Der Bayerische Landesbeauftragte
für den Datenschutz

Datenschutzkonzepte für Digitalisierungsvorhaben

Aktuelle Kurz-Information 64

Stichwörter: Digitalcheck, bayerischer – Digitalisierungsvorhaben, Planungsphase – Digitalisierungsvorhaben, Standardprozess Datenschutz – KI-System – Nachweis, datenschutzrechtlicher – Planungsphase, Digitalisierungsvorhaben – IT-Projekt – IT-Sicherheit – Standardnachweis – Vergabeverfahren | **Stand:** 15. September 2025

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Ein gelungenes Digitalisierungsvorhaben beruht auch auf einem gelungenen Datenschutzkonzept.
- Das Datenschutzkonzept leitet eine schrittweise Erstellung der datenschutzrechtlichen Nachweise an und hilft dem Projektverantwortlichen, den Überblick zu behalten.
- Ein Datenschutzkonzept hat auch sonst sehr viele Vorteile.

Digitalisierung gilt als ein wichtiger Faktor für die Optimierung von Prozessen – auch bei bayerischen öffentlichen Stellen. Mit ihr sollen Effizienzressourcen genutzt werden; zudem soll auch die Servicequalität für die Bürgerinnen und Bürger verbessert werden. 1

So soll beispielsweise der „Digitalcheck“[1] des Bayerischen Staatsministeriums für Digitales die Ressorts bei der Erstellung digitaltauglicher Regelungen unterstützen. Gesetze und Verordnungen des Landes sollen dadurch auf einen Vollzug in der digitalen Welt vorbereitet werden. Bayerische öffentliche Stellen finden zudem Unterstützung durch zahlreiche digitale Förderprojekte. Mit der Digitalisierung halten zunehmend auch KI-Systeme Einzug in die Verwaltungen. 2

Eine erfolgreiche Digitalisierung wie auch der Einsatz von KI-Systemen im öffentlichen Sektor setzt das Vertrauen der Bürgerinnen und Bürger voraus. Dieses Vertrauen wird maßgeblich durch guten Datenschutz und gute IT-Sicherheit erarbeitet, die daher auch einen der sieben Punkte des „Digitalchecks“ ausmachen. Die vorliegende Aktuelle Kurz-Information möchte kurz gerafft zeigen, wie diese „Vertrauensarbeit“ in einem Datenschutzkonzept geleistet werden kann. Datenschutzrelevante Aspekte der IT-Sicherheit sind dabei berücksichtigt. 3

Das hier behandelte Datenschutzkonzept für ein Digitalisierungsvorhaben ist von einem Konzept zu unterscheiden, das sich primär auf das gesamte Datenschutz-Managementsystem einer Stelle bezieht. Das vorliegende, einführende[2] Papier richtet sich daher in erster Linie an bayerische öffentliche Stellen, die komplexere datenschutzrelevante Digitalisierungsvorhaben umsetzen möchten. Gleichzeitig bietet es Fördergebern eine Hilfestellung. In einem Förderverfahren sollte die Datenschutzkonformität des jeweiligen Vorhabens gezielt eingefordert werden: Mit einem tragfähigen Datenschutzkonzept sind Fördergeber wie geförderte Stellen „auf der sicheren Seite“. 4

Bereits jetzt berate ich zahlreiche bayerische öffentliche Stellen bei verschiedenen innovativen IT-Projekten und anderen Digitalisierungsvorhaben. Viele dieser Stellen erstellen Datenschutzkonzepte, in welchen die zu Datenschutzfragen erarbeiteten Lösungen laufend nach dem aktuellen Stand des jeweiligen Vorhabens erfasst und dokumentiert werden. Ein solches 5

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

Konzept hilft der verantwortlichen Stelle überdies bei der Erfüllung ihrer datenschutzrechtlichen Rechenschaftspflicht (Art. 5 Abs. 2 Datenschutz-Grundverordnung – DSGVO). Bedauerlicherweise erlange ich nämlich immer wieder von Vorhaben Kenntnis, bei denen der „Digitalcheck“ und die Beachtung von Standards aus Datenschutz und IT-Sicherheit erkennbar keine Rolle gespielt haben. Projektverantwortliche erwarten dann von mir nicht selten eine Art „Freigabe“, die von allen einschlägigen Sorgen enthebt. Eine solches Instrument sieht das geltende Recht bewusst nicht vor, und so ist dann die Enttäuschung groß, wenn meine Beratung die Schwächen des Projekts in den Bereichen Datenschutz und IT-Sicherheit offenlegt. Solche Enttäuschungen lassen sich leicht vermeiden: Wer den „Digitalcheck“ verinnerlicht und das vorliegende Papier kennt, kann hier eigentlich wenig falsch machen.

