

# **Personal Data in the Cloud**

## **A GUIDE BY INTERNET VIKINGS**



# CONTENTS

---



**Cloud compliance and a future-proof cloud service**



**How GDPR and the CLOUD Act affect your storage of personal data in the cloud**

→ **About GDPR**

→ **About the CLOUD Act**

→ **Privacy Shield**

→ **How this affects iGaming**



**Achieving and securing cloud compliance as an iGaming operator**



**Checklist for the correct handling of personal data**

# **CLOUD COMPLIANCE** and a future-proof cloud service

**A lot of general expectations and business realities were upended in 2020. It's no longer enough to rely on your land-based business as your only source of income.**

**Every level of operations was affected by change, and the one thing that remains stable is the dynamic growth of online activities that need to be supported by high-level secure storage for your data.**

**Nevertheless, with change comes opportunity, and the cloud makes nearly everything possible. But only with an eye towards innovation can we future-proof our businesses.**

**To get it right, we need to evaluate all the risks, understand all the relevant legal aspects, and use that knowledge to build the systems that will support our businesses against uncertainty.**



# HOW GDPR AND THE CLOUD ACT affect your storage of personal data in the cloud

**Most organizations already use some form of cloud service or are in the process of moving parts of their IT environment to the cloud.**

**This means that your data, including the personal data that is stored and processed, ends up in the care of your cloud service provider.**

**That, in itself, is somewhat self-evident.**

**But, when we talk about the storage and handling of personal data in the cloud, it is important to also highlight the implications of EU-common legislation GDPR and the U.S. CLOUD Act.**



# GDPR

**General Data Protection Regulation (GDPR) is a regulation in EU law, in force since 2018, on data protection and privacy within the EU and the EEA. It provides mandatory rules on how organizations and companies must handle personal data.**

**Personal data means any information which, directly or indirectly, identifies a living person.**

**GDPR's main function is to protect EU citizens by ensuring the individual's right to privacy and control over his or her personal data.**

**It is allowable to move personal data between EU countries, as the legislation applies to all countries in the area.**

**However, to move personal data outside the EU, it is required that either the recipient country is already approved by the EU or that a separate agreement has been established with the entity, guaranteeing the data is protected within the provisions of the GDPR.**



# THE CLOUD ACT

**Clarifying Lawful Overseas Use of Data Act, or the CLOUD Act, is a U.S. law enacted in 2018 that both protects individual privacy and gives U.S. authorities, in the event of a suspected crime, the right to request personal data and other data from U.S. cloud service providers. This applies even if this data is stored outside the U.S.A. (For example, within the EU.)**

**The CLOUD Act also empowers the United States government to enter into new bilateral agreements with other governments that would enable law enforcement agencies to access data across each other's borders.**



# PRIVACY SHIELD

Privacy Shield is a framework approved by the European Union and the U.S. government for complying with EU data protection requirements when personal data for commercial purposes is transferred between the United States and the European Economic Area (EEA).



One of its purposes was to enable US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect European Union citizens.

However, on the 16th of July, 2020, the Court of Justice of the European Union (CJEU) declared, in a case called Schrems II, that Privacy Shield did not provide enough protection for the transfer of personal data between the EU and the U.S.

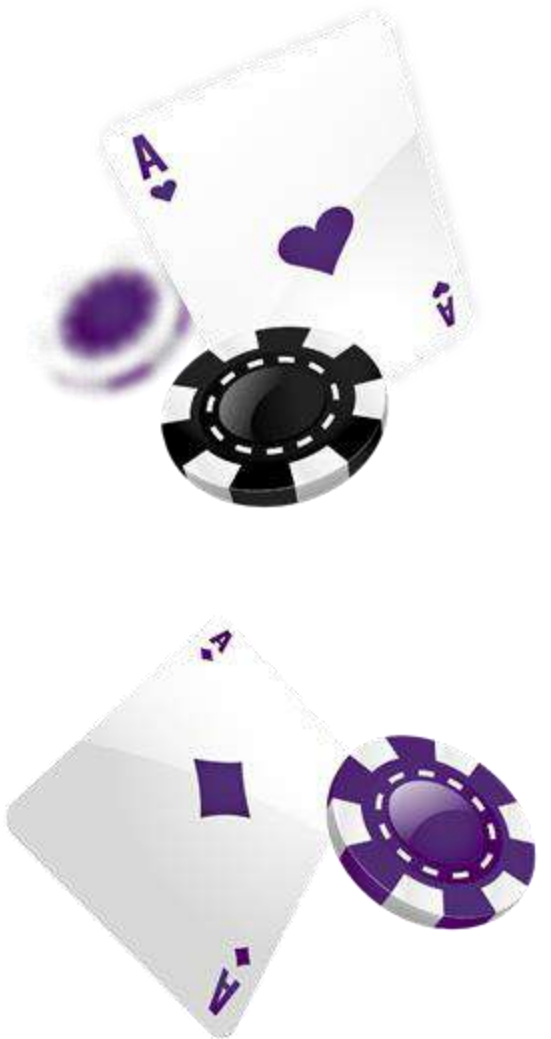


## HOW THIS AFFECTS iGAMING

**The potential conflict between GDPR and the CLOUD Act regulations, in the absence of Privacy Shield protection, could pose serious legal concerns for European organizations and companies that use and store information with U.S. cloud service providers (that are necessarily subject to U.S. legislation).**

