Aktualisierung des Datenschutzes in China

21. September 2023 Dr. Thomas Pattloch, LL.M.Eur

TaylorWessing

1 Datenverarbeitung und -export

TaylorWessing

Maßnahmen zur Sicherheitsbewertung ausgehender Datenübermittlungen

- In Kraft seit 1. September 2022, erlassen von CAC
- Legt fest, wann und wie ein Antrag auf eine Sicherheitsbewertung durch die Behörden erforderlich ist, einschließlich
  - ausgehende Übermittlung wichtiger Daten durch einen Datenverarbeiter,
  - ausgehende Übermittlung personenbezogener Daten durch einen Betreiber einer kritischen Informationsinfrastruktur oder einen Verarbeiter personenbezogener Daten, der die personenbezogenen Daten von mehr als 1.000.000 Personen verarbeitet hat,
  - ausgehende Übermittlung personenbezogener Daten durch einen Verarbeiter personenbezogener Daten, der seit dem 1. Januar des Vorjahres kumulativ die personenbezogenen Daten von 100.000 Personen oder die sensiblen personenbezogenen Daten von 10.000 Personen ausgehend übermittelt hat.
- Die Maßnahmen sehen auch vor, dass der Datenverarbeiter vor der Beantragung der Sicherheitsbewertung einer **ausgehenden Datenübermittlung** eine **Selbstbewertung der Risiken bei der ausgehenden Datenübermittlung** vornimmt und Probleme ermittelt
- **Die Zuständigkeiten und Verpflichtungen müssen in einem** mit dem ausländischen Empfänger abgeschlossenen **Vertrag klar festgelegt werden**
- Der Übermittler muss die Sicherheitsbewertung erneut beantragen, wenn die Sicherheit der abgehenden Datenübermittlung beeinträchtigt werden könnte.

Weitere wichtige verwaltungsrechtliche Regelungen

- Leitfaden für Anwendungen zur Sicherheitsbewertung von ausgehenden Datenübertragungen (erste Ausgabe), veröffentlicht am 31. August 2022
- Bekanntmachung der Staatlichen Verwaltung für Marktregulierung und der Cyberspace-Verwaltung Chinas über die Durchführung der Zertifizierung für das Datensicherheitsmanagement, verkündet am und in Kraft seit dem 6. Juni 2022

Maßnahmen für den Standardvertrag für die grenzüberschreitende Übermittlung von personenbezogenen Daten

- Ausgestellt von der CAC am 22. Februar 2023, in Kraft seit 1. Juni 2023
- Enthält den Anhang Standardvertrag für die grenzüberschreitende Übermittlung von personenbezogenen Daten
- Zusätzlich herausgegeben am 30. Mai 2023: Leitlinien für die Einreichung des Standardvertrags für die grenzüberschreitende Übermittlung personenbezogener Daten (erste Ausgabe)
- Frist für die Erfüllung der Anforderungen durch Abschluss und Registrierung des Standardvertrags **bis zum Ende des 30. November 2023** (Art. 13 Maßnahmen für den Standardvertrag für die grenzüberschreitende Übermittlung personenbezogener Daten)

2 Standard-Vertrag

TaylorWessing

Standard-Vertrag

- Derzeit geltender Standardvertrag, Sanktionen bei Nichteinhaltung auf der Grundlage der PIPL
- Standardvertrag als Hauptbegründungsgrundlage für die Ausfuhr personenbezogener Daten, Art. 38 PIPL
- Gemäß Artikel 4 kann der SC als Rechtsgrundlage für ein inländisches Unternehmen verwendet werden, um personenbezogene Daten außerhalb Chinas zu übermitteln, wenn die folgenden Voraussetzungen erfüllt sind:

  (1) kein Betreiber kritischer Informationsinfrastrukturen ist;

  (2) Umgang mit personenbezogenen Daten von weniger als einer Million Personen;

  (3) seit dem 1. Januar des Vorjahres personenbezogene Daten von insgesamt weniger als 100.000 Personen an Empfänger in Übersee weitergegeben haben; und

  (4) die seit dem 1. Januar des Vorjahres sensible personenbezogene Daten von insgesamt weniger als 10.000 Personen an Empfänger in Übersee weitergegeben haben.

  Soweit in Rechts- oder Verwaltungsvorschriften oder von der nationalen Cyberspace-Behörde etwas anderes bestimmt ist, haben diese Vorschriften Vorrang.

