DECISION **GUIDE**

HOW TO CHOOSE A PROVIDER

TRUST

Cloud applications often initially make administrators feel like they're **losing control**. With physical hardware, admins can at least pull out a plug and fiddle with screws. If a cloud service fails, the only thing an administrator can do is call the hotline. In other words, the administrator surrenders a part of his/her sovereignty. This means: **you need to trust your provider!** If necessary, bring in external support to assess the contract.

PRICE MODEL

Most cloud providers use the aforementioned "Pay per Use" model. Only the resources that are actually used are invoiced. However, additional costs can still arise, for example through use of extra features. Discounts are often offered to companies who use a certain data volume or disk space. More users also result in lower costs per user. **It is still wise to test the service with a small data set and then increase usage.** Terms of contract, payment methods and payment dates can be deciding factors as well.

TECHNICAL REQUIREMENTS

Test potential providers extensively:

- Is use of the cloud intuitive?
- Does the software really make work processes easier?
- How customizable is the software?
- What interfaces are available?

Scrutinize the service and its performance. You and the users in your company should test the cloud service. When in doubt, decide on a service that has already established itself on the market.

DATA SECURITY

Providers must conform to the data protection acts of their country. In the German market, for example, § 11 of the German Data Protection Act details the **"Commissioned Processing or Use of Personal Data"**. This must be included in the contract.
American providers often have servers located in Europe as well. Companies can also opt in to complying with **data security minimum standards** per the **Safe Harbor Principles.**

IT SECURITY

How can the provider guarantee that their computing center is secure? Both the physical building in which the servers are located as well as data encryption. **Make sure that your provider observes current SSL standards.**

FAIL SAFETY

Cloud services especially must guarantee a high level of fail safety. Redundant infrastructure and emergency management must be clearly detailed. These details must be included in the contract or on the company's website.

SERVICE

What kind of support is available for integration and setup of cloud services? **Is 24-hour support** available if problems arise? How are the service and support rated online? This should be checked out in advance as well.

CONTRACT TERMINATION

Many legal systems have codifications of commercial law. In Germany, for example, the German Commercial Code requires every company to store data for up to ten years. This means that cloud services must exhibit data export options, so that data can be archived locally. Export options are also important so that it is possible to switch to another provider and dependence on a specific provider is not too high. Unfortunately, no standards exist in this yet, **which is why it must be defined beforehand.**