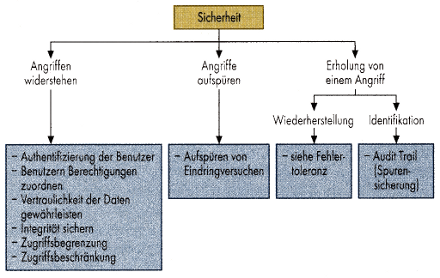
**Gewährleistung der Sicherheit der Anwendung und benutzerbezogenen Daten:**

* Einhaltung der DSGVO sowie der technischen Richtlinien des BSI
* Einhaltung der IT-Architekturrichtlinien zur Informationssicherheit:
  + Inbetriebnahme eines gültiges IT-Sicherheitskonzept gemäß BSI-Standards für IT-Grundschutz
    - regelmäßige Überprüfung des Sicherheitskonzeptes
    - ergibt sich aus Risikoanalyse & Mindeststandards nach § 8 BSIG
  + Festlegung der Schutzbedarf sowie der Anforderungen an Dienstgüte
    - regelmäßige Überprüfung des Sicherheitskonzeptes
    - besonders für Server der Cloud-Infrastrukturen
  + „Security by Design“ = zentrale Element einer ganzheitlichen Sicherheitskonzeption, um über alle Lebenszyklen eines IT-Verfahrens die passenden Informationssicherheitsanforderungen zu berücksichtigen
    - Grundsätze der sicheren Software-Entwicklung und Programmierung
  + Einsatz von aktuell zugelassenen kryptografischen Verfahren zur Verschlüsselung der Daten
    - nach BSI und DSGVO
    - Sicherstellung von Schutzzielen „Vertraulichkeit“ und „Integrität“
    - z.B. Secure Messaging = Verschlüsselungsverfahren mit Datenauthentisierung
  + Separierung, Segmentierung und Mandantentrennung
    - nach BSI-Standard 200-2 evtl. auch physische Separierung
    - Entgegenwirken von komplexen Angriffen in gemeinsam genutzter IT-Umgebung
    - einschlägige Cyber-Sicherheits-Empfehlungen des BSI als Empfehlung
  + Protokollierung, Monitoring und Detektion von sicherheitsrelevanten Ereignissen
    - Bezug zu Cyber-Angriffen
    - für spätere Analyse der Protokollierungsdaten
    - Mindeststandard „Protokollierung und Detektion von Cyber-Angriffen“
  + standardisierte Schnittstellen und Protokollformate
    - zur besseren Auswertung
  + sicheres Cloud-Computing
    - externen Cloud-Dienste müssen Anforderungen der einschlägigen Mindeststandards und IT-Grundschutz-Anforderungen des BSI erfüllen
    - notwendiger Bestandteil des ISM
  + Schadprogrammabwehr
    - Virenschutz- und Schadprogrammabwehrleistungen nach aktuellem Stand der Technik 🡪 Firewalls
    - Integraler Bestandteil der Sicherheitskonzeption im Sinne des ISM
    - Vorgaben gemäß § 8 BSIG, die Anforderungen aus IT-Grundschutz-Baustein „Schutz vor Schadprogrammen“ und weitere Empfehlungen des BSI sowie angebotenen Dienste von NdB
    - Anpassung an aktuelle Bedrohungsszenarien auch mit Bezug auf Clients
  + Sicherung von Daten
    - nächtliches Back-Up auf Sicherheitsserver in anderer System-Umgebung
    - tägliche Sicherung der Daten bei Verlust
  + Benutzerverwaltung
    - Authentifizierung der Benutzer
    - Benutzern explizit Berechtigungen zuordnen
  + Sicherung der Integrität
    - bspw. durch Prüfsummen

*Quelle:* [*https://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/architekturrichtlinie\_it\_bund\_2020.pdf?\_\_blob=publicationFile*](https://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/architekturrichtlinie_it_bund_2020.pdf?__blob=publicationFile)

[](https://raphaelbossek.files.wordpress.com/2010/10/abb80.png)