DATENSCHUTZKONFORMES LÖSCHEN BEI DATENSCHUTZ- UND INFORMATIONS-SICHERHEITSVORFÄLLEN

Louisa Rudolph, Dr. Annika Selzer, Dr. Ulrich Pordesch

Vorschlag einer Löschregel

Informationssicherheits- und Datenschutzvorfälle müssen erkannt, analysiert, bewertet, gemeldet und unter anderem zum Nachweis korrekten Handelns dokumentiert werden. Die Dokumentation enthält meist personenbezogene Daten, fast immer die der Bearbeiter des Vorfalls, aber auch die von Betroffenen oder Dritten. In diesem Beitrag wird erörtert, wann personenbezogene Daten, die im Rahmen einer Dokumentation von Datenschutz- und Sicherheitsvorfällen anfallen, entsprechend der Vorgaben der DSGO zu löschen sind und wie eine Löschregel zur Vorfalldokumentation für einen Löschregelkatalog gebildet werden kann.

1. Was sind Datenschutz- und Informationssicherheitsvorfälle und wieso bedarf es eines Vorfallmanagements?[1]

Informationssicherheitsvorfälle können in vielen verschiedenen Formen auftreten, zum Beispiel in Form von technischen Fehlern, Malware-Attacken, Hackerangriffen, Überwachungen des Datenverkehrs, Sabotage gegen die IT-Infrastruktur, unbefugte Datenverschlüsselung oder Datendiebstahl. In vielen Fällen geht es dabei um Betrug, Erpressung, Industrie- oder Wirtschaftsspionage, also die Schädigung der Unternehmen. Vielfach sind jedoch auch Personen und deren Daten das Ziel der Attacken oder sie sind von Attacken und Fehlern mittelbar betroffen. Beispiele hierfür sind der versehentliche Versand von personenbezogenen Informationen an falsche Mail-Adressen bei Beantwortung von Ersuchen betroffener Personen[2], oder das Stehlen von E-Mails und Kontakten, um gezielte Phishing-Attacken gegen Dritte durchzuführen. Ein IT-Sicherheitsvorfall ist in solchen Fällen zugleich auch ein Datenschutzvorfall.[3] Viele Unternehmen und Organisationen sind aufgrund branchenspezifischer Vorgaben verpflichtet, IT-Sicherheitsvorfälle zu melden und geeignete Maßnahmen zur Schadensbegrenzung vorzunehmen. Unternehmen, die solche konkreten Verpflichtungen nicht haben, trifft immer noch die allgemeine Pflicht zum Risikomanagement und damit auch zur Vorfallbehandlung, etwa über das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) oder aufgrund vertraglicher Verpflichtungen, Qualitäts- und Sicherheitszertifizierungen. Bei Datenschutzvorfällen ergeben sich insbesondere aus der DSGVO die folgenden konkreten Verpflichtungen:

- die unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 Abs. 1 DSGVO),
- die unverzügliche Benachrichtigung der betroffenen Personen, sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 34 Abs. 1 DSGVO).

Um den Verpflichtungen nachzukommen, müssen Sicherheits- und Datenschutzvorfälle erkannt, analysiert, bewertet und gemeldet werden; es sind die Schadensfolgen zu begrenzen und zu beseitigen und Maßnahmen gegen eine Wiederholung zu ergreifen. Dies erfordert ein Vorfall-Management mit geregelten Zuständigkeiten und Prozessen. Da Informationssicher-

[1] Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autorinnen und des Autors wieder und ist keine offizielle Stellungnahme der Fraunhofer Gesellschaft.

[2] Jandt, in: Kühling/ Buchner, DS-GVO BDSG, Art. 4 Abs. 12 DSGVO, Rn. 7.

[3] https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/emotet-trojaner-beantwortet-empfangene-emails-und-klaut-anhaenge-35502.

heits- und Datenschutzvorfälle vielfach nicht voneinander zu trennen sind, ist dabei ein integriertes einheitliches Management von Datenschutz- und Informationssicherheitsvorfällen sinnvoll.

