Der Bayerische Landesbeauftragte
für den Datenschutz

Datenschutz bei der Nutzung von Telefax-Diensten

Arbeitspapier

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Inhalt

Bearbeiterin: Angelika Müller

Version 1.0 | Stand: 1. Februar 2022

Dieses Arbeitspapier wird ausschließlich in elektronischer Form bereitgestellt. Es kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Der Versand personenbezogener Daten per Telefax (im Folgenden kurz: Fax) ist mit erheblichen Risiken behaftet, was das Gewährleistungsziel[1] „Vertraulichkeit“ betrifft. Auf diesen Umstand weisen die Datenschutz-Aufsichtsbehörden schon seit Jahren hin. Gerade die COVID-19-Pandemie hat gezeigt, wie relevant das Thema noch immer ist. Vor diesem Hintergrund stellt der Bayerische Landesbeauftragte für den Datenschutz ein sowohl hinsichtlich der Methodik als auch hinsichtlich der technischen Gegebenheiten aktualisiertes Arbeitspapier bereit.[2] Das Papier bietet bayerischen öffentlichen Stellen (Verantwortlichen) Bausteine einer Risikoanalyse und zeigt risikomindernde Maßnahmen auf, die bei der Kommunikation mittels Fax zu beachten sind. 1

Das Arbeitspapier ist auf die Darstellung der Risiken und risikomindernden Maßnahmen bezüglich des Gewährleistungsziels „Vertraulichkeit“ fokussiert. Der Verlust der Verfügbarkeit und Integrität sowie die Einhaltung weiterer Gewährleistungsziele nach dem Standarddatenschutzmodell werden nicht vertieft behandelt, da die Hauptrisiken der Nutzung von Telefaxdiensten bereits anhand des Gewährleistungsziels „Vertraulichkeit“ dargestellt werden können. 2

Der vorgenommenen Risikobewertung liegt die Methodik der Risikobewertung aus meiner Orientierungshilfe zur Datenschutz-Folgenabschätzung zugrunde.[3] Tabelle 1 „Möglicher Grad der Eintrittswahrscheinlichkeit“, Tabelle 2 „Möglicher Grad der Schwere/des Schadens“ und Tabelle 3 „Risikobewertung: Risikomatrix und Risikoindex“ befinden sich im Anhang. Sind im Rahmen der Risikobewertung die Schwere des Schadens und die Eintrittswahrscheinlichkeit festgelegt, wird das Risiko anhand Tabelle 3 ermittelt. Wird ein relevantes Risiko (gelb) oder ein hohes Risiko (rot) festgestellt, sind Maßnahmen zur Risikoreduzierung erforderlich. 3

Unabhängig von der hier dargestellten Risikoanalyse sollten die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen des IT-Grundschutzes veröffentlichen Bausteine[4], die für die Nutzung von Telefaxdiensten wesentlich sind, Berücksichtigung finden: 4

– für die Nutzung herkömmlicher Faxgeräte und Faxserver: NET.4.3 „Faxgeräte und Faxserver“;

1 Zur Begrifflichkeit Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung, Methodik und Fallstudie, Stand 10/2019, S. 7 f., Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA“.

2 Das Arbeitspapier tritt an die Stelle der Hinweise „Datensicherheit beim Telefax-Dienst“, die bisher auf https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Technik und Organisation“ bereitgestellt waren.

3 Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung, Stand 2/2021, sowie Datenschutz-Folgenabschätzung, Methodik und Fallstudie, Stand 10/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA“.

4 Internet: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html.

- für die Nutzung von Multifunktionsgeräten mit Faxfunktion: SYS.4.1 „Drucker, Kopierer und Multifunktionsgeräte“;
- sind die Telefonverbindungen bereits auf Voice-over-IP (VoIP) umgestellt: NET.4.2 „VoIP“.

5 Sollen auch nur vereinzelt Faxe mit sensiblen Inhalten versandt werden, sollten hierbei auch die Anforderungen an einen erhöhten Schutzbedarf berücksichtigt werden.

1. Risikoquellen und Maßnahmen

6 Der Faxversand kann in drei Phasen eingeteilt werden, in denen es zu einem Vertraulichkeitsverlust kommen kann. Im Folgenden werden sowohl für den Faxversand als auch für die Übertragung und den Faxempfang mögliche Risikoquellen und Maßnahmen zur Reduzierung des Risikos des Vertraulichkeitsverlusts dargestellt.