1. Vorteile eines Datenschutzkonzepts

6 Die Erstellung eines Datenschutzkonzepts bereits in der Planungsphase komplexer Digitalisierungsvorhaben bietet folgende Vorteile:

- **Transparenz schaffen:** Ein Datenschutzkonzept, das ein Vorhaben von Anfang an begleitet, bildet die Grundlage für Transparenz bei der Durchführung der Verarbeitung. Transparenz ist ein zentraler Grundsatz der Datenschutz-Grundverordnung – vgl. insbesondere Art. 5 Abs. 1 Buchst. a DSGVO – und soll gewährleisten, dass die Verarbeitung personenbezogener Daten erkennbar, nachvollziehbar und überprüfbar ist.

- **systematisches Vorgehen unterstützen:** Das Datenschutzkonzept gibt Hilfestellung zu einem systematischen, bewährten und gleichförmigen Vorgehen und erhöht damit den Reifegrad des Datenschutz-Managements beim jeweiligen Verantwortlichen.

- **Handlungsbedarfe erkennen und bearbeiten:** Bei Digitalisierungsvorhaben im öffentlichen Sektor sind häufig verschiedene Stellen beteiligt, die nur gemeinsam eine datenschutzrechtlich belastbare Lösung entwickeln und umsetzen können. Dafür sind arbeitsteilige und rechtzeitig abgestimmte Zuarbeiten der Akteure notwendig. Auch hier gilt der Grundsatz, dass eine frühzeitige Erkennung von Handlungsbedarfen eine proaktive Steuerung ermöglicht und unnötige Aufwände sowie Probleme vermeidet. Zudem sind durch diese Zusammenarbeit regelmäßig auch Synergiepotenziale realisierbar.

- **Beratung ermöglichen:** Eine zielgerichtete Beratung zu den Besonderheiten des jeweiligen Einzelvorhabens – etwa durch behördliche Datenschutzbeauftragte – setzt die Übersicht und die Kenntnis aller relevanten datenschutzrechtlichen Aspekte voraus.

- **Nachweise initiieren:** Angesichts der datenschutzrechtlichen Besonderheit, dass bestimmte Nachweise – sofern relevant – bereits vor der Verarbeitung durch den Verantwortlichen erbracht werden müssen (zum Beispiel zur Datenschutz-Folgenabschätzung – DSFA – nach Art. 35 Abs. 1 Satz 1 DSGVO oder zum Datenschutz durch Technikgestaltung nach Art. 25 Abs. 1 DSGVO), unterstützt das Datenschutzkonzept dabei, die erforderlichen Nachweise rechtzeitig zu erstellen und die notwendigen Umsetzungsschritte einzuleiten.

Ein Datenschutzkonzept zielt also darauf, alle datenschutzrechtlichen Anforderungen eines komplexen Digitalisierungsvorhabens systematisch, vollständig, transparent und effizient abarbeiten und die zugehörigen Nachweise für die geplanten Verarbeitungen führen zu können. Zudem sollen datenschutzrechtliche Sachverhalte und Anforderungen für relevante Meilensteine des Vorhabens (zum Beispiel Beschaffung, Beratung durch Experten und sonstige Abstimmungen) bereitgestellt werden. Aufgrund der Gestaltungsspielräume bei der Dokumentation[3] ermöglicht das Datenschutzkonzept eine frühzeitige Betrachtung der datenschutzrechtlichen Anforderungen und bietet Raum für zusätzliche Informationen, die nicht direkt in die Nachweise für die Verarbeitung einfließen. Gerade bei komplexen Digitalisierungsvorhaben leitet ein Datenschutzkonzept eine schrittweise Erstellung der einzelnen Nachweise an und hilft dem Projektverantwortlichen, den Überblick zu behalten. 7

2. Rahmenbedingungen

Das Datenschutzkonzept begleitet ein Digitalisierungsvorhaben von dessen Beginn bis zum Abschluss. Je nach Komplexität wird das Konzept schrittweise und parallel zum Vorhabensverlauf bedarfsgerecht konkretisiert. Ein frühzeitiger Beginn der Konzepterstellung durch die Vorhabens-/Projektleitung stellt sicher, dass alle Akteure angemessen eingebunden werden und eine solide Planungsgrundlage für die einzelnen datenschutzrechtlichen Arbeitsschritte geschaffen wird. 8