- Offene Fragen hinsichtlich der Frage, wer der "Empfänger" ist und wer außerhalb Chinas den Standardvertrag mit dem Datenexporteur abschließen muss

Art. 55 PIPL und Art. 5 Maßnahmen Standardvertrag

Die Maßnahmen wiederholen die gesetzliche Forderung nach einer Folgenabschätzung für personenbezogene Daten gemäß Artikel 55 des PIPL, bevor personenbezogene Daten aus China heraus übermittelt werden, die Folgendes umfassen muss:

- die Rechtmäßigkeit, Vertretbarkeit und Notwendigkeit der Verarbeitung personenbezogener Daten sowohl durch den Exporteur personenbezogener Daten als auch durch die ausländischen Empfänger personenbezogener Daten (z. B. Zweck, Umfang und Methode);
- die Menge, den Umfang, die Kategorie und die Sensibilität der zu exportierenden personenbezogenen Daten sowie die entsprechenden Risiken;
- die Verantwortlichkeiten und Verpflichtungen, zu denen sich die ausländischen Empfänger verpflichtet haben, sowie ihre Management- und technische Kompetenz, ihren Verpflichtungen nachzukommen und die Sicherheit personenbezogener Daten zu gewährleisten;
- das Risiko des Durchsickerns, der Sabotage, der Veränderung und des Missbrauchs personenbezogener Daten bei der Ausfuhr und die Verfügbarkeit von Rechtsmitteln für die betroffenen Personen;
- die Auswirkungen der Datenschutzgesetze und -politiken in der Rechtsprechung ausländischer Empfänger auf die Leistung der SCC; und
- andere Faktoren, welche die Sicherheit der PI gefährden.

Gemäß den Maßnahmen ist ein PIA-Bericht drei Monate vor der Registrierung bei der CAC zu erstellen und mindestens drei Jahre lang aufzubewahren. Die SC ist innerhalb von zehn Tagen nach ihrer Wirksamkeit bei der CAC einzureichen.

Muss chinesisches Recht anwenden.

Ergänzung oder neuer SC erforderlich

Ein neuer SC wird abgeschlossen und erneut durchgeführt, wenn:

1) eine Änderung des Zwecks, des Umfangs, der Art, der Empfindlichkeit, der Menge, der Methode, der Aufbewahrungsfrist und des Speicherorts der ins Ausland übermittelten personenbezogenen Daten oder eine Änderung des Zwecks und der Methode der Verarbeitung personenbezogener Daten durch den Empfänger im Ausland oder eine Verlängerung der Aufbewahrungsfrist der personenbezogenen Daten im Ausland;

(2) in dem Land oder der Region, in dem/der sich der überseeische Empfänger befindet, eine Änderung der Politik und der Vorschriften zum Schutz personenbezogener Daten eintritt, die sich auf die Rechte und Interessen an personenbezogenen Daten auswirken kann; oder

(3) andere Umstände, die die Rechte und Interessen an personenbezogenen Daten beeinträchtigen können.

3 Klassifizierung der Daten

Der Anwendungsbereich des Datensicherheitsgesetzes, Art. 2 und 3 DSL

- DSL gilt für alle in China durchgeführten Datenverarbeitungsaktivitäten und die damit verbundene Sicherheitsüberwachung. Unter Datenverarbeitung versteht das Gesetz die Erhebung, Speicherung, Nutzung, Verarbeitung, Übermittlung, Bereitstellung oder Offenlegung von Daten.
- Zu den "Daten" im Sinne der DSL gehören nicht nur elektronische Daten, sondern auch andere Daten wie Ausdrucke, Papierakten usw.
- Wenn außerhalb Chinas durchgeführte Datenverarbeitungsaktivitäten (i) die nationale Sicherheit Chinas, (ii) die öffentlichen Interessen Chinas oder (iii) die legitimen Rechte und Interessen chinesischer Bürger oder Organisationen beeinträchtigen, unterliegen sie ebenfalls dem Datensicherheitsgesetz.
- Infolgedessen führt gemäß Art. 27 DSL die Datenverarbeitung in Netzen oder über das Internet zu
  - (1) Verpflichtung zur Einrichtung und Vervollkommnung eines Managementsystems für die Datensicherheit über den gesamten Arbeitsablauf hinweg;
  - (2) Diejenigen, die Daten unter Verwendung des Internets oder anderer Informationsnetze verarbeiten, müssen auf der **Grundlage des abgestuften Systems zum Schutz der Cybersicherheit** die Datensicherheitsverpflichtungen gemäß der DSL erfüllen;
  - (3) Die Nichteinhaltung der Anforderungen von Art. 27 DSL führt zu Sanktionen gemäß Art. 45 DSL, d.h. Korrekturen, Verwarnungen, Geldbußen zwischen 50.000 und 500.000 CNY für eine Organisation und zusätzlich eine Geldbuße für die direkt verantwortlichen Beamten und andere Personen in Höhe von 10.000 bis 100.000 CNY. Im Falle der Verweigerung einer Korrektur oder eines größeren Datenlecks erhöht sich die Geldbuße auf 500.000 bis 2 Millionen CNY, die Aussetzung des Geschäftsbetriebs, der Entzug der Geschäftslizenz und eine erhöhte persönliche Haftung des Verantwortlichen und anderer Personen von 50.000 bis 200.000 CNY.