7 Vorab sei bereits die für eine Risikobeurteilung notwendige Schwere des Schadens erläutert, da diese für alle folgenden Risikoszenarien identisch ist:

8 Für die Bewertung der Schwere des möglichen Schadens muss mindestens zwischen Daten besonderer Kategorien im Sinne von Art. 9 Datenschutz-Grundverordnung (DSGVO) sowie Daten, die auf Grund anderer gesetzlicher Regelungen einem besonderen Schutzbedarf unterliegen (etwa auf Grund des Sozialgeheimnisses, im Folgenden: sensible personenbezogene Daten), auf der einen Seite und sonstigen personenbezogenen Daten auf der anderen Seite unterschieden werden, da der mögliche Grad der Schwere des Schadens auch vom Inhalt des Faxes abhängt. Tabelle 2 zeigt die Ausprägungen zum möglichen Grad der Schwere des Schadens.

- Sensible personenbezogene Daten:

  Bei sensiblen personenbezogenen Daten ist die Schwere des möglichen Schadens in der Regel mindestens als substanziell, wenn nicht sogar als groß einzustufen.

- Personenbezogene Daten:

  Die Schwere des Schadens kann nicht pauschal (in diesem Arbeitspapier) festgelegt werden, sondern muss vom Verantwortlichen anhand der Inhalte der zu versendenden Dokumente beurteilt werden. Sie kann von geringfügig bis groß eingestuft werden.

9 Das vorliegende Arbeitspapier beruht im Weiteren auf der typisierenden Annahme, dass bei einer Beeinträchtigung der Vertraulichkeit von sensiblen personenbezogenen Daten mindestens ein substanzieller Schaden droht. Sollte ein Verantwortlicher für eine Verarbeitung eine geringere Schwere des Schadens annehmen, müssen die dafür maßgeblichen Umstände eingehend dokumentiert werden, bevor sie in die eigene Risikoanalyse einfließen können.

2. Faxversand durch bayerische öffentliche Stellen

a) Versand

R.1 Risikoszenario: Fehlversand

Sowohl durch die Eingabe einer falschen Rufnummer, etwa durch Vertippen bei der Eingabe, als auch durch die Nutzung einer veralteten oder fehlerhaft hinterlegten Rufnummer kann es zu einer Fehlzustellung kommen. 10

Auch kann durch die Notwendigkeit der Vorwahl einer Ziffer oder Ziffernkombination für interne oder externe Faxe ein Fehlversand entstehen, wenn zwar die Rufnummer korrekt, aber die notwendige Vorwahl für interne oder externe Faxe falsch eingegeben oder vergessen wird (etwa die bei Nebenstellenanlagen vor einer externen Rufnummer zu wählende „0“). 11

Des Weiteren besteht die Möglichkeit, dass zwar der beabsichtigte Empfänger adressiert wird, allerdings ein falsches Schreiben versandt wird. 12

Risikobewertung

Auf Grund von zahlreichen Meldungen zu Fehlversendungen von Faxen ist nach den Erfahrungen der Datenschutz-Aufsichtsbehörden die Eintrittswahrscheinlichkeit für diesen Schadensfall als „groß“ (4) zu bewerten. Dies entspricht nach der in der Anlage wiedergegebenen Tabelle 1 „Möglicher Grad der Eintrittswahrscheinlichkeit“ der höchsten Risikostufe. 13

Aus der Risikomatrix ergibt sich somit für dieses Risikoszenario, dass unabhängig vom Grad der Schwere eines möglichen Schadens risikomindernde Maßnahmen ergriffen werden müssen. 14

Mögliche organisatorische Maßnahmen zur Risikominderung

Beschäftigte sollten etwa durch eine Dienstanweisung dazu verpflichtet werden, bei der Versendung von Faxen besondere Sorgfalt walten zu lassen. An diese Verpflichtung sollte durch regelmäßig wiederkehrende Sensibilisierungsmaßnahmen erinnert werden. Insbesondere sollten die folgenden Vorsichtsmaßnahmen vorgegeben werden: 15

- nochmalige Kontrolle der Faxnummer nach der Eingabe, falls möglich im Vier-Augen-Prinzip;
- bei Erstkontakt oder falls länger kein Kontakt bestand: Einholen der Bestätigung, dass die Faxnummer (noch) korrekt ist.

