EE2E.app

End to End Encryption

EE2E.app Licensing Requirements

Requirements:

1. Two servers controlled by and paid by client. We provide a list of server hosts in countries with decent privacy laws
2. Domain name controlled by client. Access to domain name host for 22E2.app software developers to set up software and DNS. If client does not have a domain name aka URL, client must purchase a domain name.
    - If client is licensing software that is already set up on a domain name, client must have a domain name provider for EE2E.app to transfer the domain name to client name. EE2E.app will not keep domain name under the ownership name of EE2E.app
3. Optional Cloudflare.com account (Cloudflare offers free plans). Access to the client Cloudflare account for 22E2.app software developers to set up software and DNS
4. A signed and agreed to EE2E.app licensing agreement, the **EE2E.app PDF agreement**
5. 50% of payment required upfront and 50% required after delivery of software by EE2E.app and client meeting ALL Requirements listed above.

Software Delivery

Delivery of the EE2E software is 1 business day to 5 business days from initial date of payment providing client has met all Requirements.

Countries with Top Privacy Laws,

Decent Internet Speed

and Server Hosts to Host EE2E.app Software

Privacy and confidentiality are important to some businesses and to some people in general. Free speech is a staple of society.

With that said, there are some countries EE2E.app will not host its software because our software is end to end encrypted and some countries are potentially not as receptive to our software.

Within the pages of this document, we provide links to research to select the best countries with top privacy laws "combined" with decent internet speed to host your EE2E.app software. Please do your own diligence and research, this is only our preferred options.

Our top countries we choose

to host EE2E.app software:

1. Iceland
2. Denmark
3. Brazil
4. Norway
5. Japan
6. Portugal
7. Canada

Our Preferred Server Hosts

1. Iceland
2. Denmark
3. Brazil
4. Norway
5. Japan
6. Portugal
7. Canada

2025 Internet Privacy Laws from Express VPN

https://www.expressvpn.com/blog/10-countries-with-top-data-privacy-laws/

In recent years, we've seen great strides in the implementation of data privacy laws around the world.

Any country in the European Union already has a leg up, thanks to its **General Data Protection Regulation** (GDPR), enacted in 2018 and governing the collection of personal information ranging from someone's phone number and biometric data to IP address.

And earlier this year the **California Consumer Privacy Act** (CCPA), which bears similarities to GDPR, came into force—and state residents have **just voted to strengthen it**. This legislation represents a promising framework for other parts of the U.S., if not also for laws on the federal level.

Here's a look at nine countries with strong data privacy laws.

Iceland

Iceland is part of the European Economic Area, which means it's GDPR compliant, but it has strong laws of its own. Its Data Privacy Act requires organizations to only collect personal data for legitimate purposes and with individuals' consent, and penalties for violation reaching three years in prison.

But the country is also particularly known for its protections for investigative journalism and whistleblowers. In 2010, the Icelandic Modern Media Initiative was adopted with an aim to strongly position the country "legally with regard to the protection of freedoms of expression and information." The idea was conceptualized with the involvement of WikiLeaks.

Denmark

Denmark protects the privacy of its citizens with a government agency called the Danish Data Protection Agency, which works off of the 2000 Act of Processing Personal Data. This law says that personal data can only be collected if the user gives explicit consent and can't be disclosed to third parties for marketing purposes without consent.

Brazil

Brazil's inclusion here is more about the country's future than its track record. This August, the Lei Geral de Proteção de Dados, a law **clearly inspired by the GDPR**, came into effect. The law itself isn't necessarily revolutionary, but the penalties for breaking it will give companies pause. Those found in breach of it could face fines of up to 2% of their total revenue in Brazil in the previous year or up to 50,000,000 reals (approximately 9.25 million USD), whichever is higher.

Norway

The GDPR is part of Norwegian law thanks to its inclusion in the European Economic Area, but the country already had a strong history of data privacy protections. Its Personal Data Act is particularly robust: If you're seeking to collect data from a Norwegian user you need to first inform the individual of your name and address, the purpose of the data collection, whether said data will be given to third parties, the fact that participating is voluntary, and what their rights are under the law.

Japan

Japan has strong data privacy laws comparable with GDPR, to the extent that there is an agreement on reciprocal adequacy between Japan and the EU for specifically identified companies within these countries. Japan's data privacy protection extends to commercial companies operating outside of the country that process Japanese citizens' personal information. It also protects any personal information of non-residents when processed in Japan.

