IT Cluster Vienna | Cloud Computing Group

Publisher: Paul Meinl

# Software as a Service – Correct Conclusion of Contracts

2nd enhanced edition

vienna
business
agency

IT-Cluster
Vienna

Supported by:

kapsch >>>

Stadt Wien
Wien ist anders.

Co-financed 50% by the European Union.

EUROPÄISCHE UNION
Europäischer Fonds
für regionale Entwicklung

Mit Europa für Wien

eu.Wien.at

# Foreword

Dear Readers,

Gerhard Hirczi
CEO Wirtschaft-sagentur Wien

As part of cloud computing, Software as a Service (SaaS) is one of the megatrends of today's information technology. The idea is as simple as it is forward-thinking. The software and IT infrastructure are operated by external IT service providers and used by customers as a service. The SaaS model offers numerous benefits for companies, including more flexible, location-independent access opportunities. IT costs are also reduced and made easier to manage.

However, it is essential here to take into account the issue of IT security and the legal aspects of this outsourcing model. Who is responsible for which system components? What happens when faults occurs? How is data protection guaranteed? – these and many other issues are crucial in the arguments for and against the use of software as a service.

The IT Cluster at Wirtschaftsagentur Wien has been dealing for years with the legal aspects and details of SaaS, and presents with this guide a comprehensive overview of all relevant issues. This is already the second revised edition, created on the back of high demand and positive industry feedback.

I trust you enjoy reading this publication. Yours

Gerhard Hirczi
CEO Wirtschaftsagentur Wien

# Contents

# Introduction

Paul Meinl
Judge, former CEO of factline Webservices GmbH (factline.com)

**"Application Service Providing", "Software as a Service"** and now **"Cloud Computing"** – for over ten years now, different names have been used to predict trends, identify market potential of astronomical magnitudes and usher in new Internet eras. Even if excessive expectations have disappointed, the concept of offering software and infrastructure as a service over the Internet has without doubt become one of the major pillars of modern information technology.

Certainly understandable against this background is the following statement on "Cloud Computing" accredited to Oracle CEO Larry Ellison[1]:

> *"The interesting thing about cloud is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of this announcements... Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop? We'll make cloud computing announcements. I'm not going to fight this thing. But I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads.*

Intensive discussions on terminology were also held at the start of our working group in 2004. These were most important in developing a common understanding of central features. On this basis, it was soon possible to consider the matter of terminology delineation closed so that central legal and technical issues could be addressed.

The different terms were used mainly to find names for our activities that are based on current trends. Under the title "Framework Conditions for Application Service Providing", a guide on "Software as a Service" was developed, the second edition of which is being published by the "Cloud Computing" group...

Nevertheless, or perhaps for this very reason, it was important for us to present in more detail the major features of "Cloud Computing" in this edition.
This task was kindly accepted by Mr Hans-Jürgen Pollirer, who on the following pages in his guest article gives a systematic classification of the different abstract concepts and their key attributes.

[1] *http://gevaperry.typepad.com/main/2008/09/larry-ellisons-anti-cloud-computing-rant.html*

The rapid sales of the first edition and the positive feedback we have received demonstrate that we have been able to plug a gap with this guide. We therefore feel encouraged in our plans to use this guide as an effective means of confronting the continued uncertainly when working with SaaS.

In the development of this "user guide", care was taken to address the fundamental and **generally relevant framework conditions**. Every effort was made to remain unbiased towards both providers and customers and to take both points of view into account, so as to facilitate a **coordination of interests** between the two positions.

The guide is to serve as the foundation for **targeted discussion** between provider and potential customer. It enables an interested customer to ask the right questions and therefore to clarify the relevant framework conditions. It is also aimed at simplifying the comparison between alternative offers. On the other hand, it gives providers the opportunity to prepare themselves for the relevant customer questions and to check the quality of their offer. Furthermore, it makes a contribution towards greater assurance in the legal sense by simplifying compliance with existing legal regulations – from pre-contractual duties of disclosure to the phase following contract conclusion (such as data erasure obligation).