DSL: Schutz von Kerndaten und wichtigen Daten

- Art. 21 DSL verweist auch auf ein "klassifiziertes und abgestuftes Datenschutzsystem" und legt fest, dass der "nationale Mechanismus zur Koordinierung der Datensicherheit eine Gesamtplanung für die Formulierung der Kataloge für wichtige Daten vornimmt und die zuständigen Abteilungen koordiniert".
  - **Jede Region und jedes Departement legt in Übereinstimmung mit dem klassifizierten und abgestuften Datenschutzsystem den spezifischen Katalog für wichtige Daten** für die jeweilige Region und das jeweilige Departement in relevanten Branchen und Bereichen **fest** und übernimmt den besonderen Schutz der im Katalog enthaltenen Daten
    - Das bedeutet, dass es **nicht eine einzige gesetzliche Definition von "wichtigen Daten" gibt, sondern eine Vielzahl von (ministeriellen und anderen) Katalogen**, die im Laufe der Zeit geändert, ergänzt und unterschiedlich interpretiert werden können
    - Der Entwurf der Norm "Informationssicherheitstechnologie - Leitlinien für die Identifizierung wichtiger Daten" wurde hinzugefügt, ist aber noch nicht in Kraft und wird wahrscheinlich noch geändert werden.
  - **Art. 21 DSL definiert ferner "Kerndaten des Staates"** als Daten, die die nationale Sicherheit, die Lebensadern der nationalen Wirtschaft, die wichtigsten Lebensgrundlagen der Menschen und wichtige öffentliche Interessen betreffen und die "einem strengeren Verwaltungssystem unterliegen".

Wichtige Daten

- Der Entwurf des Rundschreibens CAC Regulations on Network Data Security Management, das am 14. November 2021 veröffentlicht wurde, enthält in seinem Art. 73 eine allgemeine Definition des Begriffs "wichtige Daten":
  - 3. "Wichtige Daten" sind Daten, deren Manipulation, Sabotage, Durchsickern, illegale Beschaffung oder illegale Verwendung der nationalen Sicherheit oder dem öffentlichen Interesse schaden kann, einschließlich der folgenden Daten:
  - (1) Daten im Zusammenhang mit Regierungsangelegenheiten, die nicht offengelegt wurden, offizielle Arbeitsgeheimnisse, nachrichtendienstliche Daten und Daten der Strafverfolgungs- oder Justizbehörden;
  - (2) Ausfuhrkontrolldaten, Daten im Zusammenhang mit der Kerntechnologie, dem Entwurf, dem Produktionsprozess oder ähnlichen Informationen, die ein **Ausfuhrkontrollgut** betreffen**, Daten über wissenschaftliche und technologische Fortschritte in den Bereichen Verschlüsselung, Biologie, elektronische Informationen, künstliche Intelligenz** oder in anderen Bereichen, die sich unmittelbar auf die nationale Sicherheit oder die wirtschaftliche Wettbewerbsfähigkeit auswirken;
  - (3) **Daten über die volkswirtschaftliche Leistung, Geschäftsdaten eines wichtigen Wirtschaftszweigs, statistische Daten** und andere Daten, die aufgrund von einzelstaatlichen Rechtsvorschriften, Verwaltungsvorschriften oder Regelungen des Ministeriums ausdrücklich vor der Verbreitung geschützt und kontrolliert werden müssen;
  - (4) **Daten über die Produktions- oder Betriebssicherheit in den Bereichen Industrie, Telekommunikation, Energie, Verkehr, Wasserressourcen, Finanzen, nationale Verteidigungstechnologie, Zoll, Steuern oder anderen Schlüsselsektoren oder -bereichen, Daten über kritische Systemkomponenten oder die Lieferkette kritischer Ausrüstung**;
  - (5) **nationale Basisdaten über Bevölkerung und Gesundheit oder natürliche Ressourcen und Umwelt**, wie **genetische, geographische, mineralische und meteorologische Daten, die den** von der zuständigen staatlichen Behörde vorgeschriebenen **Schwellenwert oder Präzisionsgrad erreichen**;
  - (6) Daten über die Entwicklung oder den Betrieb nationaler Infrastrukturen oder kritischer Informationsinfrastrukturen oder deren Sicherheitsdaten, Daten über die geografische Lage oder den Sicherheitszustand oder andere Daten einer nationalen Verteidigungseinrichtung, einer militärischen Verwaltungszone, einer nationalen Verteidigungsforschungs- oder -produktionseinheit oder eines anderen wichtigen sensiblen Bereichs; und
  - (7) andere Daten, die sich auf die Sicherheit der Nation auswirken können, wie z. B. politische, territoriale, militärische, wirtschaftliche, kulturelle, soziale, wissenschaftliche und technologische, ökologische, ressourcenbezogene, nukleare Anlagen, überseeische Interessen, biologische, weltraumbezogene, polare oder maritime Sicherheit.