Canada

The country's primary protections come from the Personal Information Protection and Electronic Data Act, which require privacy policies to detail the collection, handling, and use of personal information, and the policies must be easy to find and understand. PIPEDA is built on a list of **10 guiding principles** surrounding personal information, and the government provides a **Privacy Guide for Business** to help corporations operating in the country comply.

Portugal

Portugal gets its privacy cred from its straightforward Act on the Protection of Personal Data., which dictates that personal data can only be collected after obtaining the "unambiguous consent" of the user. Transparency is a point of emphasis, as the user needs to be provided with the identity of who is processing their data, the purpose of said process, and any other recipients.

While the country uses a biometric ID card that stores fingerprint information, the system has been praised for the way it protects users' privacy. A fingerprint is only stored on the card itself, not on any central database, which is prohibited by Portuguese law. To confirm someone's identity, the system simply confirms whether an individual's fingerprint matches the one stored on the card.

Switzerland

Switzerland is a hotbed for cloud storage as its laws and values mesh with the needs of corporations whose businesses center around data privacy. The country's constitution guarantees individual privacy, with the Federal Data Protection Act requiring companies to tell users they're collecting their personal data and why.

Internet Speed from Data Pandas

Countries with Top Privacy Laws Highlighted

https://www.datapandas.org/ranking/internet-speed-by-country

Country	Broadband Speed	Mobile Speed
Singapore	345.33 Mbps	160.56 Mbps
United Arab Emirates	313.55 Mbps	543.91 Mbps
Hong Kong	312.48 Mbps	84.61 Mbps
Iceland	295.55 Mbps	
France	290.75 Mbps	133.66 Mbps
United States	279.93 Mbps	167.85 Mbps
Chile	279.53 Mbps	73.05 Mbps
Denmark	254.75 Mbps	198.48 Mbps
Spain	247.94 Mbps	79.21 Mbps
Switzerland	245.39 Mbps	101.16 Mbps
China	244.67 Mbps	174.46 Mbps
Thailand	238.41 Mbps	101.89 Mbps
Canada	237.86 Mbps	106.93 Mbps

Romania	237.61 Mbps	76.58 Mbps
Macau	232.74 Mbps	
Israel	229.65 Mbps	58.23 Mbps
Taiwan	226.37 Mbps	117.93 Mbps
Japan	217.11 Mbps	63.74 Mbps
Hungary	215.3 Mbps	68.85 Mbps
Portugal	207.95 Mbps	128.56 Mbps
Netherlands	202.75 Mbps	173.49 Mbps
Peru	200.79 Mbps	32.16 Mbps
South Korea	199.34 Mbps	205.27 Mbps
Kuwait	193.53 Mbps	309.07 Mbps
Qatar	192.83 Mbps	522.48 Mbps
Liechtenstein	188.07 Mbps	
Brazil	188.06 Mbps	205.92 Mbps
Poland	183.02 Mbps	94.37 Mbps

Sweden	178.91 Mbps	110.3 Mbps
Luxembourg	178.4 Mbps	148.34 Mbps
New Zealand	175.54 Mbps	106.79 Mbps
Panama	168.44 Mbps	31.33 Mbps
Jordan	168.38 Mbps	47.34 Mbps
Colombia	166.19 Mbps	31.21 Mbps
Vietnam	164.77 Mbps	144.5 Mbps
Malta	163.28 Mbps	
Uruguay	154.17 Mbps	
Norway	153.33 Mbps	162.37 Mbps
Ireland	148.37 Mbps	45.64 Mbps
Moldova	147.9 Mbps	52.44 Mbps
Finland	146.6 Mbps	140.01 Mbps
United Kingdom	135.66 Mbps	69.77 Mbps
Malaysia	135.64 Mbps	168.94 Mbps

Trinidad and Tobago	124.5 Mbps	
Saudi Arabia	121.87 Mbps	199.44 Mbps
Costa Rica	119.19 Mbps	52.25 Mbps
Belgium	116.69 Mbps	95.86 Mbps
Ecuador	110.44 Mbps	34.6 Mbps
Austria	100.45 Mbps	98.99 Mbps
Barbados	97.36 Mbps	
Cyprus	97.22 Mbps	114.06 Mbps
Slovenia	97.18 Mbps	118.81 Mbps
San Marino	96.82 Mbps	
Montenegro	96.78 Mbps	90 Mbps
Germany	96.33 Mbps	68.51 Mbps
Latvia	96.09 Mbps	132.72 Mbps
Paraguay	95.79 Mbps	
Philippines	94.4 Mbps	58.83 Mbps

Info by Privacy HQ

https://privacyhq.com/news/world-data-privacy-rankings-countries/

Who have we excluded?

