Datenschutz im Überblick

Durch den rasanten Anstieg der digitalen Medien rückt auch der Datenschutz immer mehr in den Blickpunkt der Menschen. Unter Datenschutz kann man den Schutz vor Missbrauch personenbezogener Daten verstehen. Dadurch sollen auch Rechte wie „das Recht auf informationelle Selbstbestimmung" geschützt werden. Der Mensch sollte selbst entscheiden können, was mit seinen persönlichen Daten geschieht. Dieses Recht wird aber ständig gebrochen, denn die Sammlung von Daten und die daraus gezogenen Schlüsse sind eine der wichtigsten Informationsquellen für die Wirtschaft, aber beispielsweise auch für die Geheimdienste. Ein Schutz gegen solchen Missbrauch der persönlichen Daten ist der eigene verantwortungsvolle Umgang mit seinen Daten, aber auch Gesetze wie das Bundesdatenschutzgesetz oder die europäische Datenschutz-Grundverordnung sowie die Implementierung von Datenschutzbeauftragen in Behörden und Unternehmen. Die Datenschutz-Grundverordnung DSGVO trat im Jahr 2018 in Kraft und regelt den Datenschutz EU-weit. Dabei lässt sie aber an einigen Stellen Raum für nationale Regelungen durch so genannte „Öffnungsklauseln", so dass jeder Staat die DSGVO entsprechend ergänzen und erweitern kann. Das geschieht in Deutschland durch das Bundesdatenschutzgesetz, das ebenfalls im Jahr 2018 in Kraft trat. Auch die Landesdatenschutzgesetze wurden entsprechend angepasst. Der „oberste" Datenschützer in Deutschland ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Seine Behörde kontrolliert und berät untergeordnete Behörden (Landesbehörden) im Zusammenhang mit Datenschutz.

Zusätzlich zu diesen Gesetzen wird der Datenschutz in bestimmten Bereichen wie der Telekommunikation oder den Medien zusätzlich durch das Telekommunikationsgesetz bzw. das Telemediengesetz geregelt. Die Einhaltung des Datenschutzes ist damit eine komplexe Angelegenheit, die in Spezialfällen nur durch Experten machbar ist. Die grundsätzlichen Gesetze und Verordnungen aus der Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz sind aber für alle Bürgerinnen und Bürger von Interesse und sollten im Rahmen einer Allgemeinbildung auch vermittelt werden.

Weltweit gesehen sind Deutschland und auch die EU sehr fortschrittlich mit dem Bundesdatenschutzgesetz und der Datenschutz-Grundverordnung. Einzelne andere Länder haben ähnlich ausgereifte Gesetze, viele Länder jedoch nicht. Die USA haben beispielsweise kein allgemeines Datenschutzgesetz, sondern branchenspezifische Lösungen. Weiterhin haben die Behörden in den USA umfangreiches Zugriffsrecht auf Daten nach dem „USA PATRIOT Act", einem Gesetz, das nach den Anschlägen vom 11. September 2001 zur Terrorabwehr verabschiedet wurde. Auch der nachfolgende „US Freedom Act" erlaubt weiterhin Zugriff auf personenbezogene Daten. Aus diesen Gründen raten Experten auch davon ab, dass Firmen ihre Daten auf US-amerikanischen Cloud-Servern speichern.

Grundlagen 1

Ausgangsszenario:

Wegen der relativ neuen Datenschutz-Grundverordnung DSGVO (2018) und der darauffolgenden Neufassung des Bundesdatenschutzgesetzes BDSG (2018) hat die Geschäftsleitung der IT-Firma ***ConSystem GmbH*** alle Abteilungsleitungen beauftragt, die Mitarbeiter über wesentliche Aspekte des Datenschutzes zu informieren.

Aufgabenstellung:

Der Leiter der Abteilung Entwicklung hat einige wesentliche Aspekte des Datenschutzes zusammengetragen. Für eine Info-Mail an alle Mitarbeiter bittet er Sie, diese Stichpunkte auszuführen und zu ergänzen.

Wichtige Datenschutzaspekte

Was regelt die DSGVO und was regelt das BDSG?

Ausgewählte Rechte betroffener Personen nach der DSGVO:

Recht auf Auskunft:

Recht auf Berichtigung:

Recht auf Löschung:

Grundlagen 2

Ausgangsszenario:

Die Geschäftsleitung der IT-Firma ***ConSystem GmbH*** ist unsicher, ob die Firma eines Kunden einen Datenschutzbeauftragen benennen muss und hat den Leiter der Vertriebsabteilung beauftragt, eine Entscheidungshilfe zu erstellen.