MIIT-Rundschreiben Maßnahmen für das Datensicherheitsmanagement 8 Dez. 2022

- Rundschreiben des MIIT über die Maßnahmen für das Datensicherheitsmanagement im Industrie- und Informationstechnologiesektor (zur probeweisen Umsetzung), gültig ab 1. Januar 2023
- Klassifizierungsanforderungen und Definition von Kriterien für die Bestimmung von wichtigen Daten und Kerndaten enthalten
- Artikel 10 Daten, bei denen das Ausmaß des Schadens eine der folgenden Bedingungen erfüllt, gelten als wichtige Daten:

  1. eine Bedrohung für Politik, Land, militärische Angelegenheiten, Wirtschaft, Kultur, Gesellschaft, Wissenschaft und Technologie, Elektromagnetismus, Netzwerke, Ökologie, Ressourcen, nukleare Sicherheit usw. darstellen und die Interessen in Übersee, Biologie, Weltraum, Polarregionen, Tiefsee, künstliche Intelligenz und andere Schlüsselbereiche im Zusammenhang mit der nationalen Sicherheit betreffen;

  2. schwerwiegende Auswirkungen auf die Entwicklung, die Produktion, den Betrieb und die wirtschaftlichen Interessen im Bereich der Industrie und der Informationstechnologie haben;

  3. die Verursachung eines schwerwiegenden Datensicherheitsvorfalls oder eines Arbeitsunfalls, der die öffentlichen Interessen oder die legitimen Rechte und Interessen von Einzelpersonen oder Organisationen ernsthaft beeinträchtigt und große negative soziale Auswirkungen hat;

  4. offensichtliche Kaskadeneffekte verursachen, die mehrere Industrien, Regionen oder mehrere Unternehmen in der Industrie betreffen, oder eine lange Wirkungsdauer haben, die schwerwiegende Auswirkungen auf die Entwicklung der Industrie, den technologischen Fortschritt, die industrielle Ökologie usw. haben; und

  5. alle anderen wichtigen Daten, die vom Ministerium für Industrie und Informationstechnologie bewertet und festgelegt werden.

MIIT-Rundschreiben - Definition von “nationalen Kerndaten"

Artikel 11 Daten, bei denen das Ausmaß des Schadens eine der folgenden Bedingungen erfüllt, gelten als Kerndaten:

1. eine ernsthafte Bedrohung für Politik, Land, Militär, Wirtschaft, Kultur, Gesellschaft, Wissenschaft und Technologie, Elektromagnetismus, Netzwerke, Ökologie, Ressourcen, nukleare Sicherheit usw. darstellen und ernsthafte Auswirkungen auf überseeische Interessen, Biologie, Weltraum, Polarregionen, Tiefsee, künstliche Intelligenz und andere Schlüsselbereiche im Zusammenhang mit der nationalen Sicherheit haben;