Das Datenschutzkonzept ist in der Datenschutz-Grundverordnung nicht ausdrücklich erwähnt, unterstützt aber die Erstellung der Standardnachweise. Diese Nachweise sind in der Datenschutz-Grundverordnung benannt und meist auch weiter konkretisiert, wie beispielsweise die Beschreibung einer Verarbeitungstätigkeit– in der Praxis auch in der Form einer Betriebsmittelbeschreibung – (vgl. Art. 30 Abs. 1 Satz 2 DSGVO), die Vereinbarung für eine Auftragsverarbeitung (vgl. Art. 28 Abs. 3 Satz 2 DSGVO) oder die DSFA (vgl. Art. 35 Abs. 7 DSGVO). Wenn im Datenschutzkonzept Inhalte eines bestimmten Standardnachweises in ausreichendem Vertiefungsgrad erarbeitet sind, sollten diese Inhalte in den eigentlichen Standardnachweis übernommen werden. 9

Im Folgenden gibt das Symbol „📄“ Hinweise im Zusammenhang mit den einschlägigen Standardnachweisen, in die die dargestellten Konzeptinhalte eingehen können. Die im Folgenden aufgeführten Verweise auf Standardnachweise nehmen teilweise Bezug auf die Form und Struktur der Standardnachweise, wie sie in meinen Materialien zur DSFA[4] dargestellt sind. 10

3. Inhaltliche Struktur

Wie bereits erwähnt, wird das Datenschutzkonzept schrittweise entwickelt – beginnend mit einer ersten Konzeptskizze bis hin zu einem Konkretisierungsgrad, der die Übernahme in die jeweils relevanten Standardnachweise für die Verarbeitung ermöglicht. Die im Folgenden beschriebenen Schritte, die durch iterative Durchläufe kontinuierlich verfeinert werden und die Struktur des Datenschutzkonzepts prägen, können im Einzelfall und bei Bedarf durch weitere Schritte ergänzt werden. Falls beispielsweise ein Vergabeverfahren Teil des Vorhabens sein 11

sollte, könnte etwa ein Schritt „Datenschutzrechtliche Vergabekriterien festlegen“ in das Datenschutzkonzept „eingebaut“ werden.[5]

Verarbeitungen identifizieren und beschreiben

12 Maßgebliche Bezugspunkte des Datenschutzkonzepts sind Verarbeitungen personenbezogener Daten. Diese können durch ein Digitalisierungsvorhaben entweder neu eingeführt oder geändert werden. Dabei kann es sinnvoll sein, den Fokus detaillierter auf bestimmte einzelne Verarbeitungsvorgänge zu legen (wie etwa Anonymisierungen, Drittlandübermittlungen), die im Rahmen eines umfassenden Verarbeitungskontextes – insbesondere aufgrund ihres spezifischen Verarbeitungsrisikos – einer vertieften Betrachtung bedürfen. Auch der Einsatz neuer Betriebsmittel, wie etwa die Einführung eines neuen Portals, KI-Systems oder eines anderen IT-Systems, bringt neue Verarbeitungsvorgänge mit sich, die datenschutzrechtlich zu würdigen sind.[6] Um einen vollständigen Überblick über die relevante „Verarbeitungslandschaft“ und die einzelnen Verarbeitungskontexte zu erhalten, ist es ratsam, eine hinreichend genaue Übersicht zu erstellen. In einem nächsten Schritt ist die Darstellung der wesentlichen Verarbeitungsschritte innerhalb jedes Verarbeitungskontextes zu empfehlen. Diese Übersichten können je nach Komplexität der jeweiligen konkreten Ausgestaltung ganz einfach gehalten oder nach bestehenden Standards gestaltet werden. Ein bestimmter Verarbeitungskontext und dessen Betriebsmittel können beispielsweise in Form eines Verarbeitungsverbundes dargestellt werden.[7]

13 Ein Verarbeitungsablauf kann als textliche Beschreibung (beispielsweise in Form eines Steckbriefs) oder als grafische Darstellung (etwa in Form einer Prozessmodellierung) beschrieben werden. Bei der Prozessmodellierung wird der Ablauf eines Prozesses in eine formale Beschreibungssprache, eine sogenannte Notation, übersetzt. Diese Notationen verwenden festgelegte Symbole zur grafischen Darstellung. Die gängigsten Notationen sind Business Process Model and Notation (BPMN), ereignisgesteuerte Prozessketten (EPK) sowie Flussdiagramme. Weitere Analyseschritte ermöglichen zudem insbesondere die Angabe der Kategorien personenbezogener Daten, der Kategorien betroffener Personen und der vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien.

