Your Security Checklist

A checklist for securing your cloud

Brought to you by Ironstone

Intro

If you are using cloud services and storing important data in the cloud, you need to know that your data is safe.

In the myriad of technical information on cloud security and personal data, it can be hard to know what you should do to protect your data in the best possible way.

In this checklist, we have gathered central information from the most important actors on cloud security, and given you three steps to ensure that your cloud is safe.

The steps

Step 1. Responsibilities

Step 2. Data Processor Agreement

Step 3. Cloud Service Provider

Step 1. Responsibilities

The first step to a safe cloud, is knowing what your responsibilities are.

Say your business have approximately 100 new customers each month. You use a cloud service provider to store your information, and each customer leaves his or her full name, address, e-mail and credit card number in your **customer database in the cloud**.

Who is responsible for securing all this personal data?

This dilemma is partially difficult to solve because of the global nature of the Internet. The expanding world wide web and the increasing amount of the transfer of personal data have made various governments and institutions seek to secure people's personal data.

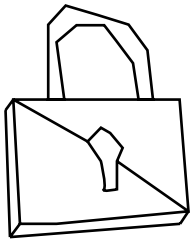
As of today, private customers have the right to know that their personal data is safe and that it will not be used for faulty purposes or shared with a third party.

But how is this responsibility shared between you, as a business, and the company providing you the cloud service?

Step 2. Data Processor Agreement

The second step to a safe cloud is making a thorough data processor agreement.

This agreement is the promise between you and your **cloud service provider** that they will treat your data in the way you have specified – and secure all your information in exactly the way you want it.



So far so good - you have established your responsibilities as a data controller and made a thorough and qualified data processor agreement, so you know that your cloud service provider will follow your rules for safety.

But in the jungle of providers of cloud services, it can be difficult to know which cloud service providers will secure your data in the best possible way, despite a good data processor agreement.

Step 3. Cloud Service Provider

The third step is finding the safest cloud service provider.

The best sign you can look for is the ISO 27018.

The many providers of various cloud solutions and the globality of the Internet made it necessary to make international standards to ensure the security of personal data in the cloud.

In 2014, The International Organization for Standardization – ISO made an international code of practice for cloud privacy, the ISO 27018.

ISO 27018 – The ultimate recognition of cloud security

One of the easiest and best ways to ensure that your data is in safe hands is choosing a cloud service provider that **complies with the requirements of ISO27018**. The first company to comply with the cloud security standards set by ISO was **Microsoft**.

What Microsoft says about personal data and cloud security

Microsoft is the **world's leading provider** of cloud services, and the company is highly conscious of the standards for securing personal data. Their privacy and security terms are **continuously updated** and changed to **comply** with ISO standards and EU law.

Microsoft states that the client is in control of the data, which means that you as a client is in control of the use, distribution and collection of your customer data.

Your customer data is not in any way redistributed to third parties for marketing or advertising purposes. Who can access your data in the cloud is limited, as Microsoft is taking measures to protect your data from inappropriate access.

If your data is stored on servers in one country, but the cloud service provider comes from another country, which of the two countries' laws apply?

We recommend you to read the case where Microsoft filed a lawsuit against the American goverment, after they requested data from Microsoft.

Good to know
Microsoft has a policy of transparency, which means that customers will always know where their data is stored, and, hence, which laws it will be protected by (in your case, EU law).

IRONSTONE

BUSINESS COMES FIRST

Essentially, **Microsoft's cloud services** are extremely well protected and the security of Microsoft's cloud is world-class.

At **Ironstone**, we are proud to offer Microsoft cloud services and years of IT experience to help you secure your data in the best possible way.

By using Ironstone's cloud services, you are closer to **securing your cloud.**