Ein Datenschutz- und Informationssicherheitsvorfallmanagement beschäftigt sich mit dem Umgang mit Verletzungen des Schutzes personenbezogener Daten (Datenschutz) und von Informationen und IT-Systemen (Informationssicherheit). Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DSGVO). Während bei Datenschutzvorfällen der für die betroffenen Personen entstehende Schaden im Vordergrund steht, bedeuten Informationssicherheitsvorfälle zumeist einen wirtschaftliche Schaden für das Unternehmen, der durch den unbefugten Zugriff auf Daten wie beispielsweise Patentanmeldungen, abgegebene Angebote oder Rezepturen entstehen kann.[4]

Da Datenschutz- und Informationssicherheitsvorfälle je nach deren Ausprägung unterschiedliche Risiken bergen und unterschiedlich schwere Folgen auslösen können, welche wiederum unterschiedliche Maßnahmen erfordern, obliegt es dem Verantwortlichen nach Kenntnis eines Datenschutz- oder Informationssicherheitsvorfalls eine Risikoeinschätzung vorzunehmen, auf Basis derer Abhilfemaßnahmen zu treffen sind.

2. Was wird im Rahmen des Vorfallmanagements dokumentiert?

Voraussetzung dafür, dass Vorfälle analysiert, bewertet und gemeldet werden können und dass Maßnahmen zur Schadensbegrenzung und Strafverfolgung daraus abgeleitet werden können, ist Angaben über eine mögliche Aufklärung des Vorfalls zu erfassen und zu speichern. Dazu zählen E-Mails, Notizen über Gespräche und Analyseergebnisse, Meldezeitpunkte und Melder, Listen betroffener Systeme, geschädigter Personen oder Unternehmen sowie Beweismittel wie gefälschte E-Mails und Protokolldaten. Vorfälle müssen möglichst nach einem standardisierten Verfahren dokumentiert werden.[5]

Neben dem unmittelbaren Zweck den Vorfall selbst bearbeiten zu können erfüllt die Dokumentation viele weitere Zwecke. Sie ist die Grundlage einer eventuellen späteren straf- oder zivilrechtlichen Verfolgung von Schadensverursachern. Sie ermöglicht es bei neuerlichen Vorfällen Parallelen zu erkennen und in einer Nachbearbeitung zu erkennen, ob IT, Regelungen oder Unternehmensprozesse anzupassen sind. Und sie dient nicht zuletzt, vor allem bei den gesetzlich geregelten Meldepflichten, dem Nachweis des korrekten Handelns gegenüber Dritten.

Art. 5 Abs. 2 i.V.m. Art. 24 Abs. 1 DSGVO erlegt dem Verantwortlichen die Pflicht zur Dokumentation von Datenschutzvorfällen auf.[6] Dies soll vor allem die Aufsichtsbehörde zur Kontrolle der Einhaltung rechtlicher Vorgaben befähigen.[7] Wichtig ist hierbei vor allem die Umstände des Vorfalls, der ergriffenen Maßnahmen und des eingetretenen Schadens zu dokumentieren. Insbesondere sollten jegliche vorgenommene Abwägungen Teil der Dokumentation sein.[8] Kurz gesagt, es muss der Nachweis erfolgen, dass im Rahmen des Vorfallmanagements alles Erforderliche getan wurde, um den Schutz der betroffenen Personen und der relevanten Daten zu erreichen.

[4] Hanschke, Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten, S. 2.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2021.pdf?__blob=publicationFile&v=2

[6] Weitere Verpflichtungen – sowohl in Bezug auf die Notwendigkeit eines Vorfallmanagements, weiterer Meldepflichten sowie zur Dokumentation von Vorfällen – können sich unter anderem aus dem BSIG, dem GHB und dem KonTraG ergeben.

[7] Brink, in: Wolff/ Brink, BeckOK Datenschutzrecht, Art. 33, Rn. 62.

[8] Strüve, Datenschutz in der ärztlichen Praxis, 13.5.