Die Darstellung der Verarbeitungsschritte der jeweiligen Verarbeitung kann unter dem Punkt „6.3 Ausführliche Eigenschaftsdarstellung“ der Beschreibung eines Betriebsmittels oder gegebenenfalls unter dem Punkt „2.1.1 Welche Verarbeitung ist geplant?“ eines DSFA-Berichts übernommen werden. Alle weiteren Analyseergebnisse tragen dazu bei, insbesondere die Beschreibung der Verarbeitungstätigkeit bzw. die Beschreibung des Betriebsmittels sowie die datenschutzrechtlichen Informationen für die betroffenen Personen (Art. 13, 14 DSGVO) zu erstellen.

Datenschutzrechtliche Rollen identifizieren

14 Die datenschutzrechtlichen Rollen „Verantwortlicher“, „gemeinsam Verantwortliche“ und „Auftragsverarbeiter“ legen fest, wer inwieweit für die Einhaltung der Datenschutzvorschriften zuständig ist und wie sowie gegenüber wem betroffene Personen ihre Rechte wahrnehmen können.[8] In diesem Schritt ist daher stets sicherzustellen, dass alle (gemeinsam) verantwort-

lichen Stellen sowie gegebenenfalls deren (Unter-)Auftragsverarbeiter identifiziert werden. Sobald alle beteiligten Akteure bekannt und ihre Rollen definiert sind, ist im nächsten Schritt zu prüfen, ob für diese Rollen besondere datenschutzrechtliche Anforderungen bestehen und ob spezielle Nachweise erforderlich sind (zum Beispiel Vereinbarungen zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO oder Vereinbarungen zur gemeinsamen Verantwortlichkeit gemäß Art. 26 Abs. 1 Satz 2 DSGVO).[9] Zudem müssen in bestimmten Standardnachweisen der Datenschutzbeauftragte des jeweiligen Akteurs sowie die Empfänger personenbezogener Daten angegeben werden.

15 Leider stelle ich immer wieder fest, dass erst im Laufe eines Vorhabens – wenn nicht sogar erst kurz vor der Einführung eines neuen Verfahrens – darüber beraten wird, wer für welche Verarbeitungen als datenschutzrechtlich Verantwortlicher angesehen wird. Das ist ein besonders ärgerlicher Fehler, vor allem wenn sich das geplante Zusammenwirken nicht in den Kategorien des datenschutzrechtlichen Rollenmodells darstellen lässt.

Die datenschutzrechtlichen Rollen sind für alle Standardnachweise mit Blick auf die datenschutzrechtliche Rechenschaftspflicht (vgl. Art. 5 Abs. 2 DSGVO) relevant.

Zwecke und Rechtsgrundlagen identifizieren

16 Für jede Verarbeitung personenbezogener Daten muss ein legitimer Zweck sowie eine tragfähige Rechtsgrundlage bestimmt werden. Die verantwortliche Stelle ist verpflichtet sicherzustellen, dass immer ein legitimer Zweck sowie eine gültige Rechtsgrundlage für die Verarbeitung vorliegen, Art. 5 Abs. 1 Buchst. a und b, Art. 6 Abs. 1 DSGVO. Ist dies nicht der Fall, gilt die Verarbeitung als rechtswidrig. Behörden und andere öffentliche Stellen verarbeiten personenbezogene Daten in der Regel zur Erfüllung einer öffentlichen Aufgabe im öffentlichen Interesse oder auf Grund einer rechtlichen Verpflichtung.[10]

17 Da Verarbeitungen regelmäßig den Einsatz von Betriebsmitteln und anderen Mitteln erfordern, sind diese ein wesentlicher Bestandteil der Verarbeitung. Ob der Einsatz eines Betriebsmittels datenschutzkonform ist, hängt in der Regel von der Rechtsgrundlage ab, die der unterstützten Verarbeitungstätigkeit zugrunde liegt. Stets sind auch die Datenschutz-Grundsätze nach Art. 5 Abs. 1 DSGVO zu beachten. Da ein Betriebsmittel oft mehrere unterschiedliche Verarbeitungstätigkeiten unterstützen kann (so zum Beispiel ein E-Mail-System), kann es im Rahmen verschiedener Zwecke und Rechtsgrundlagen eingesetzt werden. Daher ist bei den Betriebsmitteln grundsätzlich eine verarbeitungsbezogene Rechtmäßigkeitsprüfung angezeigt.