2. erhebliche Auswirkungen auf den Industrie- und Informationstechnologiesektor und seine wichtigen Basisunternehmen, kritischen Informationsinfrastrukturen, wichtigen Ressourcen usw. haben;

3. materielle Schäden für die industrielle Produktion und den Betrieb, die Telekommunikationsnetze und Internet-Betriebsdienste, die Entwicklung des Radiogeschäfts usw. verursachen und zu großflächigen Arbeits- und Produktionsausfällen, Unterbrechungen des Radiogeschäfts, Netz- und Dienstlähmungen, Verlust von großen Geschäftsverarbeitungskapazitäten usw. führen; und

4. alle anderen vom Ministerium für Industrie und Informationstechnologie bewerteten und festgelegten Kerndaten.

Wichtige Daten

- "Wichtige Daten" führen unter anderem zu
  - (1) strengere Anforderungen in Bezug auf die Sicherheitsmaßnahmen,
  - (2) obligatorische Benennung einer für die Datensicherheit verantwortlichen Person und Einrichtung einer Sicherheitsabteilung;
  - (3) periodische und regelmäßige Risikobewertungen der Datenverarbeitungstätigkeiten und regelmäßige Berichterstattung der Bewertungsergebnisse an die Behörden,
  - (4) obligatorische Lokalisierung von Daten;
  - (5) Die Ausfuhr ist an Bedingungen geknüpft und erfordert eine Sicherheitsprüfung der Ausfuhr durch das CAC mit jährlichen Berichten über die Sicherheit der Verbringung und die Einreichung dieser Berichte bei den örtlichen Behörden,
  - (6) obligatorische vertragliche Vereinbarungen mit dem Empfänger der Daten.
- Ein Export, der gegen das Cybersicherheitsgesetz (Art. 37 CSL) und andere Verwaltungsvorschriften der CAC (z. B. Measures for Security Assessment of Cross-border Data Transfer (Draft for Comment), herausgegeben am 29. Oktober 2021) verstößt, führt zu **Sanktionen wie Berichtigung, Verwarnung, Geldstrafe in Höhe von 100.000 CNY bis 1 Mio. CNY sowie Geldstrafe für direkt verantwortliche Führungskräfte und andere Personen in Höhe von 10.000 CNY bis 100.000 CNY**. Unter schwerwiegenden Umständen (nicht definiert) Geldbuße zwischen CNY 1 Mio. und CNY 10 Mio., Anordnung der Aussetzung der Geschäftstätigkeit, Entzug der Geschäftslizenz und direkte Haftung von CNY 100.000 bis CNY 1 Mio. für direkt verantwortliche Führungskräfte und andere Personen.
- Mangelnde Zusammenarbeit mit den Sicherheitsorganen zieht ähnliche Sanktionen nach sich, Art. 36,36 und 48 DSL

Weitere Verwaltungsvorschriften, die verschiedene Arten von Daten und Branchen regeln

- Mehrere neue Arten von Daten wurden in Verwaltungsvorschriften aufgenommen, z. B. "**Netzwerkdaten**", "**öffentliche Daten**" im Entwurf der CAC-Verordnung über das Sicherheitsmanagement von Netzwerkdaten vom 14. November 2021, "**industrielle Daten**" in Art. 2 des MIIT-Rundschreibens zur Herausgabe des Leitfadens zur Klassifizierung und Einstufung von Industriedaten vom 27. Februar 2020
- Maßnahmen zur Überprüfung der Cybersicherheit, verkündet am 28. Dezember 2021, die für Betreiber kritischer Informationsinfrastrukturen (CIIO) und Datenverarbeitungsaktivitäten durch einen Netzplattformbetreiber gelten und die Einrichtung eines nationalen Mechanismus zur Überprüfung der Cybersicherheit vorsehen (der unter anderem auf Unternehmen abzielt, die im Ausland gelistet sind oder mehr als 1 Million personenbezogene Nutzerdaten ins Ausland exportieren)
- Spezifische Branchenvorschriften, wie z. B.:
  - MIIT-Rundschreiben zur Stärkung der Netz- und Datensicherheit des Internets der Fahrzeuge 15. September 2021
  - MIIT-Rundschreiben zur Herausgabe des Leitfadens zur Klassifizierung und Einstufung von Industriedaten 27. Februar 2020
  - Verschiedene Bestimmungen zum Sicherheitsmanagement für Automobildaten (zur probeweisen Umsetzung) 1. Oktober 2021
  - GB/T 39725 - 2020 Informationssicherheitstechnologie - Leitfaden für die Sicherheit von Gesundheitsdaten
- Standards für die Datenklassifizierung: Network Security Standards Practicing Guidelines - Network Data Classification and Grading Guidelines, veröffentlicht im Dezember 2021 ("**Data Classification Guidelines**")
  - Drei Ebenen von Daten: Allgemeine Daten, wichtige Daten, Kerndaten
  - Wichtige Daten und Kerndaten werden hauptsächlich durch nationale und industrielle Datenkataloge ermittelt