Im Rahmen der Rechenschaftspflicht ist es für den Verantwortlichen vorteilhaft alle für diesen Nachweis gegenüber der Aufsichtsbehörde möglicherweise relevanten Daten zu speichern. Darunter befinden sich dann auch vielfältige Daten mit Personenbezug. Primär ist dies beim Dokumentieren der Umstände der Fall, etwa im Rahmen eines Vorfalltickets, welches in der Regel zum Zeitpunkt der internen Meldung eines Vorfalls erstellt wird. Enthalten sind hier die Kontaktdaten betroffener sowie meldender Personen wie Namen, Mail-Adressen und Telefonnummer. Betroffene Personen können hierbei solche sein, die den Vorfall ausgelöst haben oder von diesem in jeglicher Weise betroffen sind. So könnte beispielsweise ein Angriff auf die IT erfolgen, indem der Mailzugang eines Mitarbeiters gehackt wird und dann Mails von diesem Account aus an weitere Mitarbeiter gesendet werden.

Bei einer Dokumentation der Umstände könnten die Kontaktdaten aller Personen, welche eine Mail erhalten haben, sowie die Daten der gehackten Person oder ihres Rechners dokumentiert werden. Weitere personenbezogene Daten können bei der Dokumentation der weiteren Umstände des Vorfalls anfallen. Im Rahmen des unten angeführten Beispielsfalls könnte so die Mail abgespeichert werden, die den Schadcode enthält.

Bei der Beurteilung eines Vorfalls können ebenfalls personenbezogene Daten dokumentiert werden. So wird zwischen den zuständigen Mitarbeitern ein Mailverkehr über den Vorfall entstehen, in denen sie die Umstände des Vorfalls diskutieren. Es kann auch zu Gesprächen kommen, die protokolliert werden. Nach Abschluss des Managements eines konkreten Vorfalls liegt somit eine umfassende Dokumentation der Vorfallbearbeitung vor, die in der Regel eine ganze Reihe personenbezogene Daten enthält.

3. Was ist hinsichtlich der Aufbewahrung und Löschung personenbezogener Daten zu beachten?

Aus Sicht des Datenschutzrechts trifft den Verantwortlichen die Pflicht personenbezogene Daten zu löschen oder zu anonymisieren, wenn diese für die vor der Datenerhebung definierten Verarbeitungszwecke nicht mehr erforderlich sind (Art. 5 Abs. 1 lit. e DSGVO). Dies betrifft auch diejenigen personenbezogenen Daten, die im Rahmen der Dokumentation des Vorfallmanagements verarbeitet werden.

Entgegen dieser Pflicht zur Löschung personenbezogener Daten können unter anderem Gesetze, Kollektivvereinbarungen oder Individualverträge die Pflicht zur Aufbewahrung für einen bestimmten Zeitraum vorschreiben. Beispiele hierfür sind § 147 AO, §§ 238, 257 HGB.[9]

Dementsprechend hat der Verantwortliche Regeln festzulegen, die die Speicherdauer personenbezogener Daten auf das erforderliche Mindestmaß beschränken und trotzdem die einschlägigen gesetzlichen Aufbewahrungspflichten umsetzen. Hierbei ist zu beachten, dass – sofern für ein personenbezogenes Datum mehrere gesetzliche Aufbewahrungsfristen einschlägig sind – dieses Datum bis zum Ablauf der längsten einschlägigen Aufbewahrungsfrist zu speichern ist.[10]

Die Bildung von Löschregeln kann auf Basis der in der DIN 66398 beschriebenen Vorgehensweise erfolgen. Der Zweck der Vorgehensweise ist es, den rechtskonformen Löschzeitpunkt personenbezogener Daten (technikneutral) festzulegen.[11] Für die Entwicklung von Löschregeln wird der Datenbestand eines Verantwortlichen zunächst in Datenarten unterteilt. Für jede Datenart wird darauf folgend eine Löschregel definiert. Diese berücksichtigt

[9] Grothe, in Säcker/ Rixecker/ Oetker/Limperg, Münchener Kommentar zum BGB, § 195 Rn. 4; Macit/Selzer, BvD-News 1/20, 53, 54.

