Data Security and Data Privacy

In recent years, data privacy has become a high concern as the gold rush for data has caught the attention of lawmakers around the world. That's why businesses (as well as individuals whose data is collected and processed) has made privacy one of the top criteria when evaluating a new service, software or other system that may have access to user's information. What the provider can do or cannot do with their data is a perfectly valid question and one that should be asked more often.

Knowing that your data is in good hands when it's stored with your provider is important. But is the data actually secure and protected when it travels the Internet? What technical means does the provider implement to secure your data from being lost or stolen? That's where data security enters the scene.

#1 Does IceWarp read my emails?

The most commonly asked question is whether we can read your emails – and while we could – as long as you provide us your data in an unencrypted form, don't worry. There are both organizational and technical measures in place to guarantee privacy of your data, whether it is email, contact lists, notes or documents. This includes strict access control, maintenance logging and last but not least, proper training of our engineers.

#2 Is IceWarp GDPR compliant?

We adhere to strict data protection legislation, regardless if you chose to store your data in Germany, or in the U.S., IceWarp complies with European GDPR. This is because GDPR is applicable to personal information of any end user or business contact of any European, so it's easier to implement it across all our clusters. In fact, IceWarp has been working on enabling data discovery and compliance for other businesses, easily locate personal data in all internally used systems using full-text search, securely archive it or delete it. To address the privacy needs of US organizations working with sensitive patient health information, we can help to achieve compliance with the national standard HIPAA.

#3 Is the data encrypted?

The data you synchronize with the IceWarp Cloud flows exclusively between your client and our data center and it's always encrypted (unless you explicitly switch off the encryption, which you shouldn't do) with SSL/TLS which is the industry standard in communication encryption on all protocol levels such as HTTPS, IMAPS, POP3S, SMTPS, WEBDAVS. After the data is saved to the disk, however, it's stored in an unencrypted, readable form. One of the reasons is the responsiveness of our applications, secondly one may argue that if the data is unencrypted on your computer which isn't locked in a cabinet, needless to say it's not protected by category RC3 walls, CCTV, security, access control etc., that the physical security of the data center which is equipped with all that and more, would offer almost as good protection.

#4 I have accidentally deleted an important document, can I restore it?

You can retrieve it from trash, but even if you deleted it from trash already, it's not all lost. IceWarp keeps regular backups several times per day of all cloud data to a backup storage which works both as an archive and a backup which can be used to restore whole snapshots in case of failure of the primary storage. This means we can restore up to 7 days old emails or documents. Based on customer's demand, we plan to provide offsite backups to further increase data resiliency in case of unforeseeable events that could affect the particular data center.

#5 Can the cloud be hacked?

IceWarp Cloud is built on single-tenant architecture in which services are isolated from each other, including non-shared storage, so a breach in one site doesn't affect others. There are individual firewalls that work as a protective shell for your data. Smart cloud automation developed by IceWarp ensures the highest level of information security, as opposed to vulnerabilities that exist in commonly available virtualization platforms. Connections are secured and limited to authorized staff who are issued personal tokens and connect through a virtual private network (L2TP/IPSec) and SSH gateway. Only necessary ports are open for most of the services, further reducing the risk. There's also high physical access security in all our data centers, protecting the clusters from damage, infiltration, theft, fire, etc. In addition, the proactive monitoring of all services and the network traffic would reveal any malicious activity and allow our security team to react.

#6 Where are my data located?

Any data and apps you have in the cloud are physically stored on a server located at a data center or server farm. Location of that data center is the most important factor when considering cloud providers. Do they disclose this information at all? Can they guarantee to keep your data under one jurisdiction, such as to prevent the transfer of personal information?

With IceWarp Cloud you can select from the list of several data centers where your data will reside. Not only the distance and local connectivity to the nearest data center will make the service more responsive, but also ensures that the data remains protected by privacy laws valid in your country. We guarantee your data won't be moved abroad. You are in control.

#7 Is the on-premise version safer?

If you can replicate all the access protection and information security measures of the cloud service in your own server room, regularly patch and maintain the server and monitor it 24/7, then it could be safer in the aspect that nobody except you has administrative access to the data. If despite your best effort your data suffers any harm,

you're the one solely responsible. This is why more and more businesses appreciate working with a trusted provider like IceWarp who keeps sufficient insurance against accidents like this and who can help you out.

#8 What security implications there are to micro-services?

IceWarp Cloud micro-services are a way to offload complicated tasks from customer's own server to the cloud. They offer the best of both worlds, the simplicity and infinite capacity of cloud and the data privacy of own server infrastructure. When you use a microservice you are accessing remote service running in IceWarp data center. The connection between the servers ends at the end of your session. All data is stored on your server because IceWarp is a runtime environment only. All communication between your servers and the cloud is encrypted by SSL/TLS.

To sum it up:

- We never read your emails or any other data
- We encrypt communication for all services with SSL/TLS
- We comply with all the GDPR requirements regardless of your location
- You are in control of where you data is stored
- Our data centers are equipped with strong physical security and access controls
- We take computer security seriously and our processes are ISO/IEC 2007:2013 certified
- Your data is protected AND regularly backed-up AND insured against damage
- And last but not least –we never sell, analyze or make profit of your data