Practical aids for contract negotiations are new inclusion in this edition. A **"Topic overview"** is used for targeted preparation and a **checklist** serves as a basis for contract negotiations. Also, a comprehensive **"list of questions"** is available for download on our Internet platform **(http://saas.clusterwien.at/5562475.0).** If the questions in these documents between customer and provider are discussed and answered sufficiently accurately, there is a **solid basis for continued collaboration**.

The achievements of the members of IT Cluster Vienna and the Working Group for IT Service Contracts and Legal Policy at the **Austrian Computer Society (OCG)** were magnificent in creating this edition, as they were for the first edition. Many thanks for your all your hard work!

saas.clusterwien.at
/5562475.0

# About the term Cloud Computing

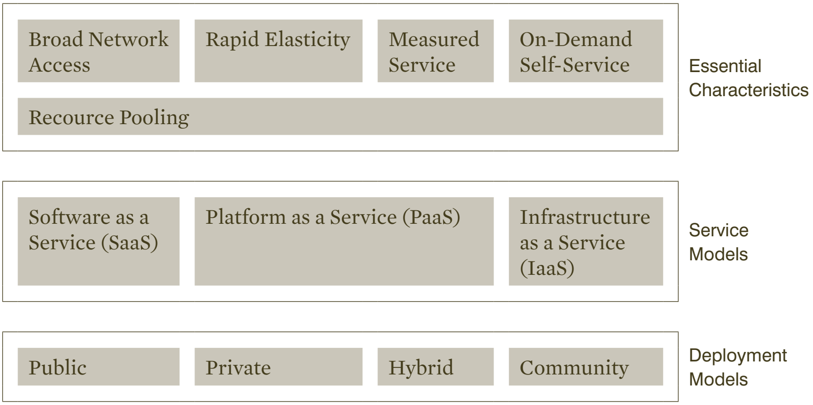
Guest article by Hans-Jürgen Pollirer, chairman of the "Information and Consulting" federal sector at the Austrian Chamber of Commerce

″Software as a Service″ (SaaS) is a part of today′s IT megatrend, namely that of ″Cloud Computing″, whereby SaaS in particular offers Austria′s small-scale economic system[1] fantastic opportunities of being able to source IT services more cost-effectively. The questions in this guide make really clear that SaaS providers must be selected carefully and that particular attention must be paid to contract design.

″Cloud Computing″ actually represents a collective term for long-existing IT concepts such as Outsourcing, Grid Computing and Application Service Providing (ASP) – all forerunners to SaaS.

Of the many certainly different definitions of Cloud Computing, those of the U.S. National Institute of Standards and Technology (NIST)[2] have established themselves amongst experts.

NIST Visual Model of Cloud Computing Definition[3]



Broad Network Access | Rapid Elasticity | Measured Service | On-Demand Self-Service

Recource Pooling

Essential Characteristics

Software as a Service (SaaS) | Platform as a Service (PaaS) | Infrastructure as a Service (IaaS)

Service Models

Public | Private | Hybrid | Community

Deployment Models

[1] *99.6 % of the 300,000 or so Austrian companies are SMEs according to the European Union definition, i.e. micro enterprises as well as small and mid-sized businesses with fewer than 250 employees (whereby 88% of Austrian companies have less than 10 employees).*

[2] *http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf*

[3] *See Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 14, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf*

NIST initially defines Cloud Computing through the necessary presence of 5 **ESSENTIAL CHARACTERISTICS**, differentiations between 3 different **SERVICE MODELS** and finally 4 different **DEPLOYMENT MODELS**: Individually these terms contain the following:

## CHARACTERISTCS

- **Broadband network access** – the Cloud user is able to access in real-time the various Cloud services via mobile telephones, laptops and PDAs using standard technology.

- **Rapid elasticity** – The necessary resources are made available to the Cloud user quickly and elastically as required – and in many cases also automatically. This way the Cloud user is given the impression of having unlimited access to the resources.

- **Measurable services** – the Cloud systems have embedded control and measurement functions that optimise resource consumption depending on the type of Cloud service. This guarantees to both the Cloud provider and the Cloud user appropriate transparency as regards the services which have been used.