Zwecke und Rechtsgrundlagen werden unter dem Punkt „6. Zwecke und Rechtsgrundlagen der Verarbeitung“ der Beschreibung einer Verarbeitungstätigkeit und gegebenenfalls (etwa bei zusätzlicher Rechtsgrundlage im Einzelfall eines KI-Systems) unter dem Punkt „6.3 Ausführliche Eigenschaftsdarstellung“ der Beschreibung eines Betriebsmittels angegeben.

Risiko abschätzen

18 Im Bereich des Datenschutzes kann das Risiko einer Verarbeitung in verschiedenen Zusammenhängen bewertet werden.[11] Die Prüfung, ob eine Verarbeitung voraussichtlich ein hohes

Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat und damit eine DSFA nach Art. 35 Abs. 1 DSGVO erforderlich ist, hat vor der Durchführung der Verarbeitung – also frühzeitig – zu erfolgen. Um die anschließende Abstimmung mit der Informationssicherheit vorzubereiten, ist zudem ratsam, die maximalen Ausgangsrisiken der betrachteten Verarbeitung im Hinblick auf die Risikobereiche Vertraulichkeit, Verfügbarkeit und Datenintegrität zu ermitteln.[12]

Das Ergebnis der DSFA-Erforderlichkeitsprüfung wird unter dem Punkt „15. Datenschutz-Folgenabschätzung" der Beschreibung einer Verarbeitungstätigkeit festgehalten. Die DSFA-Erforderlichkeitsprüfung selbst sollte anhand des Formulars „DSFA-Erforderlichkeitsprüfung"[13] durchgeführt und nachgewiesen werden.

Mit der Informationssicherheit abstimmen

19 Der technisch-organisatorische Datenschutz und die Informationssicherheit weisen vielfältige Überschneidungspunkte auf. Die im vorherigen Schritt ermittelten maximalen Ausgangsrisiken für die Risikobereiche Vertraulichkeit, Verfügbarkeit und Datenintegrität ermöglichen es, datenschutzrechtliche Erkenntnisse zeitgerecht in die Schutzbedarfsfeststellung des IT-Sicherheitskonzepts einzubringen. Dadurch wird ein abgestimmtes Vorgehen beider Disziplinen unter Realisierung von Synergiepotenzialen ermöglicht.

Geeignete Schutzmaßnahmen identifizieren und umsetzen

20 Die Datenschutz-Grundverordnung fordert an verschiedenen Stellen geeignete technische und organisatorische Maßnahmen, um die Risiken einer Verarbeitung für die Rechte und Freiheiten natürlicher Personen im Ergebnis angemessen zu minimieren.[14] Die Geeignetheit der Maßnahmen ist dabei in zwei Schritten zu beurteilen:

- **Erstens** sind die Risiken einer Verletzung des Schutzes der Rechte und Freiheiten natürlicher Personen sowie deren mögliche Folgen zu ermitteln, wobei die Bewertung grundsätzlich unter Berücksichtigung der Eintrittswahrscheinlichkeit und der Schwere der Risiken erfolgen muss.
- **Zweitens** ist zu prüfen, ob die umgesetzten technisch-organisatorischen Maßnahmen, insbesondere unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, die Risiken ausreichend mitigieren und somit angemessen sind.[15]

21 Instrumente wie die DSFA, die allgemeine datenschutzrechtliche Risikoanalyse[16] und weitere Risikobetrachtungen (zum Beispiel anwendbare Verhaltensregeln) dienen dazu, die Geeignetheit technischer und organisatorischer Maßnahmen nachzuweisen. Diese Nachweise können auch wichtige Kriterien für eine geplante Beschaffung[17] liefern und müssen ordnungsgemäß dokumentiert werden. Die als geeignet erachteten Schutzmaßnahmen sind grundsätzlich vor Beginn der Verarbeitung umzusetzen. Zudem verlangt die Datenschutz-Grundverordnung ein Verfahren zur (regelmäßigen) Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen (vgl. Art. 24 Abs. 1 Satz 2, Art. 32 Abs. 1 Buchst. d DSGVO).