While there are currently 194 countries globally, the UN report that only 128 have any form of data privacy legislation or regulations. This leaves 66 countries that offer their citizens no legal data privacy protection. These include some of the larger countries where internet use is rapidly expanding and established centers for commerce. The list includes:

- Afghanistan
- Bangladesh
- Belize
- Botswana
- Burundi
- Cambodia
- Cameroon
- Central African Republic
- Congo
- Cuba
- Dominica
- Egypt
- El Salvador
- Eswatini
- Ethiopia
- Fiji
- Guatemala
- Guinea-Bissau
- Guyana
- Haiti

- Iraq
- Jordan
- Liberia
- Libya
- Malawi
- Maldives
- Mozambique
- Myanmar
- Namibia
- North Korea
- Pakistan
- Papua New Guinea
- Rwanda
- Saudi Arabia
- Seychelles
- Sierra Leone
- Somalia
- South Sudan
- Sri Lanka
- Sudan
- Syria
- Timor-Leste
- Uganda
- Tanzania
- Venezuela
- Zimbabwe

Who are the top 5?

Based on the ranking criteria we have set out, the results of our qualitative assessment have identified the following top five countries

The European Union

OK, so the European Union isn't a country. Still, its member states all have data privacy regulations that encompass GDPR with minor tailoring to the rules in areas such as national security. As such, rankings of data privacy protections would be dominated by a list of EU member states. This is why we've grouped them all together. It's also worth mentioning that although the UK is no longer an EU member state, its data privacy regulations have not changed since it was a member. They continue to incorporate the GDPR principles with no immediate plans for change.

The European Union is arguably home to the countries with the best data privacy with the introduction of the GDPR into all member states' data protection legislation. It defines strict limits to what anyone who manages personal data can and cannot do. It enshrines individuals' rights into laws backed up with financial and criminal penalties for wrongdoing. The main feature of GDPR beyond previous privacy laws was all EU citizens' personal data was protected. This protection is irrespective of where that personal data is collected, processed, or stored. This had enormous implications for US companies with European customers. They were required to comply with regulations outside of their own legal jurisdiction. This prompted many companies to move the processing and storage of European customers' data into European located facilities. It even results in some US companies ceasing to deal with customers in the European Union.

Iceland

Iceland has a long history of data privacy regulations. Although it is not part of the European Union, its legislation was updated to incorporate all the requirements of GDPR, so it provided its citizens with the same levels of protection. However, the regulations are backed with financial and criminal penalties for non-compliance, with the potential for a three-year jail sentence for the most severe violations. This has gained it a reputation for being one of the world's best countries for data privacy.

Norway

Norway has implemented robust data privacy regulations. Although it is not part of the European Union, its legislation addresses the requirements of GDPR. It is designated by the EU as having equivalence. The regulations are focused on protecting individuals' data privacy and freedoms of speech. They include provisions for additional safeguards for

personal data related to legal and medical information. Monitoring of protection compliance is the responsibility of the Norwegian Data Protection Authority. As an independent public authority, it can impose financial penalties for non-compliance.

Japan

Japan has strong data privacy laws comparable with GDPR, to the extent that there is an agreement on reciprocal adequacy between Japan and the EU for specifically identified companies within these countries. Japan's data privacy protection extends to commercial companies operating outside of the country that process Japanese citizens' personal information. It also protects any personal information of non-residents when processed in Japan.

Switzerland

Switzerland has guaranteed its citizens the right to privacy under its constitution and enacted regulations. The Swiss Federal Data Protection Act (DPA) prohibits personal data processing without the individual's consent the data relates to. While these regulations are comparable with GDPR and have been assessed as adequate by the EU, there are significant differences. Individuals have fewer rights to how data is handled once consent has been given. Some rights regarding correction and deletion of personal data are covered outside of the data privacy regulations through Swiss civil law. Also, the penalties for violation of the data privacy regulations are less severe than for GDPR.

Who are the bottom 5?

Based on the ranking criteria we have set out, our qualitative assessment of the countries with privacy protection has identified the following bottom five countries. Those countries without any privacy protection legislation are not listed. Indeed, countries that do not allow citizens' privacy rights, such as North Korea, are also not included here.