Mögliche technische Maßnahmen zur Risikominderung

Zudem sollten – soweit möglich – technische Maßnahmen umgesetzt werden. Hierzu gehört beispielsweise die Einspeicherung häufig verwendeter Faxnummern im Faxgerät oder – bei Versand über den PC – in einem Adressbuch. Das Adressbuch ist – nach Maßgabe der Infrastruktur beim Verantwortlichen – idealerweise zentral zu hinterlegen und zu pflegen. 16

b) Übertragungsweg

17 Der Übertragungsweg umfasst die Übertragung des Faxes

- vom Endgerät (Faxgerät, PC, Faxserver oder Router) des Senders zu dessen Provider,
- vom Provider des Senders zum Provider des Empfängers,
- vom Provider des Empfängers zum entgegennehmenden Gerät des Empfängers (Faxgerät, PC, Faxserver oder Router).

R.2 Risikoszenario: Unbefugtes Mitlesen auf dem Übertragungsweg

18 Viele Telefonverbindungen sind providerseitig inzwischen auf VoIP umgestellt. Da für die Übertragung von VoIP-Daten – je nach Telefonprovider des Absenders und Empfängers – eine Übertragung über das öffentliche Internet nicht zur Gänze ausgeschlossen werden und diese Übertragung unter Umständen sogar unverschlüsselt erfolgen kann, kann auf dem Übertragungsweg die Möglichkeit des unbefugten Mitlesens durch Angreiferinnen oder Angreifer bestehen. Im Übrigen wäre selbst bei einem unverschlüsselten Versand ausschließlich über Netze des Providers zumindest dieser in der Lage, den Inhalt der Faxe mitzulesen.

Risikobewertung

19 Für die Konfiguration der Endgeräte und der VoIP-Telefonanlage ist im Regelfall die hausinterne IT beziehungsweise ein IT-Dienstleister zuständig. Die Konfiguration ist maßgeblich für die Verbindungssicherheit zum Provider des Senders und vom Provider des Empfängers zum Empfänger. Anbieter von Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten unterliegen der Aufsicht der Bundesnetzagentur und damit deren Sicherheitsanforderungen. Die Bundesnetzagentur fordert an sicherheitsrelevanten Stellen eine Verschlüsselung von Daten nach dem Stand der Technik.[5] Die nachfolgende Aufstellung folgt dem Übertragungsweg. Der Sender hat für seine Infrastruktur die in Rn. 4 erwähnten Bausteine umgesetzt und einen Telekommunikationsanbieter beauftragt, welcher der Aufsicht durch die Bundesnetzagentur unterliegt.

1 Vom Sendegerät zum Provider des Senders

Typisierende Betrachtung der Eintrittswahrscheinlichkeit:

Für die Risikobewertung kann hier die Erfüllung der in Rn. 4 genannten IT-Grundschutz-Bausteine herangezogen werden. Sind sowohl die Standard-Anforderungen wie auch die Anforderungen für einen erhöhten Sicherheitsbedarf erfüllt, so kann von einer Eintrittswahrscheinlichkeit „geringfügig“ (1) für diesen Teil des Übertragungswegs ausgegangen werden.

[5] Näher Bundesnetzagentur, Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG), Version 2.0, Stand 4/2020, Internet: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Unternehmenspflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Sicherheitsanforderungen.

2 Vom Provider des Senders zum Provider des Empfängers

Typisierende Betrachtung der Eintrittswahrscheinlichkeit:

Szenario 1: Sender und Empfänger haben Telekommunikationsanbieter beauftragt, die der Aufsicht durch die Bundesnetzagentur unterliegen.

Vor dem Hintergrund der Aufsicht der Provider durch die Bundesnetzagentur ist anzunehmen, dass jedenfalls große Telekommunikationsanbieter sowohl bei der Übertragung im eigenen Netz als auch bei der Übertragung aus dem eigenen Netz zum Netz des Empfangsproviders für eine angemessene Transportverschlüsselung sorgen, und dass sie in der Rolle eines Empfangsproviders transportverschlüsselte Faxe entgegennehmen können.