- **On-Demand Self-Service** – Cloud users are able to request services and resources by themselves without the need for human interaction with the Cloud provider.

- **Resource Pooling** – The resources of the Cloud provider are bundled and made available dynamically to Cloud users in line with their requirements. The services offered are characterised by location-independence. This means that Cloud users have no control over or knowledge of where the services offered originate from geographically. In the best case, the service location can be determined on a higher level of abstraction (such as country, state or computer centre).

## CLOUD SERVICE MODELS

The NIST model differentiates between 3 different archetypical service models, also known as the "SPI Model" in technical literature (Software, Platform and Infrastructure). These 3 models differ in the content of the services made available to the Cloud user.

- **Software as a Service (SaaS)** – With this Cloud service, Cloud users use the software applications offered by the Cloud provider that are operated within a Cloud infrastructure. Cloud users access the required software applications using their devices and a web browser. Cloud users have no control at all over the Cloud infrastructure provided to them or the software applications. Salesforce.com, SAP Business by Design, Apple iWork.com, Google Apps for Business and Microsoft CRM online are typical examples of SaaS.

- **Platform as a Service (PaaS)** – This variant offers Cloud users the option of creating and operating their own software applications within a development environment provided to them via a platform. In contrast to SaaS, Cloud users retain control over the software application in this service form. Google Apps Engine, Windows Azure and IBM Smart Business Development are typical examples of PaaS.

- **Infrastructure as a Service (IaaS)** – The whole purpose of this Cloud service is to make available to Cloud users computing time, storage area, network and other IT components in such a manner that they are able to operate their software applications as they wish. With this Cloud service, Cloud users have no control at all over Cloud infrastructure, but do have control over operating systems, storage area and software applications used (possibly also with limited control over individual network components such as a firewall). Oracle, IBM and Amazon EC2 and S3 are typical examples of this Cloud service.

## DEPLOYMENT MODELS

Notwithstanding the 3 Cloud service models (SaaS, PaaS and IaaS),
NIST distinguishes between four different deployment models:

- **Public Cloud** – In this deployment model, the Cloud infrastructure is made available by a Cloud provider to the public or a large industry group.

- **Private Cloud** – In this variant, the Cloud infrastructure is only made available to a closed group (e.g. a corporate group). The Cloud infrastructure need not necessarily be installed at one location and may be operated by a third party (such as a service provider).

- **Community Cloud** – In this deployment model, multiple Cloud providers group together and service a specific Cloud user group with common requirements.

- **Hybrid Cloud** – This means the amalgamation of at least two different Cloud models; the individual Cloud providers remain independent but are linked via standardised or proprietary technologies in a way which supports both data and software interoperability.

# 1.0

# The SaaS Contract

## 1.1 Contractual settlement of all potentially contentious issues

In order to prevent contractual disputes from arising at a later date, it is expedient to anticipate **potential conflicts** and to agree appropriate regulations. However, one must remember that rights should not be assigned to just one party while the other party bears the obligations. Such regulations are often deemed by courts as immoral, and therefore as void, on the basis of serious equivalence mandates. Such regulations therefore only produce the exact opposite of what was originally intended.

Most contractual disputes arise because neither party really racks their brains and clarifies what they actually want and what can really be achieved. Deliberations that either contain vague advertising messages or reflect wishful thinking are channelled too frequently into the description of services.

Openness between customers and providers in the initial phase averts difficulties in contract fulfilment.

Both parties **should therefore speak as openly as possible** with each other when entering into contract negotiations. This is often difficult, but unavoidable, in the early stages for reasons of non-disclosure or due to the fear that the conclusion of the contract may be jeopardised by addressing the unpleasant truth. Concealing too much in this phase risks serious difficulties in contract fulfilment because no real understanding has been reached on certain key points. The failure to inform the contractual partner can subsequently be deemed a basis for blame, resulting in compensation. This is then judged outside contractual settlement and in accordance with legal regulations.