**If U.S. authorities exercise their rights under the Act (for example, placing demands on a U.S. cloud provider for the disclosure of personal data), this would be in direct conflict with GDPR as such a transfer is not permitted under GDPR regulation, at least not without a separate agreement.**

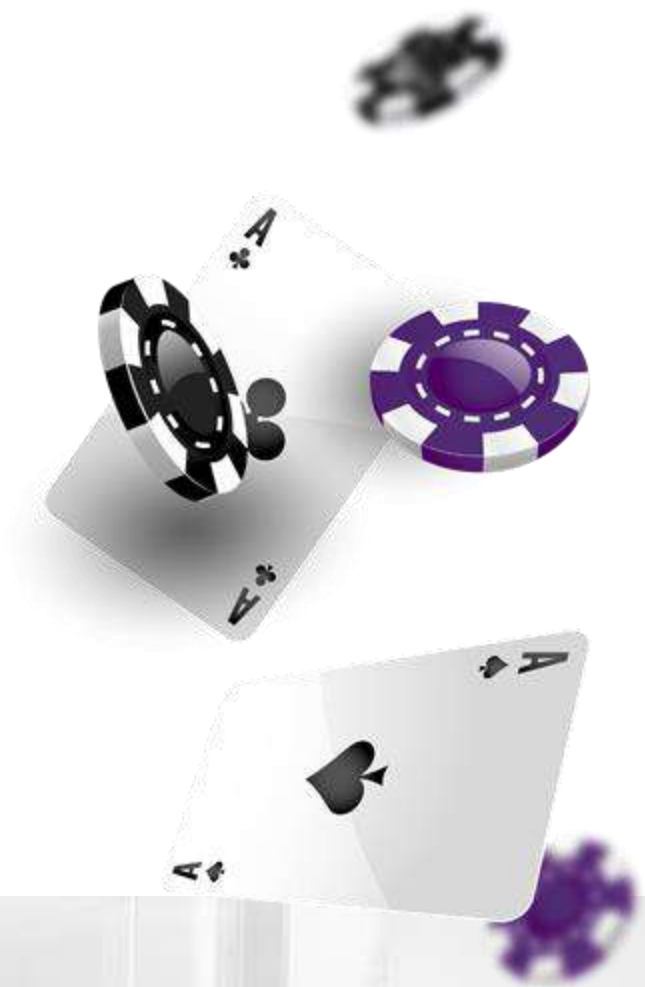
**It does not matter that an American cloud provider may have its servers physically located within the EU - they are still subject to the CLOUD Act and may thus be forced to disclose information to U.S. authorities.**



## HOW THIS AFFECTS iGAMING

Many European iGaming companies currently store their data with one of the American cloud giants: Amazon Web Services (AWS), Google Cloud, or Microsoft Azure. As such, there is a substantial risk of ending up in legal difficulties regarding the handling of personal data.

To have a secure and future-proof cloud service, the recommendation is therefore to use a European-based cloud service provider that stores your data within the EU. This gives peace of mind that the storage of personal data fulfils approved protection requirements, following the provisions of GDPR, and you can also be sure that no other countries' regulations risk trumping EU legislation.



## HOW THIS AFFECTS iGAMING



To underline the importance of this issue, we can refer to a recent data protection report by Norton Rose Fulbright, a leading resource for business stakeholders who need to understand the business impact of the rapidly evolving global privacy, data protection, and cybersecurity regulatory and litigation environment. They published the following:

”

European Regulators found that the CLOUD Act could cause service providers to face a conflict between complying with U.S. law and complying with the personal data protection required by the General Data Protection Regulation (GDPR) and other EU laws. They pointed to Article 48 of GDPR, ‘transfers or disclosures not authorized by Union law.’ That Article provides that a foreign court or agency’s order to a data controller or processor - such as a service provider - to transfer data ‘may only be recognized or enforceable in any manner if based on an international agreement, such as a Mutual Legal Assistance Treaty (MLAT) ...’

”

Because the CLOUD Act specifically contemplates court orders/warrants requiring the transfer of personal data without an MLAT, the European Regulators concluded: ‘service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the U.S. on such requests.’ ... Their clear preference is for such disclosures to be made under a MLAT where ‘data is disclosed in compliance with EU law, and under the supervision of the courts in the EU’.