Malaysia

With its development as a regional center for a wide range of business sectors, Malaysia offers its citizens' data privacy protections through the Personal Data Protection Act (PDPA). This is comparable with the EU's GDPR for personal data that is processed within Malaysia. However, through its national identity card scheme, the Malaysian government collects personal and biometric information on all citizens with little control over how that data is used and shared. The shared information includes sensitive medical and financial information. This is aggregated in a single location all the information a malicious person would need to commit identity theft, fraud, embezzlement, and coercion. Security controls are also lacking in some Malaysian organizations, with recent major data breaches of

patient records and customer information in the telecommunications and air travel sectors.

India

India has no single comprehensive data privacy regulations. Instead, various aspects that fall under data privacy protection are distributed amongst other legislation that does not have a data privacy focus. This includes specific rules covering the banking and healthcare sectors. There is also no particular authority is responsible for enforcing data privacy regulations. India has a prominent position in the off-shore data processing market. However, its data protection regulations have been assessed by the EU as not providing an adequate level of protection. Privacy is also compromised by linking the national Aadhaar based biometric identity card with personal information, including financial details. This has raised concerns that the government would have complete access to each citizen's online activities, including purchases, travel booking, and financial transactions. Also, reported breaches of information from government systems have demonstrated controls to protect this enormous aggregation of personal data collected from the citizens are inadequate.

Thailand

Thailand could join the countries with adequate data privacy protection thanks to the Personal Data Protection Act (PDPA). This would bring in controls equivalent to GDPR, backed with financial and criminal penalties. However, although this act has been approved by the National Legislative Assembly, a royal decree has delayed its introduction. This highlights the limitations of regulatory controls in the country and their ability to be bypassed. The Thai government has also enacted some of the strictest censorship laws that severely restrict freedom of expression. Custodial sentences are routinely applied to those arrested and prosecuted for publishing views that violate the government rules. These include criticizing a member of the Thai monarchy. They also include simply agreeing with such sentiments. The Thai government also routinely monitors online activity on a mass scale.

Russia

Russia undertakes widespread monitoring of the online activity of internet users. It has some of the strictest laws on where commercial organizations operating within Russia can store personal data to maximize state monitoring capabilities. There are moves towards creating a state-controlled internet service where only approved services are permitted, and content can be more easily censored. The Russian Federal Law on Personal Data provides citizens with data privacy protection from commercial organizations. These

include rights to access their personal data and limited controls on how the data may be used. However, where personal data has been lawfully collected, individuals have very little control over how it may be used. Rules are mainly restricted to processing related to direct marketing.

China

China has strict access controls and undertakes widespread monitoring of internet users' online activity, offering little to no privacy from state agencies. This includes restrictions on where commercial organizations operating within Chinese territories can store personal data to maximize state monitoring. Of most significant concern is that data interception, collection, processing, and sharing by state agencies has no judicial oversight, court orders are not required. However, China has recently introduced a cybersecurity law and guidance in the form of a Personal Information Security Specification to govern how commercial organizations manage customer data. While the regulations are simple compared to the EU's GDPR, it represents a recognition that personal data requires protection from misuse by commercial and criminal organizations. There are significant weaknesses. For example, data retention specifies minimum periods but not maximums. There are also no controls on sensitive private data. For example, medical records can be used for research purposes without consent. On the plus side, the movement towards consumer protection is expected to be followed by positive changes in other countries in Asia that look towards China for direction or are influenced by its behavior.

Where is the US and Canada in the rankings?

The US may be the home to most large online organizations, but it has some of the least integrated data privacy regulations. There are currently no countrywide federal data privacy regulations in place. Instead, rules exist for specific business sectors such as the Health Insurance Portability and Accountability Act (HIPAA) or Gramm–Leach–Bliley Act. Some states also have regulations such as the California Consumer Privacy Act (CCPA) and the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act. There are plans for federal privacy regulations with the proposed Data Care Act, which, if enacted, would help consolidate data privacy protections for US citizens. Currently, laws vary significantly from state to state. Commercial organizations are given free rein to self-police data collection and processing processes, often to their advantage rather than individuals' protection.

Canada has reasonable data privacy laws but is currently making them more robust, bringing them into line with GDPR by bringing in the Digital Charter Implementation Act. This will draw on the Consumer Privacy Protection Act and the Personal Information and

Data Protection Tribunal Act to provide comprehensive data privacy regulations. The legal protection will be backed up with financial penalties similar to GDPR in scope. However, individual provinces in Canada also have different data privacy regulations that complicate enforcement and compliance.