Für die **sichere Übertragung personenbezogener Daten im Internet** ist es grundsätzlich erforderlich, dass die Übertragungskanäle sicher sind, d.h. die dafür vorgeschriebenen Kriterien erfüllen:

- *Vertraulichkeit*: Sicherstellung, dass nur der Empfänger Kenntnis der ihm übermittelten Daten erhält,
- *Authentizität*: Sichere Zuordnung der übermittelten Daten zum Absender,
- *Integrität*: Sicherung der Unverfälschtheit der übermittelten Daten.

Eine Übertragung, bei der Teile des Transportweges außerhalb des Netzwerkes der Bergischen Universität liegen, ist daher eine *durchgängige* und *unterbrechungsfreie* Sicherung der transportieren Daten erforderlich!

Konkret bedeutet dies:

- E-Mail darf nur *Ende-zu-Ende-verschlüsselt* genutzt werden! Dies lässt sich durch sichere und vertrauliche E-Mail per *S/MIME oder PGP/MIME* erreichen oder dadurch, dass Daten in *bereits vorher gesicherter Form* als E-Mail-Attachment verschickt werden, also z.B. als per PGP gesicherte Anhänge.
- BSCW oder andere Client-Server-basierte Dienste, bei denen von außerhalb der Universität auf Server innerhalb der Universität zugegriffen wird, dürfen nur mit sicheren Anwendungsprotokollen wie *https* oder *sftp* genutzt werden, da nur dann die Transportverschlüsselung via TLS/SSL einen sicheren Datentransport zwischen dem Serverdienst in der Uni und dem Clientprogramm auf dem externen Rechner garantiert.
- Eine Zwischenspeicherung der Daten auf externen Datenspeichern (USB-Sticks, mobilen Festplatten, beschreibbaren DVD- oder BluRays-Datenträgern etc.) nur dann zulässig, wenn die Daten in verschlüsselter Form gespeichert werden, damit im Fall eines Verlusts oder Diebstahl des Datenträgers keine Datenschutzverletzung erfolgen kann.
- Für die Datenspeicherung auf mobilen Geräten gelten dieselben Regeln wie bei externen Datenträgern: Die Daten müssen in verschlüsselter Form gespeichert werden, am besten durch Verschlüsselung der gesamten Festplatten.
- Die Speicherung der Daten in Uni-externen Datenspeicherdiensten gelten zunächst dieselben Regeln wie bei externen Datenträgern: Diese dürfen nur dann genutzt werden, wenn Daten in verschlüsselter Form gespeichert werden, was durch Verschlüsselung einzelner Dateien z.B. mit PGP, Verschlüsselung von Datei-Archiven oder sichere Containerlösungen erfolgen kann.
  Für die Speicherung beliebiger dienstlicher Daten in der Cloud sind ausschließlich solche Dienste zulässig, deren datenschutzrechtliche Überprüfung durch die behördlichen Datenschutzbeauftragten der Universität erfolgt ist. Cloud-Speicherdienste wie DropBox, Amazon Drive, Microsoft Azure etc. dürfen *grundsätzlich nicht* für dienstliche Daten genutzt werden, da in diesem Fall personenbezogene, dienstliche oder vertrauliche Daten nicht mehr im Einflussbereich der Universität liegen!
  Die Nutzung der Campus-Cloud Sciebo für dienstliche Daten ist zulässig, wobei aber auch dieser Dienst ohne weitere technische Sicherungsmaßnahmen nicht für die Speicherung personenbezogener Daten genutzt werden darf., z.B. Cloud-Speicherdiensten bei externen Providern ist zu beachten, dass dies grundsätzlich dann nicht genutzt werden, wenn personenbezogene, dienstliche oder vertrauliche Daten gespeichert werden sollen, da in diesem Fall hochschulinterne, vertrauliche Daten nicht mehr im Einflussbereich der Hochschule liegen.