Datenklassifizierung nach der DSL - Grundsätze

- Datenklassifizierung im Rahmen der DSL - Grundsätze der Leitlinien für die Datenklassifizierung:
  - Datenklassifizierung auf der Grundlage "**mehrerer Dimensionen**" wie individuelle/öffentliche/zu verbreitende Daten/industriespezifische Daten/organisatorische Daten, die "unterteilt" werden können.
  - **Klare Abstufung und Umsetzung der Maßnahmen**: Unterschiedliche Schutzmaßnahmen für verschiedene Kategorien und den jeweiligen Geheimhaltungsgrad der Daten.
  - Wenn ein Datensatz **mehrere Datenebenen** enthält, sollte er nach der höchsten Datenebene im Datensatz klassifiziert werden. Wenn ein Datensatz beispielsweise Kerndaten, wichtige Daten und allgemeine Daten enthält, sollte er auf der Ebene der Kerndaten klassifiziert werden.
  - **Rechtzeitige Anpassung**: Die Klassifizierung und Einstufung von Daten kann sich ändern und sollte rechtzeitig angepasst werden, wenn sich die Umstände ändern, z. B. bei Änderungen der einschlägigen Leitlinien oder beim Auftreten bestimmter Sicherheitsereignisse.
  - Bei der Einstufung von Netzdaten **sollte** ein **Datenverarbeiter zunächst prüfen, ob es sich bei den Daten um Kerndaten oder wichtige Daten auf der Grundlage nationaler und branchenspezifischer Standards handelt**. Wenn die nationalen oder branchenüblichen Normen keinen Hinweis darauf enthalten, kann der Datenverarbeiter das Ausmaß der Auswirkungen analysieren, wenn die Daten manipuliert, zerstört, durchgesickert, unrechtmäßig erlangt oder verwendet werden, und entscheiden, ob es sich um Kerndaten oder wichtige Daten handelt, und zwar auf der Grundlage der bestehenden Normen und Vorschriften zur Identifizierung von Kerndaten oder wichtigen Daten. Handelt es sich bei den **Daten um einen Datensatz, sollte der Datenverarbeiter den Grundsatz "vorbehaltlich der höchsten Geheimhaltungsstufe" befolgen.**

Mindestklassifizierungsstufen

- Die Mindestreferenzwerte für spezifische allgemeine Daten:

(1) Mindestens Stufe 4 für sensible persönliche Daten und mindestens Stufe 2 für allgemeine persönliche Daten.

(2) Persönliche Informationen von Mitarbeitern innerhalb der Organisation sind nicht weniger als Stufe 2.

