UBINODES

RESEARCH DATA PRIVACY

GERMANY

VS

SWITZERLAND

Research: Data Privacy, Germany vs. Switzerland

When looking at data security in European countries, Germany and Switzerland stand out. Here are the differences between these two nations when it comes to data security and related issues:

Disclaimer: We want to clarify that we have no affiliation with any of the companies mentioned in this article. Our content is based solely on independent research and findings. There is no affiliate marketing associated with the provided links below for your convenience.

How we write our reviews: For an impartial and comprehensive review, all apps undergo the following testing procedures:

- Real-time usage on actual projects.
- Evaluation by diverse team members situated in different countries.
- Testing on various devices and operating systems.
- A minimum of two weeks, with an average duration of four weeks.
- Peer review by multiple team members, followed by submission to the app's publisher for a final review.

In today's world, privacy has become a hotly debated issue. Governments are under scrutiny for privacy violations, and individuals or organizations are illicitly obtaining sensitive information worldwide. Protecting this data has become crucial for both businesses and individuals.

The location of servers and service providers plays a crucial role in ensuring the security of sensitive information. Due to concerns about government surveillance in countries like the United States and China, many people consider Europe a preferable choice. When it comes to data security, relying on the developed world is often seen as a wise decision.

1. History, Culture and Mutual Agreements:

1.1 Germany:

1.1.1 Pros:

- A troubled history marked by ongoing state surveillance within the government.
- A legacy of resistance against governmental oppression.
- A public stance firmly opposing the provision of information to foreign intelligence.

1.1.2 Cons:

- Vulnerable to laws and pressures imposed by the EU.
- The German Intelligence Agencies are known for sharing data with other intelligence agencies.

1.2 Switzerland:

1.2.1 Pros:

- Troubled history with pervasive state surveillance within the government.
- A culture of secrecy rooted in the banking sector.
- Not directly subjected to EU laws.

1.2.2 Cons:

- Limited advancement in cyber-security legislation.
- Lack of specific legislation addressing cyber-security or cyber-crime.
- A history of government monitoring of private information of businesses and individuals.

Switzerland maintains mutual legal assistance treaty relationships with the United States, which require foreign governments to provide any legally available information to their local authorities upon request.

Germany has a significant history of state surveillance, leading to a pervasive wariness of government overreach among generations of the German people. Switzerland also has a history with state surveillance, notably the secret files scandal of 1981. However, this scandal revealed mass surveillance rather than a prolonged experience of governmental oppression. As a result, the impact of historical surveillance practices is more pronounced in Germany than in Switzerland.

2. National Laws:

2.1 Germany:

2.1.1 Pros:

- Within the EU, data privacy regulations rank among the most stringent globally.
- The German Constitution guarantees citizens' right to privacy.
- Strict regulations mandate the storage of metadata only within the country.
- The Federal Data Protection Act (Bundesdatenschutzgesetz) is designed to ensure data security.
- General surveillance is prohibited by EU law.

2.1.2 Cons:

- Laws allow data retention for up to 10 weeks, excluding emails.
- Specific statutes mandate the retention of business documents for 6–10 years.

2.2 Switzerland:

2.2.1 Pros:

- Switzerland has generally stringent privacy laws.
- Not obligated by the EU to Pan-European agreements for data sharing.
- The Swiss Data Protection Act safeguards access to locally stored data.
- In cases where courts grant access to otherwise inaccessible data, parties must be notified and provided with an opportunity to contest.

2.2.2 Cons:

Swiss email providers are required to retain user data for a minimum of 6 months. In 2016, 65.5% of Swiss voters supported a stricter surveillance law. Switzerland is currently considering a revision to its data retention law (BÜPF) to extend the storage duration of all communication data (post, email, phone, text messages, IP addresses) to 12 months.

From a legal perspective, Switzerland has set precedents that make communications and stored data there more susceptible to government and related party access. In contrast, German laws are explicitly more protective of the privacy rights of individuals and organizations. In Switzerland, data security is more implicitly ingrained in the culture, which is subtle yet prevalent.

3. National Technology and Infrastructure:

3.1 Germany:

- Advanced IT infrastructure.

3.2 Switzerland:

Both Switzerland and Germany have sophisticated IT infrastructures, with significant areas dedicated to IT hosting. However, Switzerland stands out with repurposed bunkers and underground tunnels providing secure data storage. Additionally, Switzerland offers affordable electricity, leading to lower overall costs, which makes it particularly appealing to larger organizations.

4. Sources

- **Secret files scandal:**
  https://en.wikipedia.org/wiki/Secret_files_scandal
- **Switzerland votes in favor of greater surveillance:**
  https://www.theguardian.com/world/2016/sep/25/switzerland-votes-in-favour-of-greater-surveillance
- **Telecommunications data retention:**
  https://en.wikipedia.org/wiki/Telecommunications_data_retention#Switzerland
- **Federal data protection act in Germany:**
  https://en.wikipedia.org/wiki/Bundesdatenschutzgesetz
- **Data Security in Switzerland:**
  https://www.digitaltrends.com/computing/switzerland-data-security/
- **The EU's highest court rules against data retention:**
  https://tutanota.com/blog/posts/eu-ruling-data-retention
- **MR. Robot uses Protonmail but it still isn't fully secure:**
  https://www.wired.com/2015/10/mr-robot-uses-protonmail-still-isnt-fully-secure/
- **Swiss civil society struggles against digital surveillance laws:**
  https://edri.org/swiss-civil-society-struggles-digital-surveillance-laws/