Unternehmen sind verpflichtet, angemessene Informationssicherheitssysteme zu installieren, wenn sie personenbezogene Daten verarbeiten. Eine wichtige gesetzliche Grundlage ist die Datenschutzgrundverordnung (DSGVO).

Datenschutz:
Im Vordergrund steht hierbei der Schutz personenbezogener Daten vor Missbrauch. Insbesondere Rechte wie „das Recht auf informationelle Selbstbestimmung“ sollen dadurch geschützt werden. Der Mensch sollte selber entscheiden können, was mit seinen persönlichen Daten geschieht. Aber gerade die Erhebung und Analyse von Daten stellt für die Wirtschaft, aber auch Geheimdienste, eine wichtige Informationsquelle dar. Der Schutz vor dem Missbrauch personenbezogener Daten soll z. B. durch Gesetze wie das Bundesdatenschutzgesetz (BDSG) oder die europäische Datenschutzgrundverordnung sowie durch die Implementierung von Datenschutzbeauftragten in Behörden und Unternehmen gewährleistet werden.
Die Datenschutzgrundverordnung (DSGVO) trat 2018 in Kraft und regelt den Datenschutz EU-weit. Es gibt aber einzelne Öffnungsklauseln, die den Mitgliedstaaten Gestaltungsmöglichkeiten geben. Das geschieht in Deutschland durch das Bundesdatenschutzgesetz (BDSG), das ebenfalls 2018 in Kraft trat. Neben der DSGVO und dem BDSG regeln Datenschutzgesetze der Bundesländer und bereichsspezifische Gesetze den Umgang mit personenbezogenen Daten, die in IT- und Kommunikationssystemen oder manuell verarbeitet werden.

- **Recht auf Auskunft: Artikel 5**
  Eine betroffene Person hat das Recht zu erfahren, ob personenbezogene Daten von ihr verarbeitet werden. Falls ja, so hat sie Auskunftsrecht über den Verarbeitungszweck, über die Kategorie der Datenerhebung, über die Empfänger der Daten, über die Dauer der Speicherung und über die Datenherkunft (sowie weitere Detailrechte).

- **Recht auf Berichtigung: Artikel 16**

  Eine betroffene Person hat das Recht auf sofortige Berichtigung oder Ergänzung nicht korrekter personenbezogener daten.

- **Recht auf Löschung: Artikel 17**
  - Eine betroffene Person hat das Recht auf sofortige Löschung der personenbezogenen Daten, sofern eine der folgenden Bedingungen zutrifft:
  - Die Daten sind für den Zweck der Erhebung nicht mehr notwendig
  - Die betroffene Person widerruft ihre Einwilligung oder legt Widerspruch ein und es ist keine andere Rechtsgrundlage für die Verarbeitung vorhanden.
  - Die Daten wurden unrechtmäßig erhoben
  - … weitere Detailrechte möglich

Aufgabe 1:

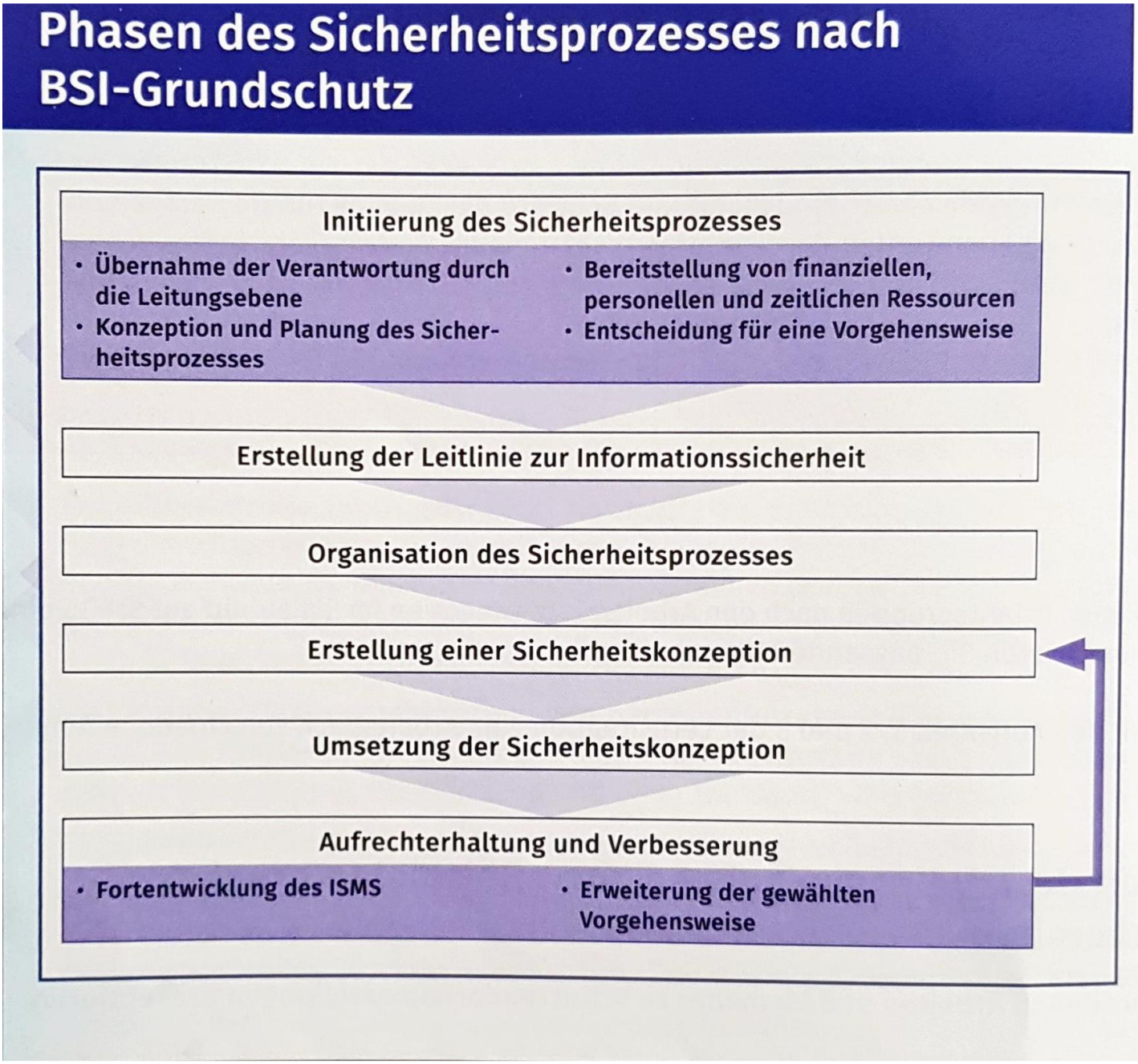
1. Überprüfen Sie, gegen welche Artikel (12-23) in nachfolgenden Beispielen verstoßen wurde:

Kundenbeschwerden		
1	Der Kunde erfährt nicht, bei welcher Behörde er sich beschweren kann.	
2	Das Unternehmen ist nicht bereit, Kundendaten auf Verlangen zu löschen.	
3	Das Unternehmen löscht Kundendaten nicht, die es zum Zweck nicht benötigt.	
4	Da die Löschung nicht möglich ist, verlangt der Kunde eingeschränkte Datennutzung.	
5	Der Kunde erfährt nicht, welche Daten an Dritte weitergegeben wurden.	
6	Das Unternehmen lehnt die Mitteilung anderer über die Löschung ab.	
7	Das Unternehmen ist nicht bereit, auf Wunsch zusätzliche Daten zu erfassen.	
8	Das Unternehmen sendet Daten auf Kundenwunsch nicht anderen Unternehmen.	
9	Das Unternehmen verweigert dem Kunden, unrichtige Daten zu berichtigen.	
10	Dem Kunden wird die Auskunft verweigert, an wen die Daten gegeben wurden.	
11	Der Kunde habe nicht das Recht zur Auskunft über die Dauer der Speicherung.	
12	Der Kunde erhält keine Information, dass andere seine Daten verwenden.	
13	Der Kunde erhält nur die Information, dass die Daten elektronisch gespeichert wurden.	
14	Der Kunde erhält auf elektronisches Verlangen keine Information.	
15	Der Kunde wird nicht über die werbliche Nutzung seiner Daten informiert.	
16	Die Kundendaten werden ohne Information über die Speicherung erfasst.	
17	Trotz Löschung senden anhängige Datenverarbeiter weiterhin Werbung.	
18	Ein älterer Kunde erhält eine englische Datenschutzgrundverordnung ausgehändigt.	

