

## Bevor es losgeht:

Überprüfen Sie, ob Ihr Smartphone, Tablet oder der Laptop reisesicher sind:



- ✓ Nutzen Sie starke Passwörter und Zwei-Faktor-Authentifizierungen und haben Sie die aktuellsten Sicherheitsupdates installiert?
- ✓ Sind Backups von wichtigen Daten erfolgt und sind diese an einem sicheren Ort gespeichert?
- ✓ Können Geräte bei Verlust geortet werden? Haben Sie Informationen griffbereit, um die SIM-Karte sperren zu lassen und Konten zu schützen?

## Weitere Infos



- Jugendportal zum Thema Datenschutz und Informationsfreiheit
  - <https://youngdata.de/a/datenschutztz-im-urlaub-wie-deine-daten-im-ausland-sicher-sind>



- Mastodon-Kanal der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ)
  - Kampagne #KindersindkeinContent
  - <https://social.bund.de/@BzKJ>



- EU-Initiative zur Förderung der Online-Kompetenz der Menschen
  - <https://klicksafe.de>



## Datenschutz im Urlaub

Tipps für einen sicheren Umgang mit Ihren Daten.

**Info für die Fernreise**  
Zoll- und Grenzbeamte z. B. in China, den USA oder in Kanada können u. a. Smartphones und Laptops auf ihren Inhalt prüfen.

### Fragen zum Datenschutz?



Wenn Sie Fragen haben oder Unterstützung benötigen, wenden Sie sich gerne an die Landesbeauftragte für den Datenschutz, Frau Rost.

Landesbeauftragte für den Datenschutz  
des Landes Sachsen-Anhalt  
Otto-von-Guericke-Straße 34a  
39104 Magdeburg



Telefon: 0391 81803-0  
E-Mail: [poststelle@lfd.sachsen-anhalt.de](mailto:poststelle@lfd.sachsen-anhalt.de)

Stand: August 2025



SACHSEN-ANHALT

Landesbeauftragte  
für den Datenschutz

## Tipps für den Urlaub – Datensicherheit im Blick

- ✓ **Posten Sie** Ihren aktuellen Standort nicht öffentlich oder nur **mit zeitlicher Verzögerung**. Nicht alle sollten wissen, dass Sie nicht zu Hause sind.
- ✓ **Nutzen Sie** zum Online-Banking, Online-Shopping oder für E-Mails **keine öffentlichen WLAN-Netze**. Verwenden Sie mobile Daten, z. B. auch über einen persönlichen Hotspot. 
- ✓ **Laden Sie** Ihre Geräte **nicht an öffentlichen USB-Anschlüssen** auf, benutzen Sie den Netzstecker. Beim Laden nur mit dem USB-Kabel besteht das Risiko, dass Ihre Daten ausgelesen werden können oder das Gerät mit Schadsoftware infiziert wird.
- ✓ **Überprüfen Sie App-Einstellungen** auf Ihrem Smartphone. Manche Anbieter erstellen mit Ihren Standortdaten Bewegungsprofile zum Verkauf an Dritte. Inhalte aus Dating-Apps können in vielen Ländern (z. B. Ägypten) mitgelesen, teils kriminalisiert und polizeilich verfolgt werden. 
- ✓ **Bewahren Sie Reisedokumente** und wichtige elektronische Geräte (Smartphone, Tablet, Laptop) zum Schutz **sicher auf**, z. B. im Hotelsafe.

## Datenschutz – Wahren Sie Ihre Rechte

In der **Europäischen Union** sowie **Norwegen, Island und Liechtenstein** schützt die Datenschutz-Grundverordnung (DS-GVO) Ihre Rechte.



Ihre persönlichen und familiären Daten dürfen nur mit einer rechtlichen Grundlage verarbeitet werden.

**Wenn Sie unsicher sind**, welche Daten im Hotel oder bei Reiseveranstaltern abgefragt werden dürfen, **fragen Sie nach**. Die zuständige Person, die die Daten erhebt, muss Sie umfassend nach der DS-GVO über die Datenverarbeitung informieren. Die Datenerhebung muss notwendig sein, um z. B. den Reisevertrag mit Ihnen zu erfüllen.

**In Drittstaaten** (z. B. Türkei, USA, Ägypten) **gelten landesspezifische Regelungen**.

 Der Schutz vor Zugriffen auf Ihre persönlichen und familiären Daten durch staatliche Stellen ist allerdings oft nicht gegeben.

**Informieren Sie sich** über Ihr Reiseland vorab.

## Kinderfotos im Netz – Hochladen vermeiden

**Seien Sie sehr vorsichtig** beim Veröffentlichen von Fotos und Videos im Internet, insbesondere in sozialen Netzwerken wie Instagram, Facebook, Snapchat, Youtube, sowie im WhatsApp-Status.



**Alle fotografierten Personen** die auf den Bildern gut erkennbar und nicht nur zufällig darauf sind, **müssen mit dem Hochladen einverstanden sein**. Minderjährige können je nach Einsichtsfähigkeit selbst entscheiden. Die Sorgeberechtigten müssen zustimmen.



Die Bilder können **unkontrolliert** weltweit gesehen und **geteilt werden**. Sie können für **kriminelle Zwecke** missbraucht oder zur Bloßstellung der Kinder verwendet werden und dies auch noch nach vielen Jahren.

**Schützen Sie Ihre eigene Privatsphäre und die Ihrer Familie!**