Szenario 2: Der Sender hat einen Telekommunikationsanbieter beauftragt, welcher der Aufsicht durch die Bundesnetzagentur unterliegt. Über den Telekommunikationsanbieter des Empfängers ist dem Sender nichts Näheres bekannt.

Es ist unklar, ob der Empfangsprovider ausreichende Sicherheitsmaßnahmen getroffen hat. Insbesondere kann ein Fax-Cloud- oder ein Fax2Mail-Dienst eingesetzt sein, der nicht zwangsläufig die Standards der Bundesnetzagentur erfüllen muss.

Szenario 2.1: Der Empfänger ist eine öffentliche Stelle.

Grundsätzlich ist die Annahme statthaft, dass ein großer Telekommunikationsanbieter beauftragt ist. Dann darf die Eintrittswahrscheinlichkeit für ein unbefugtes Mitlesen auf der Übertragungsstrecke, für die Sende- und Empfangsprovider zuständig sind, grundsätzlich als „geringfügig“ (1) eingestuft werden.

Szenario 2.2: Der Empfänger ist eine nicht öffentliche Stelle oder eine Privatperson.

Zunächst kann keine Annahme zum Sicherheitsniveau beim Empfangsprovider getroffen werden. Gerade bei Privatpersonen kommt oftmals kein „klassisches“ Faxgerät zum Einsatz; verbreitet sind hier auch Empfangsmöglichkeiten über E-Mail-Provider. Auch wenn bisher aus Meldungen nach Art. 33 DSGVO sowie der Fachpresse keine Angriffe bekannt geworden sind, bei denen Dritte auf der vom Sende- oder Empfangsprovider verantworteten Strecke Inhalte mitgelesen hätten, ist die Eintrittswahrscheinlichkeit für dieses Risiko mindestens als „überschaubar“ (2) einzustufen.

3 Vom Provider des Empfängers zum Empfangsgerät

Typisierende Betrachtung der Eintrittswahrscheinlichkeit:

Szenario 3.1: Über die Telefonanlage und/oder die Empfangsgeräte beim Empfänger ist nichts Näheres bekannt.

Ohne nähere Kenntnis der Verhältnisse beim Empfänger sollte die Eintrittswahrscheinlichkeit mindestens als „überschaubar“ (2) eingestuft werden.

Szenario 3.2: Der Empfänger hat für seine Infrastruktur die in Rn. 4 erwähnten IT-Grundschutz-Bausteine umgesetzt.

Soweit sich der Sender darüber vergewissern konnte, dass der Empfänger die erforderlichen Sicherheitsmaßnahmen getroffen hat, kann die Eintrittswahrscheinlichkeit als „geringfügig“ (1) gewertet werden.

Um die **Eintrittswahrscheinlichkeit** für den gesamten Übertragungsweg festzulegen, wird als „Worst-Case-Szenario“ die höchste Eintrittswahrscheinlichkeit aus den drei Teilübertragungswegen angenommen. 20

21 Wann ein relevantes Risiko (gelb) erreicht wird, hängt von der **Schwere des Schadens** ab (siehe Tabellen 2 und 3): Bei einem relevanten Risiko (gelb) sind risikomindernde Maßnahmen zu ergreifen und zu dokumentieren. Für sensible Daten ist dies somit obligatorisch.

Mögliche Maßnahmen zur Risikominderung

Reduzierung möglicher Grad der Schwere des Schadens:

22 – Beim Versand von sensiblen Inhalten sollte überprüft werden, ob es andere geeignete Übertragungsmöglichkeiten gibt (bei Eilbedürftigkeit insbesondere eine Ende-zu-Ende-verschlüsselte E-Mail oder eine bereits im Vorfeld etablierte Nutzung einer sicheren Cloud-Ablage, ansonsten auch der postalische Weg).

23 – Es können identifizierende personenbezogene Merkmale durch ein Pseudonym ersetzt und die Zusammenführung von Pseudonymen und Content-Daten auf einem getrennten Weg (etwa durch Telefon) durchgeführt werden. Dies stellt allerdings einen erheblichen organisatorischen Aufwand dar.