The **service specification** and the **equivalent in money** are not substitutable by anything else and represent the most important parts of a contract. If there is agreement here, an effectual contract is generally concluded.

The type, the place and the time of contract fulfilment are the other key points. The time in particular is often contentious because the party rendering the service often overestimates and makes promises that cannot be kept just so that they receive the order. The expectations raised this way end up in disappointment and the contract ends up in a precarious situation – one that can be avoided by setting a realistic timeframe.

## 1.2 Terms of a contract

### 1.2.1 Subject matter of a contract

A clear, non-ambiguous and understandable description of the subject matter of the contract is a prerequisite for a good contract.

As intimated above, the description of the subject matter of a contract is **the most important** part of a good contract. All the work put into the description is a worthwhile investment when the description is as clear, non-ambiguous and understandable as possible. There is no reliance on terms or abbreviations which are already familiar. The other party could interpret all this very differently and a dispute would then be inevitable. This does not mean that page upon page of descriptions are required. The aim must be to describe sensibly and non-ambiguously (also for a reasonable third party) what the two contractual parties want. However, since the service definition can still turn out to be very complicated, it can sometimes be very wise to have an abridged version within the contract text and the actual service description in an (also legally binding) appendix. It can also be sensible to include milestones in the service description so as to be able to monitor contract fulfilment.

One issue that should not be disregarded is the bearing force majeure can have on the subject matter of the contract. In the classic rental contract, predominant opinion and legal practise state that the destruction of the rental property through no fault of the renter or its broad rendering as a non-usable property terminates the rental contract. As with the rental contract, if the service provider's IT infrastructure is destroyed through no fault of their own or is made unfit for use, the contract will be terminated irrespective of influencing factors.

However, this cannot be readily accepted by the customer, especially when the existence of his company is under threat. This means that in those circumstances in which existential services are outsourced to the service provider, the service provider must always offer an alternative solution that averts this threat for the customer. The solution lies in redundant IT infrastructures that are physically separated and that, in the event of major disruption to one IT infrastructure, quickly assume the functions of the services being provided. This of course has a bearing on cost.

### 1.2.2 Terminology

The use of term definitions in an agreement is extremely helpful given that parties not familiar with specialist terminology are often helplessly confronted with different technical terms and abbreviations (that can then also have different meanings). This can help make the contract much clearer because specialist terms used need not always be explained or paraphrased. Abbreviations are used very often in the IT industry in particular and their meaning must therefore be defined.

### 1.2.3 Provision, operation and support

Together with the service description, the contract should also specify how the agreed service is to be delivered, i.e. which availabilities can the party receiving the service expect? A measurement period must always be defined because availability is a probability judgement on the time period during which the service is mainly available. An example of how this is regulated is shown in Section → 3.2. A whole array of contractual availabilities is up for discussion here because there may well be **different requirements** for a customer as regards availability of services at different workplaces. They must all be regulated clearly as regards the measurement period. See Section → 3.2 for further details.

### 1.2.4 Problems, faults and malfunctions

The careful definition of faults has an influence on contract design and must not be neglected.

Faults differ as regards causes and consequences and have a bearing on warranty.

In this context, differentiation of the following terms, often used synonymously, is relevant: A **malfunction** is understood to be an evident impairment that includes technical and organisational **faults**, and also negative external influences on the software service (such as lightning strike, flooding and power cut over a long period). **"Deficiency"** on the other hand is a legal term entailing important legal consequences. It is defined in the ☞ ABGB (GENERAL CIVIL CODE) as part of the contractual warranty (§ 922ff, see also → 1.2.19) and covers every type of departure from the service owed. Non-technical services such as documentation, training and fault rectification can therefore also be deficient. One of the reasons why the distinction is relevant is that not every fault in the IT system manifests itself as a malfunction and therefore as a deficiency triggering warranty obligations.

The term "Problem" for faults and malfunctions, often used in international standards (☞ ITIL Vers. 2 and 3) and in the literature[1] is imprecise and misleading in this context. The term should be avoided in this context because it does not cover the scenario presented in the previous paragraph[2].