[10] Enzmann/Selzer/Spychalski, EDPL 2018, 416, 417.

[11] Hammer, in Jandt/Steidle, Datenschutz im Internet, S. 420.

- den erforderlichen Verarbeitungszeitraum zur datenschutzrechtlichen Zweckerreichung,
- die gegebenenfalls bestehenden Aufbewahrungspflichten und
- die datenschutzrechtlich vertretbare Frist zur Umsetzung der Löschung nach Ablauf der beiden vorgenannten Zeiträume.[12]

4. Was ist bei der Festlegung von Löschregeln für die Vorfalldokumentation zu beachten?

Auch für personenbezogene Daten, die im Rahmen der Dokumentation des Vorfallmanagements verarbeitet werden, müssen Verantwortliche Löschregeln festlegen. Hierbei ist zu betonen, dass für die Bildung von Löschregeln alle für einen bestimmten Verantwortlichen in diesem Zusammenhang relevanten Umstände berücksichtigt werden müssen. Nötig ist also eine *Einzelfallbetrachtung*. Dementsprechend erfolgt die nachfolgende Diskussion *exemplarisch*.

4.1 Festlegung des erforderlichen Zeitraums zur Zweckerreichung

Bei der Entwicklung von Löschregeln für das Vorfallmanagement liegt die wohl größte Herausforderung in der Festlegung des erforderlichen Verarbeitungszeitraums zur datenschutzrechtlichen Zweckerreichung. Die datenschutzrechtlichen Zwecke der Verarbeitung personenbezogener Daten im Rahmen des Vorfallmanagements bestehen regelmäßig darin den Vorfall zu bearbeiten, bestehende Melde- und Benachrichtigungspflichten zu erfüllen, Schutzmaßnahmen zur Verhinderung von Folgeschäden zu implementieren und den Rechenschaftspflichten und der Beweissicherung nachzukommen.

Verantwortliche stehen hierbei insbesondere vor der Herausforderung zu bewerten, wie lange personenbezogene Daten für die Zweckerfüllung der Rechenschaftspflichten verarbeitet werden dürfen. Im Rahmen des Art. 5 Abs. 2 i.V.m. Art. 24 Abs. 1 DSGVO wird keine zeitliche Grenze festgelegt, bis zu welcher der Verantwortliche die Daten zum Nachweis aufbewahren sollte. Sinnvoll erscheint es, die Haftungsvermeidung als Ausgangspunkt der notwendigen Aufbewahrungsdauer heranzuziehen. Hierbei liegt es im Interesse des Verantwortlichen, mögliche Bußgelder abzuwehren, indem die Konformität seines Handelns durch eine umfangreiche Dokumentation nachgewiesen werden kann. So drohen i.S.d. Art. 83 Abs. 5 lit. a DSGVO Bußgelder bei Verstößen gegen die Grundsätze der Verarbeitung gemäß Art. 5 DSGVO.

Im Rahmen der DSGVO wird jedoch keine konkrete Verjährungsfrist vorgegeben. Das BDSG legt in § 41 Abs. 2 die Anwendbarkeit des OWiG im Fall von Verstößen gegen Art. 83 Abs. 4 bis 6 DSGVO fest. So verjährt eine Verletzung der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO gemäß Art. 83 Abs. 5 lit. a DSGVO i.V.m. § 31 Abs. 2 Nr. 1 OWiG spätestens nach drei Jahren. Die Frist beginnt i.S.d. § 31 Abs. 3 OWiG mit dem Abschluss der Handlung, die die Ordnungswidrigkeit begründet und damit am Tag der Tat.[13]

Nach Ablauf dieser Frist können Verstöße aufgrund der Verfolgungsverjährung nicht mehr geahndet werden.[14] Ein weiterer in diesem Zusammenhang zu berücksichtigender Faktor ist die Beweislast bei Schadenersatzansprüchen betroffener Personen nach Art. 82 DSGVO, welcher der Verantwortliche im Rahmen der Rechenschaftspflicht unterliegt.