Reduzierung Eintrittswahrscheinlichkeit:

24 – Bereits die Umsetzung der Standardmaßnahmen aus den in Rn. 4 genannten Maßnahmen wirkt sich mindernd auf die Eintrittswahrscheinlichkeit für den ersten Teil des Übertragungswegs aus. Die Umsetzung der Anforderungen an einen erhöhten Schutzbedarf wirkt sich weiter risikomindernd aus; insbesondere sorgt die Aktivierung von SRTP (Baustein NET.4.2.A15 Sicherer Medientransport mit SRTP (H) für eine Stärkung des Gewährleistungsziels „Vertraulichkeit“ (siehe Rn. 1 ff.).

25 – Soll ein regelmäßiger Faxaustausch etabliert werden, können Informationen zum Provider des Empfängers eingeholt werden. Ist dies ebenfalls ein großer Telekommunikationsdienstleister, der die Standards der Bundesnetzagentur erfüllen muss, wirkt sich dies mindernd auf die Eintrittswahrscheinlichkeit aus.

26 – Ebenso können in diesem Fall Informationen über den Umsetzungsstand der drei in Rn. 4 genannten IT-Grundschutz-Bausteine eingeholt werden.

27 – Im Hinblick auf Einzelempfänger, mit denen häufig Faxe ausgetaucht werden sollen, können auch risikomindernde Maßnahmen im Bereich der Übertragungstechnik getroffen werden. So können beispielsweise die Empfänger und deren Provider auf die dort umgesetzten Sicherheitsmaßnahmen überprüft werden, oder es kann eine Ende-zu-Ende-Verschlüsselung etabliert werden.

28 **Hinweis:** Da diese Maßnahmen nicht in jedem Empfangsszenario umsetzbar sind, ist im Einzelfall eine Abwägung erforderlich. Eine Nutzung von Telefaxdiensten trotz Risiken für die Vertraulichkeit personenbezogener Daten sollte nur dann in Betracht gezogen werden, wenn ohne den Fax-Einsatz ein Schaden für hochwertige Rechtsgüter droht. Insbesondere im Fall des Versands sensibler personenbezogener Daten sollte die Nutzung der Faxtechnik Ultima Ratio sein (Beispiel: Nachteile für die Gesundheit, wenn ein dringend benötigter Laborbefund übermittelt werden soll, ein gleich schnelles, sichereres Kommunikationsmittel aber nicht zur Verfügung steht). Alle in diesem Arbeitspapier aufgeführten und umsetzbaren Maßnahmen

sollten ergriffen worden sein, und es sollte eine Einwilligung des Betroffenen eingeholt werden. Die Abwägung sollte dokumentiert werden.

c) Empfang

R.3 Risikoszenario: Unbefugter Zugriff auf ausgedrucktes Fax

Ein klassisches Faxgerät bzw. ein Multifunktionsgerät, das empfangene Faxe direkt ausdruckt, steht häufig an einem Ort, an dem mehrere Beschäftigte der empfangenden Stelle bzw. Mitglieder eines Haushalts Zugriff haben. Somit kann die unbefugte Kenntnisnahme eines Faxes möglich sein. 29

Risikobewertung

Zumeist ist die Situation beim Empfänger nicht bekannt. Sicherlich kann nicht generell angenommen werden, dass Faxgeräte immer an geeigneten (insbesondere ausreichend zugangsbeschränkten) Stellen situiert sind. Deshalb ist die Eintrittswahrscheinlichkeit zunächst als mindestens „überschaubar“ (2) zu bemessen. 30

Aus der Risikomatrix ergibt sich somit für dieses Risikoszenario, dass spätestens ab einer Schwere von „überschaubar“ (2) risikomindernde Maßnahmen ergriffen werden müssen. Für sensible Daten ist dies somit obligatorisch. 31