The type, time and place of a fault must be reported and then recorded so that in can be reproduced.

Given that the subject matter of the contract generally contains uninterrupted services to the greatest extent possible, the **recording** of impairments to these services (fault recording and reporting) is a key task for both sides to facilitate restoration of the uninterrupted services and to prevent disputes. For this to happen, the service provider must set up a point of contact where his customers can report the faults detected by them.

[1] *e.g. Heinrich, Information Management, 2002*

[2] *Problem (gr. Πρόβλημα, próblema = issue presented [to be resolved]) is the name given to a task or matter of dispute whose solution is associated with difficulties.*

For it to be also possible to monitor the contractually agreed availability, the type, the time and, if it can be traced, the place of the fault must be reported and recorded for reproduction (in writing or with a voice recording), and be assigned a unique code (name or number). Receipt must be confirmed to the reporting party (″trouble ticket″). Following rectification of the fault, or following estimation of the rectification time, rectification (time and type of fault) or the estimated rectification time must be communicated to the reporting party using the same or a comparable channel. Communication in writing with confirmation of receipt using a secure method is preferred to communication over the telephone if possible, provided written communication is possible and not impeded by the nature of the fault.

The protocols of these fault reports, their classification and the rectification times determined form the basis for calculating the availability of services. Operating errors on the part of the customer that are not attributable to training or documentation errors, and that result in fault reports, are not covered by the provider′s service and can be invoiced by the provider at agreed rates.

### 1.2.5 Data backup and data protection

If personal details are used in a software service, adherence to the applicable version of the ☞ DATA PROTECTION ACT (DSG 2000) is an absolute requirement. Also deemed as personal information by the Austrian legal system and DSG 2000 is all internal company data and data capable of being protected. The Data Protection Act defines all data with which a person or company is identified or identifiable as personal. If this data is ″sensitive″ (race or ethnic group, religion or ideology, political conviction, trade union affiliation, health, sexual tendencies), a general processing prohibition applies with legal exclusions and special sanctions.

The **constitutional provision** of § 1 DSG 2000 specifies (paragraphs 1 to 4):

Everyone has the right to non-disclosure of personal data pertaining to them.

Fundamental right to data protection

§ 1. (1) Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject.

(2) Insofar as personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another, namely in case of an intervention by a public authority, the restriction shall only be permitted based on laws necessary for the reasons stated in Art. 8, para. 2 of the European Convention on Human Rights (Federal Law Gazette No. 210/1958). Such laws may provide for the use of data that deserve special protection only in order to safeguard substantial public interests and shall provide suitable safeguards for the protection of the data subjects' interest in secrecy. Even in the case of permitted restrictions, the intervention with the fundamental right shall be carried out using only the least intrusive of all effective methods.

(3) 1. the right to obtain information as to who processes what data concerning him, the source of the data, for which purpose they are used, as well as to whom the data is transmitted
2. the right to rectification of incorrect data and the right to erasure of illegally processed data

(4) Restrictions of the rights according to para. 3 are only permitted under the conditions laid out in para. 2.

Of particular interest are the rights defined in § 1 para. 3 of all those concerned to "information as to who processes what data concerning him, from where the data originates, for which purpose it is used, as well as to whom the data is transmitted", the right to rectification of incorrect data and the right to erasure of illegally processed data." This is substantiated in §§ 26-29 DSG 2000 (see also → 2.3.3).

§ 6 and § 7 effect this constitutional framework in more detail. §§ 8 and 9 define the governance for sensitive and non-sensitive data. Also note § 14 DSG 2000 which sets out the general requirements for data processing (for more details see → 2.2.1). These **apply for every provider** of software as a service that processes personal data. Because, as mentioned above, company data is also deemed personal, **virtually all software service providers are in practise subject to the Data Protection Act**. This requires conformance to the Data Protection Act at all times (see also → 2.1.6 and → 2.2.1).