Schadenersatzansprüche aus Art. 82 DSGVO verjähren gem. § 195 BGB regelmäßig innerhalb von drei Jahren.[15] Die regelmäßige Verjährungsfrist beginnt i.S.d. § 199 Abs. 1 BGB mit dem Ende des Jahres, in dem der Anspruch entstanden ist oder von ihm Kenntnis erlangt wurde.

Zusätzlich kann im Rahmen der Beweissicherung unter anderem die Aufbewahrung zur Vermeidung einer Produkthaftung auf Grundlage des ProdHaftG notwendig werden. Hierbei liegt eine verschuldensunabhängige Gefährdungshaftung vor, auf Basis derer Schadenersatz geltend gemacht werden kann. Dieser Anspruch verjährt i. S. d. § 12 Abs. 1 ProdHaftG innerhalb von drei Jahren ab Kenntnis des Ersatzberechtigten, oder ab dem Zeitpunkt, in dem Kenntnis hätte erlangt werden müssen. Auch können sich Aufbewahrungspflichten

[12] Weiterführende Informationen zur Bildung von Löschregeln auf Basis der DIN 66398: Stummer/ Selzer, BvD-News 3/19, 26, 26 u. 29; Macit/Selzer, BvD-News 1/20, 53, 54 f.
[13] Ellbogen, in: Karlsruher Kommentar zum OwiG, § 31, Rn. 23.
[14] Voigt, in: Taeger/ Gabel, DSGVO BDSG, Art. 5 DSGVO, Rn. 44 f.; Schantz, in: BeckOK Datenschutzrecht, Art. 5 DSGVO, Rn 39; Herbst, in: Kühling/ Buchner, DS-GVO BDSG, Art. 5 DSGVO, Rn. 80.
[15] Frenzel, in: Paal/ Pauly, DS-GVO BDSG, Art. 82 DSGVO, Rn. 19; Voigt, in: Taeger/ Gabel, DSGVO BDSG, Art. 5 DSGVO, Rn. 44 f.

aus mit Kooperationspartnern oder – insbesondere im Forschungsumfeld – mit Projektfördergebern geschlossenen Verträgen ergeben.

4.2 Aufbewahrungspflichten

Darüber hinaus ist zu prüfen, ob einer Löschung personenbezogener Daten in Vorfalldokumentationen Aufbewahrungspflichten entgegenstehen. In der vorliegenden, exemplarischen Betrachtung gehen die Autorinnen und der Autor davon aus, dass keine solche Aufbewahrungspflichten für die Vorfalldokumentation bestehen.

4.3 Datenschutzrechtlich vertretbare Frist zur Umsetzung der Löschung

Schließlich ist die datenschutzrechtlich vertretbare Frist zur Umsetzung der Löschung nach Ablauf der Zweckerreichung und etwaiger bestehender Aufbewahrungspflichten zu ermitteln. Die Speicherung der Vorfalldokumentation erfolgt häufig im Rahmen eines Ticketsystems, in dem eine Löschung oft händisch erfolgen muss. Die Bestimmung der vertretbaren Frist zur Löschung sollte diesen Umstand berücksichtigen.

Darüber hinaus ist das Risiko, das von der Datenspeicherung für die Rechte und Freiheiten der betroffenen Personen ausgeht zu berücksichtigen. Für die Speicherung der Daten im Rahmen des Vorfallmanagements liegt ein geringes bis maximal mittleres Risiko vor. In der Gesamtschau handelt es sich bei der Mehrzahl der personenbezogenen Daten um Stammdaten. Die Speicherung solcher Daten stellt ein eher geringes Risiko dar. Sensible Daten, welche eines höheren Schutzes bedürfen, kommen in der Regel nicht vor, oder höchstens in verhältnismäßig geringem Umfang im Rahmen von Freitextfeldern oder Anhängen. Die Sicherheit der sensiblen Daten wird hierbei meist durch technische und organisatorische Maßnahmen wie restriktive Berechtigungskonzepte und Verschlüsselungen erhöht.[16] Damit kann die Eintrittswahrscheinlichkeit der Risiken für die Rechte und Freiheiten betroffener Personen gesenkt werden, welche sich aus der Speicherung ergeben könnten.