Aufgabenstellung:

Der Leiter der Vertriebsabteilung hat die relevanten Artikel aus der DSGVO und dem BDSG zusammengetragen. Als Auszubildender der Firma erhalten Sie den Auftrag einen Programmablaufplan zu erstellen, der eine Entscheidung für die Benennung ermöglicht.

§ 38 BDSG

Datenschutzbeauftragte nichtöffentlicher Stellen

1. Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen. […]

Art. 35 DSGVO

Datenschutz-Folgenabschätzung

1. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.
2. Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

Art. 37 DSGVO

Benennung eines Datenschutzbeauftragten

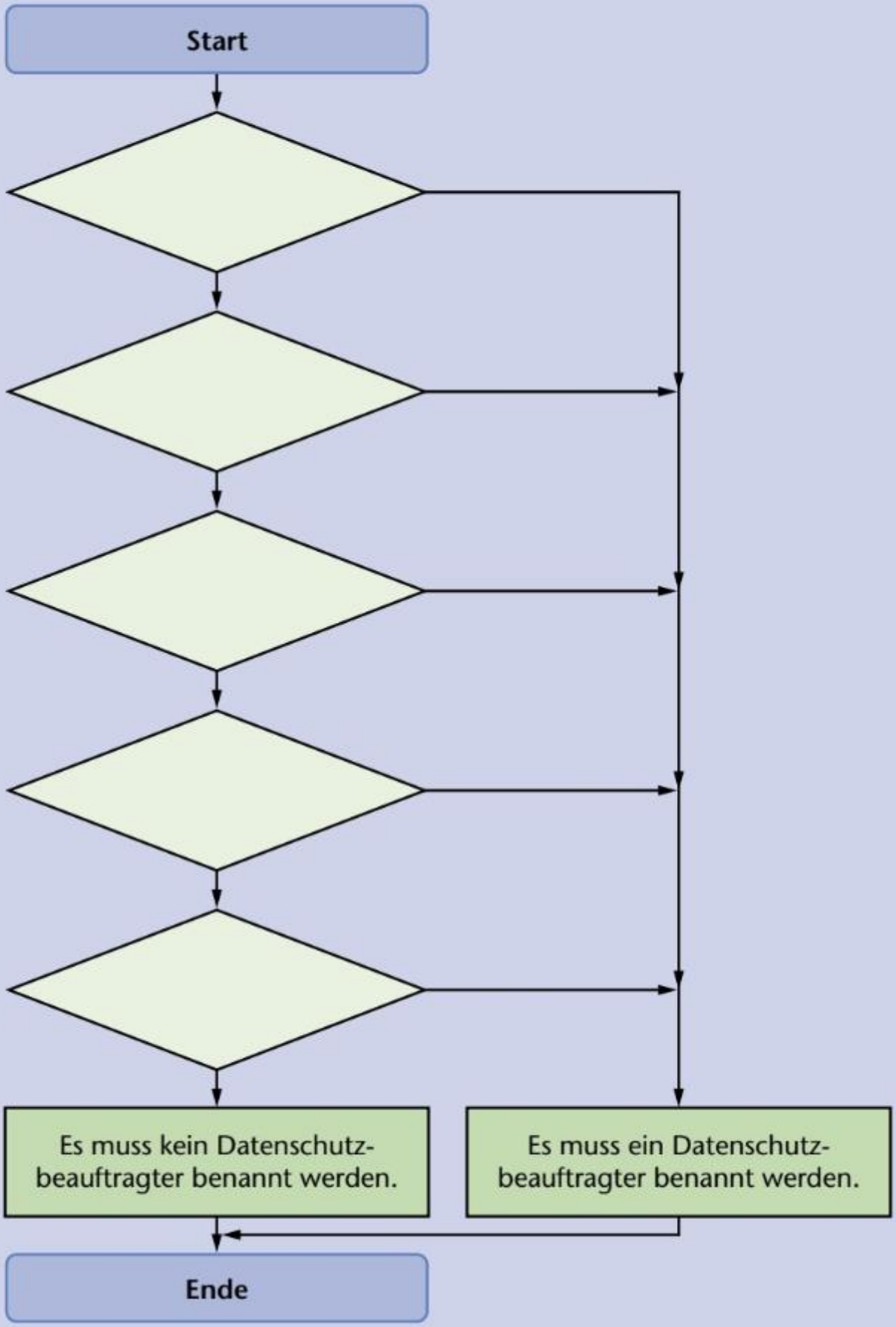
1. Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
   a) […]
   b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
   c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder […]

Art. 9 DSGVO

Verarbeitung besonderer Kategorien personenbezogener Daten

1. Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.
2. Absatz 1 gilt nicht in folgenden Fällen: […]

Benennung eines Datenschutzbeauftragten – Programmablaufplan:



Grundlagen 3

Ausgangsszenario:

Die IT-Firma ***ConSystem GmbH*** berät ihre Kunden auch im Bereich Datenschutz. Einige Kunden haben neue Projektideen, die auch mit der Verarbeitung personenbezogener Daten verbunden sind.