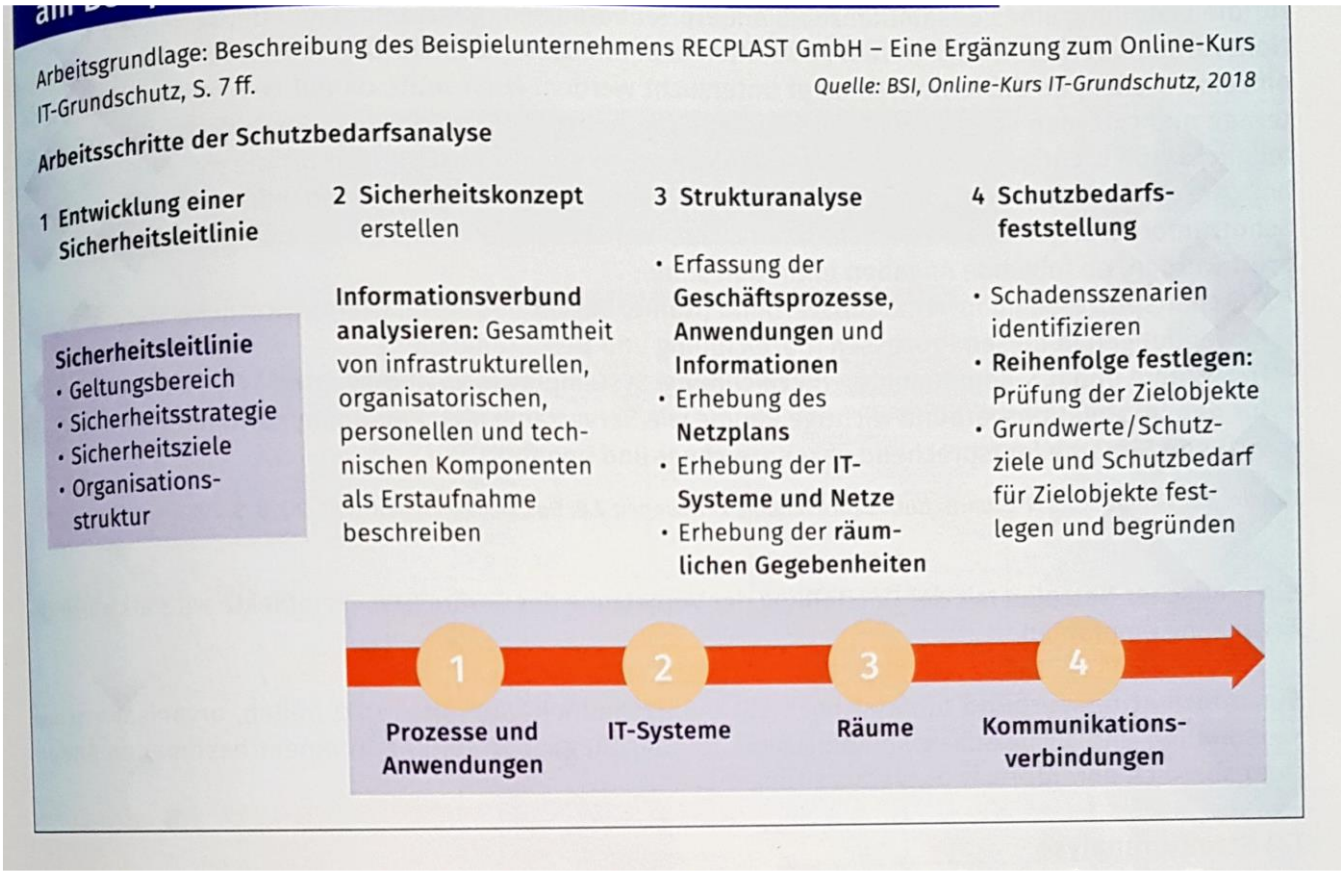
2. Geben Sie an, welche Stellung das Bundesdatenschutzgesetz (BDSG) zur DSGVO hat:

Nachdem Sie sich einen Überblick über wichtige gesetzliche Grundlagen und Schutzziele verschafft haben, geht es nun konkret darum, den IT-Sicherheitsbeauftragten zu unterstützen und die Zertifizierung nach ISO 27001 vorzubereiten.

Hierzu sind folgende Phasen zu durchlaufen:



Auf Grundlage der Sicherheitsleitline erfolgt die Erstellung eines Sicherheitskonzepts, die Strukturanalyse und die Schutzbedarfsfeststellung.