Back to  
content

# ACHIEVING AND SECURING CLOUD COMPLIANCE as an iGaming operator



**The iGaming industry is heavily reliant on consumer data, particularly when it comes to marketing and developing products; the new legal situation requires significant adjustments.**

**Plus, iGaming companies' customers are often high-net-worth individuals who value privacy, so there is a huge potential for reputational damage for operators who do not understand the implications of the new reality.**

**No matter what type of cloud service your organization plans to use - private, public, or hybrid clouds - many laws and guidelines must be followed to achieve cloud compliance.**

**It is a complex task that requires a lot of commitment on your part and from your cloud service provider. Of course, it does not get any easier when these guidelines are changed and updated regularly. But, some key factors will give you a good foundation for a safe and secure cloud service.**



# ACHIEVING AND SECURING CLOUD COMPLIANCE as an iGaming operator

**1** Firstly, the most important thing you need to do is gain knowledge about which laws and guidelines apply to iGaming and the type of data you plan to store in the cloud.

In addition to GDPR, which regulates the handling of *personal* data in the cloud, there are, for example, various other rules for how data linked to payments and credit cards should be handled, as well as different ones for financial information about individuals and companies.

By mapping which regulations apply to the type of data that your organization handles, you can then go ahead and find a cloud service provider that meets these requirements.

**2** Next, it is important to have full control of data security within your organization. A major reason for data intrusion is precisely the lack of good verification when logging in and poor routines regarding who has, or should have, access to your data.

A cloud service provider should ensure full data security protocols are implemented.



## ACHIEVING AND SECURING CLOUD COMPLIANCE as an iGaming operator

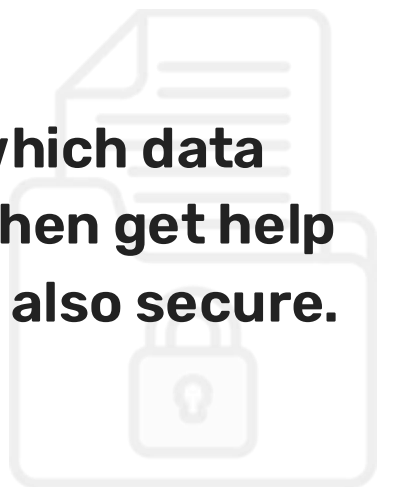
**3** After that, in the event of a compliance review, you'll need to be able to track exactly where your clients' personal data is stored, prove its exact position, and explain what measures have been taken to protect it.

Therefore, you should request clear documentation from potential cloud service providers showing where they have their servers. (i.e. the exact location of the information.)

As we mentioned earlier in this guide, it plays a major legal role whether the servers are within the EU or completely outside the EU, and in which country the cloud service provider is registered. Legislation of other countries can cause legal issues if the servers are owned by an American provider, for example, even if they are physically located in the EU.

Additionally, data should be classified to determine the correct level of security that is required. For security reasons, or sometimes for compliance reasons, some may choose not to move sensitive data into the cloud. However, to maintain security and still realize the benefits of cloud storage, the solution may be to use private clouds.

By classifying the data, you'll know which data requires special protection and can then get help with a cost-effective solution that is also secure.



# ACHIEVING AND SECURING CLOUD COMPLIANCE as an iGaming operator

**4** Furthermore, once it's decided which data to store in the cloud, and in which way, it is important to ensure that it is sufficiently encrypted. By encrypting the information, protection in the event of a data breach is increased. Encryption also helps to meet compliance requirements. Qualify which type of encryption your cloud service provider offers, and how and when it is applied.

Also, make sure that the provider has the appropriate certifications when it comes to handling information security. For example: ISO 27001. The vast majority of data breaches occur by insiders and people with direct access to the data. It may be intentional or unintentional, but the majority of intrusions occur inside your organization. Your cloud hosting provider's expertise can help to mitigate this risk.

**5** Lastly, the key to ensuring proper cloud compliance is follow-up. As mentioned earlier, laws and regulations change. Especially vis-a-vis the legislation of other countries.

Therefore, your organization must have routines for follow-up and control. These processes and procedures ensure that you can check regularly that your data is protected in the right way.



# CHECKLIST for the correct handling of personal data



**You know the laws and regulations that apply when storing information in the cloud - specifically as related to iGaming and your valued customers**



**You know who has access to data and implement a high level of security for login protocols**



**You have routines in place to monitor any updates that occur regarding relevant regulations**



**You know exactly where your data is stored, keep track of which information requires an extra level of security, and ensure information is encrypted before it is sent to the cloud**



**Following the above means that you have laid a perfect foundation for cloud compliance in your cloud service**





**INTERNETVIKINGS**



Copyright © 2026 Internet Vikings International AB | VAT SE556545890701  
Roslagsgatan 26A, 113 55 Stockholm, Sweden | All rights reserved