Aufgabenstellung:

Die Geschäftsleitung von ***ConSystem GmbH*** hat dem Leiter der Entwicklungsabteilung diese Projektideen übermittelt und bittet nun um eine Einschätzung, ob diese Projektideen datenschutzkonform sind. Als Auszubildender der Firma erhalten Sie den Auftrag, die Ideen zu prüfen. Als Grundlage hat Ihnen der Leiter der Entwicklungsabteilung den Artikel 5 der DSGVO zur Verfügung gestellt.

Art. 5 DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

1. **Personenbezogene Daten müssen**
   a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
   b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
   c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
   d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
   e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
   f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Projektidee 1:

Auf der Internetseite einer Firma sollen potenzielle Interessenten erfasst werden, die über das Produkt der Firma informiert werden sollen. Dazu sollen die Interessenten folgende Daten in einem Formular eingeben: *Name, Vorname, E-Mail, Telefon, Geburtsdatum und Familienstand*

Ihre Einschätzung:

Projektidee 2:

Eine Firma hat die Daten ihrer Kunden erfasst, die einen Wartungsvertrag abgeschlossen haben. Die Firma möchte diese Daten nutzen, um die Kunden auf interessante Angebote in anderen Bereichen, auch von Partnerfirmen, aufmerksam zu machen.

Ihre Einschätzung:

Projektidee 3:

Eine Firma hat Daten von Interessenten zu einem bestimmten Event erfasst. Dieses Event ist bereits durchgeführt worden. Die Firma möchte die Daten dieser Interessenten gerne weiter speichern, da es in der Zukunft möglich sein könnte, dass ein ähnliches Event durchgeführt wird.

Ihre Einschätzung:

Standard-Datenschutzmodell

Ausgangsszenario:

Die IT-Firma ***ConSystem GmbH*** berät ihre Kunden auch im Bereich Datenschutz. Einige Kunden brauchen Unterstützung bei der praktischen Umsetzung der DSGVO.

Aufgabenstellung:

Die Geschäftsleitung von ***ConSystem GmbH*** möchte ihren Kunden eine Übersicht zum Standard-Datenschutzmodell geben, um die Kunden bei der praktischen Umsetzung des Datenschutzes zu unterstützen. Dazu wurden die Gewährleistungsziele des Standard-Datenschutzmodells zusammengetragen und kurz erläutert. Als erfahrener Auszubildender der Firma erhalten Sie den Auftrag, einige wichtige Anforderungen den entsprechenden Gewährleistungszielen zuzuordnen.

Das Standard-Datenschutzmodell:

Allgemeine Beschreibung:

Das **Standard-Datenschutzmodell (SDM)** wurde von der Konferenz der Datenschutzbehörden des Bundes und der Länder entwickelt. Es ist eine Methode, um die Anforderungen der DSGVO praktisch umzusetzen – vor allem auch in technisch-organisatorischen Hinsicht. Dazu wurden so genannte Gewährleistungsziele vereinbart, in denen die Aspekte der DSVGO praktisch umgesetzt werden sollen.

Die Gewährleistungsziele:

Datenminimierung
Das Gewährleistungsziel Datenminimierung erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken.

Verfügbarkeit
Das Gewährleistungsziel Verfügbarkeit bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können.

Integrität
Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig, richtig und aktuell bleiben.

Vertraulichkeit
Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann.

Nichtverkettung
Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden.

Transparenz
Das Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

Intervenierbarkeit
Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen.

Ordnen Sie den Anforderungen der DSVGO die entsprechenden Gewährleistungsziele zu:

Anforderungen DSGVO	Gewährleistungsziel(e)
Zweckbindung (Art. 5)	
Datenminimierung (Art. 5)	
Richtigkeit (Art. 5)	
Speicherbegrenzung (Art. 5)	
Vertraulichkeit (Art. 5)	
Identifizierung und Authentifizierung (Art. 12)	
Belastbarkeit (Art. 32)	
Berichtigungsmöglichkeit von Daten (Art. 5)	

Datenschutzfreundliche Voreinstellungen (Art. 25)	
Verfügbarkeit (Art. 32)	
Löschbarkeit von Daten (Art. 17)	
Wiederherstellbarkeit (Art. 32)	
Einwilligungsmanagement (Art. 4)	
Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12)	