Mögliche Maßnahmen zur Risikominderung

Der Absender kann mit dem Empfänger die Situation des Telefax-Zugangs abklären. Er kann sich dabei Gewissheit verschaffen, dass der Empfänger ausreichende dem Gewährleistungsziel „Vertraulichkeit“ (siehe Rn. 1 ff.) dienende Maßnahmen ergriffen hat (etwa das Empfangsgerät in einem dem Publikum nicht zugänglichen, verschlossen gehaltenen Raum vorgehalten wird, oder – bei bayerischen öffentlichen Stellen als Empfängern – datenschutzrechtlich abgeschirmte Organisationseinheiten wie etwa die Personalstelle, vgl. Art. 103 Satz 1 Bayerisches Beamtengesetz, über exklusiv genutzte Empfangsgeräte verfügen). Die möglichst am Beginn eines regelmäßigen Faxverkehrs stehende Abklärung sollte dokumentiert werden. 32

3. Faxempfang durch bayerische öffentliche Stellen

Vor allem wenn ein Verantwortlicher den Faxempfang als Kommunikationsform für den Empfang von personenbezogenen Daten zur Verfügung stellt, muss auch dieses Szenario betrachtet werden. Hierbei sind die beiden Phasen „Übertragungsweg“ und „Empfang“ gesondert zu betrachten. 33

a) Übertragungsweg

Die Übertragung ist bereits unter Rn. 17 ff. erläutert; die dort dargelegten Grundsätze sind auch im vorliegenden Zusammenhang maßgeblich. Es sollten entsprechend sichere Anbindungen genutzt werden. 34

b) Empfang

R.4 Risikoszenario: Unbefugter Zugriff auf ausgedrucktes Fax

35 Je nach Größe und Ausstattung eines Verantwortlichen werden eingehende Faxe an einer zentralen Poststelle, an mehreren Stellen (beispielsweise pro Organisationseinheit) oder sogar (zumeist per interner E-Mail) direkt an die Empfänger zugestellt.

36 Werden eingehende Faxe mit personenbezogenen Daten angefordert oder wird die Kommunikation per Fax ermöglicht, so sollte der Verantwortliche mindestens dokumentieren, in welchen Geschäftsprozessen Faxe für den Empfang von personenbezogenen Daten aktiv angefordert oder entgegengenommen werden und dies in eine Risikoanalyse einbeziehen.

37 Eine allgemeine Risikoanalyse kann im Rahmen dieses Arbeitspapiers nicht erfolgen. Die Eintrittswahrscheinlichkeit sowie die Schwere eines möglichen Schadens hängen von mehreren Faktoren ab. Insbesondere müssen der erwartete Inhalt der Faxe sowie die Empfangssituation bewertet werden, vor allem im Hinblick auf die Frage, welcher Personenkreis auf eingehende Faxe zugreifen kann.

38 Beschäftige bayerischer öffentlicher Stellen sind zur Verschwiegenheit verpflichtet, allerdings gilt auch für eingehende Faxe das Erforderlichkeitsprinzip. Demnach dürfen nur diejenigen Beschäftigten von Daten Kenntnis erlangen, die diese auch für die Ausübung ihrer Tätigkeit benötigen. Bei der Wahl des Aufstellungsortes für das Faxgerät dürfen Zugangsmöglichkeiten des Publikums oder externer Dienstleister nicht außer Acht gelassen werden, die eine unbefugte Kenntnisnahme von Faxen erleichtern können.

39 Risikomindernde Maßnahmen lassen sich hier nicht abschließend formulieren. Zumindest folgende Maßnahmen können ergriffen werden:

Mögliche Maßnahmen zur Risikominderung

40 – Es sollte eine Dienstanweisung zur Beschaffung und Aufstellung von Faxgeräten vorhanden sein, die die Anforderungen des Datenschutzes beachtet und umsetzt.

41 – Für jedes Faxgerät sollten der Standort und die Zugriffsmöglichkeiten durch Beschäftigte und Publikum geprüft werden. Diese Prüfung sollte dokumentiert werden.

42 – Sind Prozesse zum internen Datenaustausch via Fax etabliert, sollten diese Prozesse auf Alternativverfahren zur Kommunikation überprüft werden. Intern könnte sogar auf unverschlüsselte E-Mails ausgewichen werden, wenn sichergestellt wird, dass die E-Mails den E-Mail-Server des Verantwortlichen nicht verlassen und dieser ausreichend geschützt ist.