Unter Berücksichtigung der Risikobewertung, sowie der Verhältnismäßigkeit der Maßnahmen zur Löschung zugunsten des Verantwortlichen, sollten die Prozesse zur tatsächlichen Umsetzung der Löschung nicht länger als ein Jahr dauern.

Beispielhafte Löschregel für die Vorfalldokumentation[17]	
Inhaltlicher Umfang	Die Löschregel umfasst alle Datenobjekte, die im Rahmen des Vorfallmanagements gespeichert werden, um Vorfälle ab deren Meldung zu bearbeiten.
Verwendungszwecke	• Bearbeitung des Vorfalls • eventuell Erfüllung von Melde- und Benachrichtigungspflichten • eventuell Ergreifen von Schutzmaßnahmen zur Verhinderung von Folgeschäden • Rechenschaftspflichten und Beweissicherung - Art. 5 Abs. 2 DSGVO i.V.m. § 195 BGB, § 31 Abs. 2 Nr. 1 OWiG - § 12 ProdHaftG
Zeitraum bis zur vollständigen datenschutzrechtlichen Zweckerreichung	Vollständiger Abschluss der Vorfallbearbeitung und Ablauf aller relevanter Verjährungsfristen (meist nach drei Jahren ab dem Ende des Jahres, in dem der Anspruch entstanden ist).
Aufbewahrungspflichten	-
Frist zur Umsetzung der Löschung	1 Jahr

Tabelle 1: Löschregel für die Datenschutz- und Informationssicherheitsvorfalldokumentation

[16] Stummer/Selzer, BvD-News 3/19, 26, 29.

[17] Die Tabelle ist angelehnt an die DIN 66398, jedoch stark vereinfacht und verkürzt.

5. Wie kann eine Löschregel für die Vorfalldokumentation aussehen?

Wie bereits betont ist die Bildung von Löschregeln abhängig von branchenspezifischen rechtlichen Vorgaben zur Aufbewahrung und muss unter allen für die Organisation/das Unternehmen relevanten Umstände vorgenommen werden. Insofern stellen die Autorinnen und der Autor dieses Beitrags nachfolgend eine *exemplarische* Löschregel vor, die eine Orientierung für eine Vielzahl von Organisationen sein dürfte, jedoch keine branchen- und organisationsspezifischen Anforderungen abbildet.

Es ist grundsätzlich möglich im begründeten Ausnahmefall von einer zuvor definierten Löschregel abzuweichen, zum Beispiel im Falle eines noch offenen Rechtsstreits (etwa Strafverfolgung eines Angreifers) für den die Vorfalldokumentation als Beweismittel dienen soll. Für diese Fälle muss individuell geklärt werden, ob und wie lange die vordefinierte Löschregel der Vorfalldokumentation überschritten werden muss oder darf. Dieser Schritt sollte wiederum dokumentiert werden.

Über die Autor*innen

Louisa Rudolph
Informationsjuristin (LL.B.), E-Mail:
louisa.rudolph@zv.fraunhofer.de

Dr. Annika Selzer
Gruppenleiterin für Informationsrecht und interdisziplinäre Recht-Technik-Forschung am Fraunhofer-Institut für Sichere Informationstechnologie (SIT), E-Mail:
annika.selzer@sit.fraunhofer.de

Dr. Ulrich Pordesch
Bereichsleiter für Sicherheit der Fraunhofer Gesellschaft, Informationssicherheits- und Datenschutzkoordinator der Fraunhofer-Gesellschaft, E-Mail:
ulrich.pordesch@zv.fraunhofer.de

▶ www.sit.fraunhofer.de

Fraunhofer SIT