In meinen Arbeitshilfen wird anhand von fiktiven Beispielen gezeigt, wie Nachweise für Risikoanalysen, die von den Anforderungen der Datenschutz-Grundverordnung systematisch hergeleitet wurden, gestaltet werden können.[18]

Datenschutzrechtliche Nachweise finalisieren

In einem letzten Schritt werden die im Datenschutzkonzept identifizierten, initialisierten und nach sachgerechter Priorisierung kontinuierlich weiter bearbeiteten datenschutzrechtlichen Standardnachweise – und gegebenenfalls auch weitere Nachweise – vervollständigt, qualitätsgesichert und abschließend finalisiert. 22

1 Internet: https://www.stmd.bayern.de/wp-content/uploads/2024/08/Digitalcheck_Starterpaket_V7.pdf.
2 Einen am Projektmanagement orientierten und deutlich umfassenderen Ansatz zeigt etwa das Konzept „Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben" der Berliner Beauftragten für Datenschutz und Informationsfreiheit, Internet: https://www.datenschutz-berlin.de/themen/behoerden/standardprozess.
3 Im Datenschutzkonzept können nicht nur die Standardnachweise, sondern weitere zusätzliche Informationen sinnhaft gebündelt abgebildet werden.
4 Siehe insbesondere auf https://www.datenschutz-bayern.de, Rubrik „DSFA".
5 Vgl. auch Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz als Kriterium im Vergabeverfahren, Orientierungshilfe, Stand 2/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".
6 Siehe insbesondere auf https://www.datenschutz-bayern.de, Rubrik „DSFA", Dokumente der Module 4 bis 6.
7 Beispiel dazu auf https://www.datenschutz-bayern.de, Rubrik „DSFA", Dokument „Modulhinweise".
8 Siehe Europäischen Datenschutzausschuss; Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Stand 7/2021, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de.
9 Das Bayerische Staatsministerium des Innern, für Sport und Integration hat etwa Muster für eine Vereinbarung zur Auftragsverarbeitung sowie für eine Vereinbarung zur Regelung gemeinsamer Verantwortlichkeit bereitgestellt, Internet: https://www.stmi.bayern.de/a-z/anzeigen/datenschutz-in-bayern.
10 Siehe hierzu Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DSGVO; diese Vorschriften tragen die Verarbeitung jedoch nicht allein. Es kommt vielmehr darauf an, dass der Unionsgesetzgeber oder ein nationaler Gesetzgeber die Rechtsgrundlage für die Verarbeitung im Einzelnen festlegt (vgl. Art. 6 Abs. 3 Satz 1 DSGVO).
11 Risikobetrachtungen werden beispielsweise im Rahmen einer DSFA, einer allgemeinen Risikoanalyse, eines Transfer Impact Assessment (TIA) bei der Datenübermittlung in Drittländer, einer Bewertung der Re-Identifizierbarkeit nach einer Anonymisierung oder der Erstellung von Verhaltensregeln durchgeführt.
12 Bei der Methode des IT-Grundschutzes für die Informationssicherheit können beispielsweise diese drei maximalen Ausgangsrisiken für die Bestimmung des Schutzbedarfs genutzt werden; näher zum IT- Grundschutz: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.
13 Siehe auf https://www.datenschutz-bayern.de, Rubrik „DSFA", Dokumente, Dokumente zu Modul 2.
14 Siehe etwa Art. 24 Abs. 1 und 2, Art. 25 Abs. 1 und 2, Art. 28 Abs. 1, Art. 32 Abs. 1 und Art. 35 Abs. 7 DSGVO.
15 Vgl. Europäischer Gerichtshof, Urteil vom 14. Dezember 2023, C-340/21, Rn. 42.
16 Zur DSFA und zur allgemeinen Risikoanalyse siehe Bayerischer Landesbeauftragter für den Datenschutz, Risikoanalyse und Datenschutz-Folgenabschätzung – Systematik, Anforderungen, Beispiele, Stand 5/2022, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".
17 Siehe Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz als Kriterium im Vergabeverfahren (Endnote 5).
18 Siehe auf https://www.datenschutz-bayern.de, Rubrik „DSFA", Dokumente der Module 3 bis 6.