### 1.2.6 Customer system requirements

For the service provider to be able to deliver the required scope of services, the customer must often fulfil **certain technical requirements**. These must be communicated to the customer by the provider in an adequate and understandable form prior to conclusion of the contract. This also includes appropriate consultation on the link between provider and customer (switched/non-switched connection, bandwidth, error rate, usable protocols, software interfaces, suitable network providers). Clarification is also required on who procures these connections, who maintains them and who bears the costs (the network provider would probably be responsible for the direct maintenance of the connection line). The service provider (who would have greater technical expertise) and the customer can both be responsible for reporting a potential fault to the network provider.

Providers must communicate the required technical prerequisites to customers prior to contract conclusion.

### 1.2.7 Service changes and updates

As a part of the contract, updates should be mandatory within the scope of services.

It may be expedient, or even imperative from a technical or cost viewpoint, for the service provider to carry out certain updates or modifications to the IT system as part of the contractual scope of services. Mandatory modifications usually entail when a supplier of hardware or software is no longer able or willing to continue to support ageing hardware components or functions. These kinds of modifications and updates must therefore be made compulsory for the customer from a particular point in time.

Technically necessary service changes must be agreed specifically beforehand or in the form of a contract modification right on the part of the provider.

Service changes by the provider must be agreed beforehand in the contract (if they can already be recorded in a specific manner) or be submitted to the customer at the specified time in the form of a **binding quotation**. The customer can either accept or reject this quotation.

Modifications that are virtually unavoidable due to a technical situation must also be agreed in the form of a contract modification right on the part of the provider. A permissible framework should be defined for this. For this scenario, the customer is entitled to an ordinary, or at least an extraordinary, right of termination. If a service existential for the customer is affected, this service modification must be announced by the provider early enough for the customer to locate and set up an alternative. This grace period must also be agreed in the contract.

### 1.2.8 Supplementary contractual services

Any amendments to the scope of services made at a later date must be arranged in advance.

Contracts over a longer term are generally exposed to factors that necessitate supplementary services, and hence also a **modification to the scope of services agreed**. These factors can become effective from within the domain of the service provider, that of the customer or from outside (economic or legal). The recommendation therefore is to include a clause in the contract that regulates these factors with foresight. A distinction is made between two fundamental forms:

Those changes that are **specifically foreseeable** and are normal, and so should usually be in the contractual service, and those changes that are foreseeable in principle, but individually are **not yet definable** as regards their effect (such as announced changes to the law, software releases and hardware modifications). In the latter case, it is expedient to impose on the provider the duty of submitting to the customer, as soon as the impact of the modification can be ascertained and its cost effect calculated, a binding quotation including a description of the effects such that the customer can accept or reject it within a certain time. For mandatory changes, the customer can be entitled to an ordinary or extraordinary right of termination of the contract.

Given that compliance is usually part of the content of the contract, and hence part of the service, the offer obligation on the part of the provider as described previously must be selected for such changes in the law necessitating a considerable change to the service.

But the customer can also request that the service provider offers, within an agreed or particular timeframe, a required service enhancement that the customer needs to define exactly or negotiate with the provider.

### 1.2.9 Testing of new application modules and their acceptance

If new contractually agreed services are introduced, it must be possible to test them, including the necessary constraints, prior to acceptance. For this the service customer may be required to provide relevant, up-to-date test data following the provider announcement. It is not until after positive conclusion of the agreed tests that the customer must adopt the new services. These are then transferred to live operation and invoiced by the provider in line with the agreement.

When concluding the additional agreement, both parties must furthermore determine who owns the **rights to use** these developments, whether the customer can be assigned a co-copyright, what share of the profits should the customer receive and how this can be settled.

Caution – do not forget a regulation for rights to use developments which have been produced by joint collaboration!

For developments requiring patents, it must be determined who registers the patents where, who pays the patent charges, who defends the patents and who grants licenses and how.

### 1.2.10 Documentation and storage of source code

Because the underlying SaaS application is always a very complex system, it is necessary to provide the customer with all the relevant **documentation**. This documentation must be organised such that the customer can use it. It should be complete (as defined by the contractual services) and eradicate most operating errors (☞ USABILITY). If the contract expires, for whatever reason, the customer may retain the documentation (but not pass it on to third parties) so as to have available relevant documentary evidence in the event of potential judicial proceedings.

