand der Informationssicherheit und des Datenschutzes in ihrem Institut sowie über aufgetretene Vorfälle und Schwachstellen.
- Für jede Verarbeitungstätigkeit bzw. das jeweilige Verfahren, mit dem personenbezogene Daten verarbeitet werden, wird eine verantwortliche Person festgelegt, die auch für die Einhaltung des Datenschutzes innerhalb dieses Verfahrens zuständig ist.

- Die Projektleiter und -leiterinnen tragen für den Schutz der Projektergebnisse sowie Kundendaten die Verantwortung und stimmen sich zu speziellen Erfordernissen der Informationssicherheit mit dem/der lokalen Informationssicherheits-Beauftragten und zu speziellen Erfordernissen des Datenschutzes mit der lokalen Datenschutz-Ansprechperson ab.

Alle Fraunhofer-Mitarbeitenden sowie die von der Fraunhofer-Gesellschaft beauftragten Dienstleister sowie Nutzerinnen und Nutzer ihrer informationsverarbeitenden Systeme, Programme und Daten sind für die Informationssicherheit und den Datenschutz in ihren jeweiligen Aufgabengebieten verantwortlich.

Unterstützende Services für den Informationssicherheit und Datenschutz sind:

- Die Rechtsabteilung unterstützt alle Beteiligten bei der Beurteilung rechtlicher Sachverhalte, der Erstellung von Klauseln sowie Vertragsverhandlungen. Diese Unterstützung kann im Falle eines hohen Arbeitsaufkommens, auch an Anwälte mit entsprechendem Rahmenvertrag delegiert werden.
- Das Fraunhofer Security Operations Center (SOC) unterstützt die an ISO/IEC 27035 orientierte Behandlung von Informationssicherheits- und Datenschutz-Vorfällen.
- Die Fraunhofer Audit- und Monitoring-Services (AMS) unterstützen die Innenrevision bei der Fraunhofer-weiten Prüfung der Einhaltung der gültigen Regelungen der Fraunhofer-Gesellschaft durch zielgerichtete Informationssicherheits- und Datenschutz-Audits. Sie stellen Self-Assessments für die Einheiten bereit und werten deren Ergebnisse aus. Darüber hinaus führen die Services regelmäßig sowie anlassbezogen Schwachstellen-Scans aller von außen erreichbaren Fraunhofer Informationssysteme durch und überwachen permanent die Verfügbarkeit aller Fraunhofer-weiten IT-Services.
- Die Provider der Fraunhofer-weiten IT-Services erarbeiten für ihre IT-Services Informationssicherheits- und Datenschutz-Konzepte und stimmen diese mit dem Informationssicherheitsbeauftragter und Datenschutz-Ansprechperson der zentralen Services ab.

6 Umsetzung von Richtlinien

Die zentrale Informationssicherheits- und Datenschutzkoordination gibt verbindliche Mindeststandards im Rahmen von Richtlinien vor, die für alle Institute verbindlich sind. Dabei werden folgende Themengebiete abgedeckt:

- a) Zugangssteuerung;
- b) physische und umgebungsbezogene Sicherheit;
- c) Verwaltung der Werte;
- d) Informationsübertragung;
- e) sichere Konfiguration und Handhabung von Benutzerendpunktgeräten;
- f) Netzwerksicherheit;
- g) Handhabung von Informationssicherheitsvorfällen;
- h) Datensicherung;
- i) Kryptographie und Schlüsselverwaltung;
- j) Informationsklassifizierung und deren Handhabung;
- k) Handhabung von technischen Schwachstellen;
- l) sichere Entwicklung;
- m) Verfahrensverzeichnis;
- n) Löschkonzept;
- o) Datenschutzfolgenabschätzung;
- p) Technische und organisatorische Maßnahmen

Um das verzahnte Informationssicherheits- und Datenschutzmanagementsystem der Fraunhofer-Gesellschaft zu etablieren und die vorgegebenen Richtlinien zu erfüllen, wurden folgende Organisationsanweisungen (Regelungen unterhalb der Satzung der Fraunhofer-Gesellschaft) verabschiedet:

- Informationssicherheit
- Informationsklassifizierung
- IT-Benutzerordnung
- Datenschutz

Alle Einheiten müssen eigene, von den Anforderungen ihres Forschungsbereichs sowie vom Bedarf ihrer Kunden abgeleitete angemessene Sicherheits- und Datenschutzkonzepte, welche die Leitlinien und Richtlinien berücksichtigen, entwickeln.

7 Kommunikation & Schulung

Diese Policy wird intern veröffentlicht und kann für ausgewählte externe Parteien (Kunden, externe Auditoren, etc.) ohne den Bedarf einer Freigabe bereitgestellt werden.

Jede Einheit ist verpflichtet, ein Informationssicherheitstraining mindestens einmal im Jahr für ihre Mitarbeitenden und Externe durchzuführen.

Alle Mitarbeitenden der Fraunhofer-Gesellschaft müssen gemäß der Pflicht der/des Datenschutzbeauftragten aus Art. 39 Abs. 1 lit. B DSGVO eine Datenschutzbildung in Form eines von der Zentrale zur Verfügung gestellten web-basierten Trainings inklusive Abschlusstest durchführen.

8 Inkrafttreten

Diese Policy wurde vom Vorstand der Fraunhofer-Gesellschaft erstmals am 01.09.2014 beschlossen und trat zum 01.10.2014 in Kraft. Erstmals wurde diese Leitlinie dann am 31.08.2020 aktualisiert und in der Fassung vom 13.12.2022 erneut überarbeitet. Bei dieser hier vorliegenden Fassung wurde zuletzt am 30.04.2024 eine Überarbeitung durchgeführt. Diese Fassung tritt nun zum 15.05.2024 in Kraft und wird spätestens zum 31.12.2027 wieder überprüft.

Kontakt

Informationssicherheits-Koordination der Fraunhofer-Gesellschaft:

IS-Koordination@zv.fraunhofer.de

Datenschutz-Koordination der Fraunhofer-Gesellschaft:

Datenschutzkoordination@zv.fraunhofer.de