Mobile Geräte zur Weiterverwertung oder Entsorgung

Folgende Schritte dienen als Empfehlung (Checkliste) vor einer Übergabe, beispielsweise an eine andere Person, zur Entsorgung oder zur Weiterverwertung (z.B. Geräte Sammelboxen):

Grundsätzlich sollten alle persönlichen Daten, die sich im Laufe der Zeit auf dem Gerät angesammelt haben, vor einer Weitergabe gelöscht werden und das Gerät auf „Werkseinstellungen“ (Ursprungszustand) zurückgesetzt werden.

Abhängig vom Alter der Geräte und vom Hersteller, können sich die hier genannten Schritte sowie die Funktionen und die Namensgebung in den Auswahlmenüs unterscheiden.

1. Daten sichern!

Daten die für eine spätere Verwendung erhalten bleiben sollen, müssen gesichert werden.

Datensicherung durchgeführt?	
Datensicherung nicht erforderlich?	

2. SIM-Karte und Speicherkarten entfernen!

SIM-Karte entfernt? (Falls das Gerät eine SIM-Karte besitzt?)	
Speicherkarte entfernt? (Optional eingesteckten Speicherkarten?)	

3. Überprüfen ob das Gerät persönliche Daten verschlüsselt speichert!

Aktuelle Betriebssysteme (Android, iOS von Apple) verschlüsseln persönlichen Daten standardmäßig. Bei Android finden sich die Einstellungen unter Sicherheit und Verschlüsselung.

Falls keine Verschlüsselung aktiviert wurde, diese aber in den System-Einstellungen angeboten wird, sollte jetzt die Verschlüsselung aktiviert werden, damit alle persönlichen Daten verschlüsselt werden. Durch diese Maßnahme wird später beim „Zurücksetzen auf Werkseinstellung“ u.a. auch der erforderliche Schüsselcode zum Entschlüsseln entfernt.

Daten werden bereits verschlüsselt gespeichert?	
Daten werden nicht verschlüsselt gespeichert. Die Funktion wurde aktiviert?	
Das System biete keine Möglichkeit zur Verschlüsselung? (Punkt 5 beachten!)	

4. Geräte auf Werksteinstellungen zurücksetzen!

Die Funktion ist in der Regel unter den Einstellungen zu finden: z.B. Einstellungen – System – Suche nach dem Punkt „Zurücksetzen“ oder „Daten löschen“.

Dabei ist zu beachten, dass die Daten nicht in jedem Fall unwiederbringlich entfernt werden. Ein sicherer Löschprozess würde sehr viel Zeit in Anspruch nehmen, sodass in der Regel nur die „Verzeichnisdaten“ (Informationen wo die Daten technisch auf dem Datenträger zu finden sind) entfernt.

Für den Fall, dass die Daten bisher unverschlüsselt gespeichert waren, können die Informationen mit entsprechend technischem Aufwand rekonstruiert werden. Bei verschlüsselt gespeicherten Daten, ist ein Zugriff auf Daten ohne dem Schlüsselcode, der durch den Vorgang beim „Zurücksetzen“ sicher entfernt wird, nicht möglich.

Das Gerät wurde auf die Werkseinstellung zurückgesetzt?	

5. Speicher überschreiben

Bei dieser Methode können alte Datenextrakte mit Hilfe von großen Dateien, z.B. unkritische Videodateien, überschrieben werden. Das ähnelt dem sicheren Löschen von Festplatten, in dem der Datenträger mehrfach mit einem Muster überschrieben wird.

Der Gerätespeicher ist nicht verschlüsselt, der Speicher wurde überschrieben? Danach wurde Punkt 4 durchgeführt (Werkseinstellung zurückgesetzt)!	
Der Gerätespeicher war verschlüsselt, der Speicher wurde nicht überschrieben?	
Der Gerätespeicher war verschlüsselt, der Speicher wurde überschrieben? Danach wurde Punkt 4 durchgeführt (Werkseinstellung zurückgesetzt)!	

Weitere hilfreiche Quellen:

Daten auf Festplatten und Smartphones endgültig löschen:
https://www.bsi.bund.de/dok/6599236

Smartphone und Laptop verkaufen: Wie Sie Ihre Daten sicher löschen
https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/smartphone-und-laptop-verkaufen-wie-sie-ihre-daten-sicher-loeschen-89124