Aufgabe 2:

Als Auszubildender der IT Sol GmbH sollen Sie sich zunächst einmal einen Überblick über die wichtigsten Begriffe verschaffen.

1. Erläutern Sie die Begriffe „BSI“ und „IT-Grundschutz“:

2. Was ist eine Sicherheitsleitlinie im Vergleich zu einem Sicherheitskonzept?

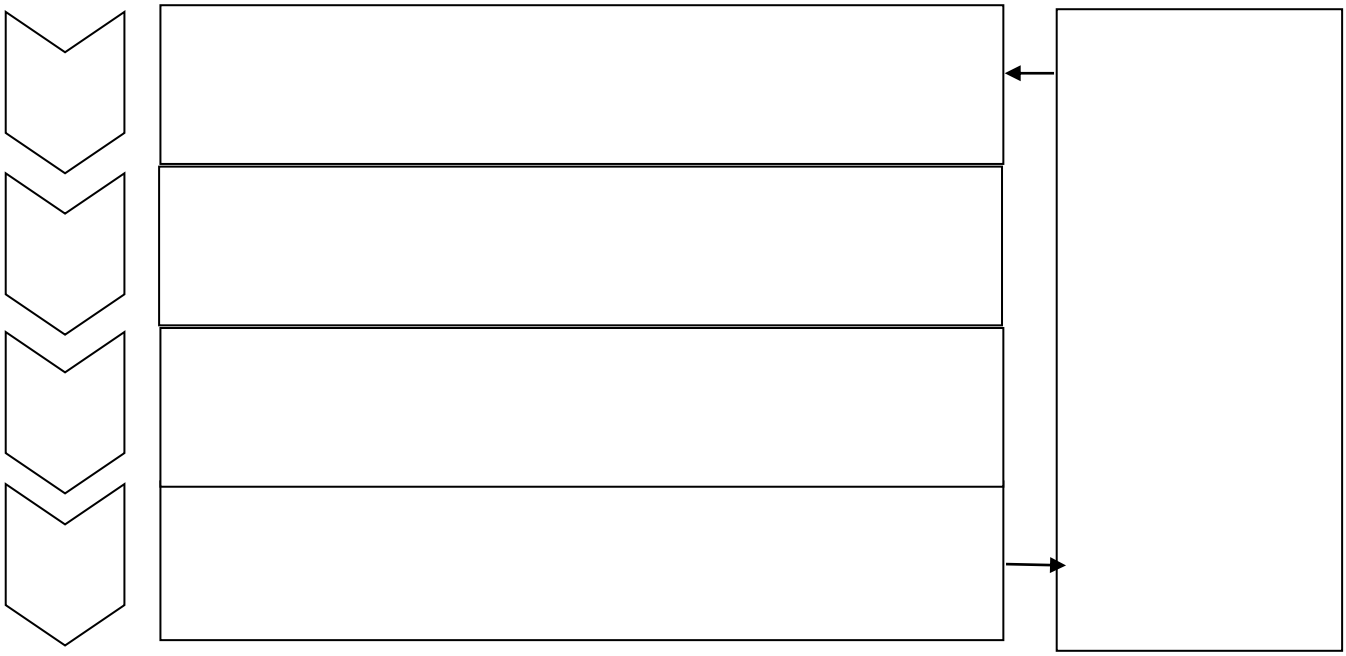
Aufgabe 3:

Im Rahmen des IT-Grundschutzes wird ein Sicherheitskonzept (Standard-Absicherung) vom BSI vorgeschlagen. Tragen Sie die Schritte dieser Absicherung in der korrekten Reihenfolge in das Diagramm ein.

Schritte:

- Auswahl der Sicherheitsanforderungen
- Analyse des IT-Zustandes
- Realisierung der Maßnahmen
- Aufrechterhaltung und kontinuierliche Verbesserung
- Schutzbedarfsfeststellung

Diagramm:



Welche Aufgaben hat ein Informationssicherheitsbeauftragter:

- ☐ Konfiguration der Sicherheitstechnik in der Firma
- ☐ Koordination der Entwicklung eines Sicherheitskonzeptes
- ☐ Berichte an die Geschäftsleitung über den aktuellen Stand der Informationssicherheit
- ☐ Frage der Presse oder interessierten Bürgern zum Stand der Informationssicherheit beantworten
- ☐ Leitung des Einkaufes der Software zur Abwehr von Schadprogrammen