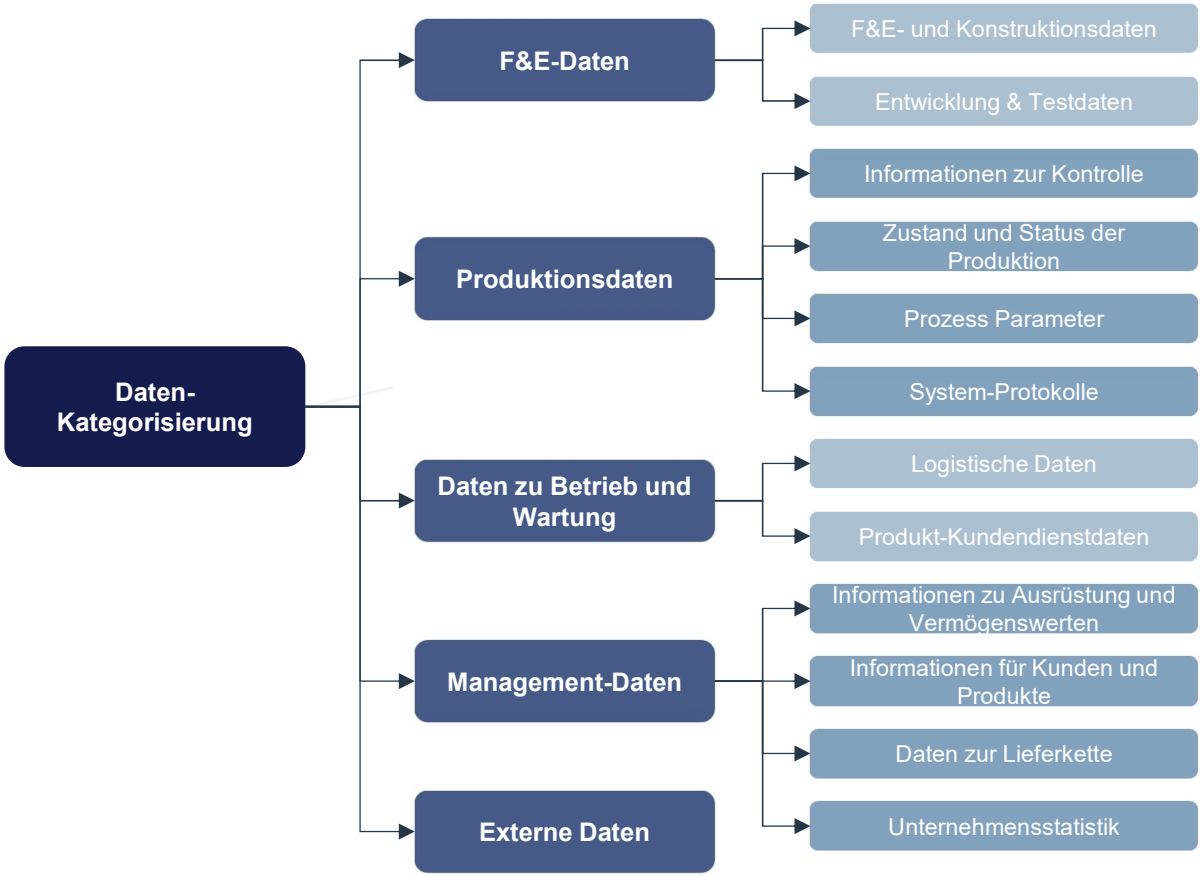
(3) Der Grad der öffentlichen Daten, die bedingt offen/gemeinsam genutzt werden, ist nicht geringer als der Grad 2, und offen/gemeinsam genutzt ist verboten

(4) Öffentliche Daten sind nicht weniger als Stufe 4.

- **"Rohdaten"** können nach der gleichen Methode eingestuft werden;
- Das Niveau der "**abgeleiteten Daten**" wird gegenüber dem Niveau des verarbeiteten Rohdatensatzes grundsätzlich nach dem Prinzip "höher und strenger" eingestuft, wobei die Daten je nach Verarbeitungsgrad auch herauf- oder heruntergestuft werden können.
  - Das Niveau der desensibilisierten Daten kann vom Niveau des ursprünglichen Datensatzes auf nicht weniger als Niveau 2 für de-identifizierte persönliche Informationen und nicht weniger als Niveau 1 für anonymisierte persönliche Informationen reduziert werden.
  - Die Ebene der sog. Label Daten kann von der Ebene des Originaldatensatzes reduziert werden, wobei nicht weniger als 2 Ebenen einzelner Label Daten zur Verfügung stehen.
  - Statistiken, die großräumige Gruppenmerkmale oder Handlungsverläufe betreffen, sollten auf einer höheren Ebene als der ursprünglichen Datensatzebene festgelegt werden.
  - Die Ebene der abgeleiteten Daten ("fusionierte Daten") sollte das Ergebnis der Datenaggregation und -fusion berücksichtigen. Wenn die Ergebnisdaten mehr Originaldaten aggregieren oder sensiblere Daten abbauen, muss die Ebene angehoben werden, aber wenn die Ergebnisdaten den Grad der Identifizierung usw. verringern, kann die Ebene gesenkt werden.

Daten-Kategorisierung

Vor der Klassifizierung und Einstufung der Empfindlichkeit empfiehlt sich ein System zur Kategorisierung der Daten entsprechend der vorherrschenden industriellen Praxis.