R.5 Risikoszenario: Empfang von fehladressierten Faxen

43 Auch wenn für die korrekte Eingabe der Rufnummer der Absender zuständig ist, kann ein Verantwortlicher, der den Faxempfang als Möglichkeit zur Kontaktaufnahme anbietet, die Wahrscheinlichkeit der Fehlversendung durch den Absender reduzieren:

Allgemeine Maßnahmen zur Risikominderung für die Einrichtung des Faxempfangs

Ist das Faxgerät an eine Nebenstellenanlage angeschlossen, kann eine Nebenstellennummer verwendet werden, die möglichst wenig Spielraum für Fehleingaben durch den Absender zulässt (Vermeidung ähnlicher Fax-Nummern bei anderen Stellen). 44

4. Erfüllung der Rechenschaftspflicht

a) Dokumentation

Folgende Dokumente sollte der Verantwortliche, der einen Telefaxdienst nutzt, zur Erfüllung seiner Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) mindestens vorhalten: 45

- eine Dokumentation über die Standorte seiner Faxgeräte einschließlich Angaben zu Maßnahmen, mit denen unbefugte Zugriffe verhindert werden sollen;
- eine Dienstanweisung zur Beschaffung und Aufstellung von Faxgeräten;
- eine Dienstanweisung zur Nutzung von Fax als Kommunikationsmittel;
- eine einzelfallbezogene Dokumentation zu Faxen, die aus Eilbedürftigkeit trotz hohem Risiko verschickt werden. Diese Dokumentation sollte formularmäßig und zentral geführt werden; sie dient nicht nur der Erfüllung der Rechenschaftspflicht des Verantwortlichen, sondern auch dessen Planung, was die Gestaltung häufig benötigter Kommunikationsbeziehungen betrifft;
- Risikoanalyse zum Versand von Faxen mit sensiblen Inhalten. Diese sollte mit dem behördlichen Datenschutzbeauftragten abgestimmt sein.

b) Protokollierung

Kommunikationsjournale zu ausgehenden Faxen sollten für einen gewissen Zeitraum (etwa 14 Tage) aufbewahrt werden, um Fehlsendungen nachgehen zu können und erforderlichenfalls einen falschen Adressaten kontaktieren zu können. Parallel zur Festlegung einer passenden Aufbewahrungsfrist für diesen Zweck ist eine Löschung bzw. Vernichtung der Kommunikationsjournale sicherzustellen. 46

5. Fazit

Da der Versand von personenbezogenen Daten per Fax mit verschiedenen Risiken behaftet ist, sollten die hier aufgeführten Maßnahmen umgesetzt werden. Sollen sensible personenbezogene Daten per Fax versandt werden, ist zusätzlich in einer Risikoanalyse zu prüfen, ob die Risiken durch risikomindernde Maßnahmen derart gesenkt werden können, dass ein Versand möglich ist. Bayerische öffentliche Stellen haben bei einer Kommunikation per Fax diverse Dokumentationspflichten zu erfüllen. 47

Anhang[6]

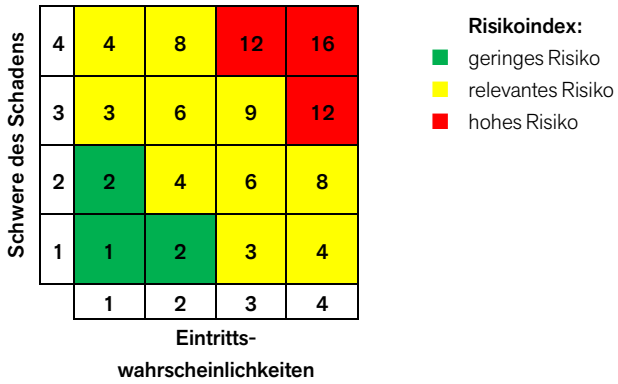
Tabelle 1: Möglicher Grad der Eintrittswahrscheinlichkeit

Grad	Bezeichnung	Beschreibung
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.
3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich zu sein.

Tabelle 2: Möglicher Grad der Schwere des Schadens

Grad	Bezeichnung	Beschreibung
1	geringfügig	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
2	überschaubar	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
3	substanziell	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.
4	groß	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

Tabelle 3: Risikobewertung: Risikomatrix und Risikoindex



[6] Ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung, Methodik und Fallstudie, Stand 10/2019, S. 9 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".