- Zunächst sollte geprüft werden, ob die geltenden Industriestandards für die Datenkategorisierung eingehalten werden müssen.
- Zu den anwendbaren Standards gehören die *Richtlinien für die Kategorisierung und Klassifizierung von Industriedaten (Trial)*, deren Kategorisierung auf der linken Seite dargestellt ist und je nach Geschäftsbetrieb angepasst werden kann.
- Für den Fall, dass die linke Kategorisierung bei der Bewertung nicht zum konkreten Geschäftsbetrieb passt, kann eine andere Kategorisierung vorgenommen werden (z.B. Kategorisierung der Daten - aus organisatorischer Sicht - in Kundendaten, Geschäftsdaten, Betriebs- und Managementdaten, Systembetriebs- und Sicherheitsdaten).

Klassifizierung der kategorisierten Daten - Beispiel

Art/Klasse der Daten	Betroffene Interessen			
	Nationales Interesse	**Öffentliches Interesse**	**Rechte des Einzelnen**	**Rechte von Organisationen und Unternehmen**
Allgemeine Daten - Stufe 1	Keine Gefahr	Keine Gefahr	Keine Gefahr	Keine Gefahr
Allgemeine Daten - Stufe 2	Keine Gefahr	Keine Gefahr	Geringes Risiko	Geringes Risiko
Allgemeine Daten - Stufe 3	Keine Gefahr	Keine Gefahr	Allgemeine Gefahr	Allgemeine Gefahr
Allgemeine Daten - Stufe 4	Keine Gefahr	Keine Gefahr	Ernsthafte Bedrohung	Ernsthafte Bedrohung
Wichtige Daten	Geringe Gefahr	Geringfügige oder allgemeine Gefahr	K.A.	K.A.
Nationale Kerndaten	Allgemeine oder ernste Gefahr	Ernsthafte Bedrohung	K.A.	K.A.

Grundsätze der Neueinstufung

Measures or situations	Security level change
Increase in data volume to a specific size leading to significant social impact	Upgrade
Data to achieve the accuracy of the relevant national departments	Upgrade
Correlate data from multiple business units	Upgrade
Large amount of multidimensional data for correlation	Upgrade
Occurrence of specific events leading to increased data sensitivity	Upgrade
Data has been made public or disclosed	Downgrade
Data is desensitized or key fields are removed	Downgrade
Data is de-identified, pseudonymized, and anonymized	Downgrade
Data loss of sensitivity due to specific events in the data	Downgrade

Hinweis: Datenverarbeiter, die personenbezogene Daten von mehr als einer Million Menschen verarbeiten, werden gemäß den Bestimmungen für wichtige Datenverarbeiter verwaltet und sollten entsprechende Datenschutzanforderungen erfüllen.

Skizze des Verfahrens (weitere Einzelheiten gelten für das jeweilige Verfahren)

- Ein Datenverarbeiter sollte die nachstehenden Schritte befolgen, um seine Datenbestände zu kategorisieren, zu klassifizieren und zu bewerten:
  1) eine Bestandsaufnahme ihrer Datenbestände durchführen und eine Liste der Datenbestände erstellen ("Daten(fluss)abbildung" oder "**Dateninventar**").
  2) Kategorisierung von Datensätzen auf der Grundlage verschiedener Dimensionen in Übereinstimmung mit Industriestandards oder anderen relevanten Datenklassifizierungsvorschriften ("**Datenkategorisierung**").
     - Identifizieren Sie Kerndaten, wichtige Daten, allgemeine Daten und persönliche Informationen.
     - Eine Einstufung auf der Grundlage der Sensibilitätsstufe für verschiedene Benchmarks vornehmen
     - Dokumentieren Sie den Prozess
  3) Selbsteinschätzung der Sensibilitätsprüfung auf der Grundlage der Klassifizierung und Einstufung, Aktualisierung der oben genannten Klassifizierung und Einstufung ("**Datenklassifizierung**" auf der Grundlage der "**Datenfolgenabschätzung**")
  4) Ergreifen geeigneter Maßnahmen zum Schutz von Daten verschiedener Ebenen und Klassifizierungen ("**Datenschutzmaßnahmen**"), einschließlich, falls erforderlich, der Einreichung bei staatlichen Behörden für eine fachkundige Sicherheitsbewertung ("**Sicherheitsüberprüfung**") oder für eine Registrierung vor dem Export
  5) Regelmäßige Überprüfung der Bewertung, der Einstufung und der damit verbundenen Sicherheitsmaßnahmen ("ständige Überwachung" und "**Neueinstufung**", wo angezeigt)