Storage of the source code and documentation guarantees the customer continued use of custom software after the contract expires.

If the service provider has developed and made available for use to the customer **custom software**, it is advisable to commit the provider to make available in a sealed form the source code for this software including relevant documentation (programme specifications, programme flow diagrams, data flow charts, test methods, etc.), including all changes made, so that the customer is able to reuse this software with a third party provider when the contract expires. Otherwise a switch of provider is not possible. If the provider is not willing to make these available to the customer directly, a ″custodian″ can be appointed who must release them under precisely defined conditions (″deposit″).

### 1.2.11 Training and support

For complex services, it is necessary to train all the personnel who apply the services provided. It must be agreed in the contract when training is held for which applications, the goals to be met in these training sessions (only application or also ″train the trainer″) and which presumed qualifications personnel undergoing training must have for the training to have any prospects of success.

### 1.2.12 Availability of the service as a whole

As mentioned in → 1.2.3, certain parameters must be agreed in defining the availability of services in order to satisfy conditions that are understandable and acceptable to both parties. The service customer naturally has different interests as the provider. A compromise is necessary and must be defined contractually. Exaggerated demands from either party are not conducive to a successful outcome. Nobody can maintain 100% availability and it is generally not necessary. Services having a central importance usually require higher availability than peripherals. It is therefore important for both parties to agree the targeted and maintainable availability for every identifiable service, as well as permissible upper and lower limits. A relevant example is shown in → 3.2.

The availability to be agreed depends on the specific requirements of an individual case.

### 1.2.13 Payment and payment conditions

Apart from the negotiation phase, the agreement of payment for certain services is considered relatively unproblematic because it is the clear-cut and easily definable part of a contract. However, where payment is to be made for a sophisticated service package, it can be just as complex to determine the various pay elements as it is to render the service. This section of the contract should therefore not just be the subject of intense negotiations; it should also be treated with the same level of care as the service description and availability sections. Payment reductions for shortfalls in service can create particular difficulties when it comes to establishing absolute and relative values and how these should be settled.

The popular **no set-off clause** contained in many sample contracts, which prohibits the deduction of counterclaims (e.g. contractual penalties, payment reductions, payment of damages etc.) from due payments, is prone to error and counterproductive. The possibility of offset with a counterclaim provides additional security for both sides. Strictly separating the reciprocal demands from each other may lead to the scenario that the full

The contractual exclusion of set-off willingly agreed has more downsides than benefits.

amount of one's own payment must be made, whilst a counterclaim due to payment difficulties on the part of a business partner for example is not secure and fails to materialise (in part). One downside can result from the contractual partner attempting to block the enforcement of a claim with freely contrived counterclaims. It is preferential nevertheless not to include a no set-off clause in the contract. Note also that the effectiveness of any agreed no set-off clause is subject to legal constraints (§ 6 para. 1 Z 8 ☞ KSCHG (CONSUMER PROTECTION ACT)[3]) in consumer business transactions. This may also apply to transactions between two companies when compensation is excluded in the general terms and conditions (i.e. in the small print). The deadlines for payments and their conditions, as well as the sanctions in the event of infringement, are necessary parts of the payment conditions.

Similar to the no set-off clause, an "☞ASSIGNMENT PROHIBITION" is also often agreed. A contractual assignment prohibition prohibits the assignment (§ 1396a General Civil Code) of claims to a third party. It therefore curtails the financial scope of the party concerned, but saves the other party overhead (mainly in accounting).

### 1.2.14 Term and cancellation

A SaaS contract is **concluded for a period** of time and therefore is subject to different legal conditions than for a purchasing agreement. This applies in particular when the time period is to be open-ended. It is particularly important for both contractual partners to disclose their positions to agree a time line that does not entail unsolvable or particularly disadvantageous problems for either side. Included here is the fundamental decision on whether to enter into a limited or open-ended relationship.

(Balanced) terms of notice must be agreed for open-ended contracts.

These should be defined so that both sides are able to prepare for as smooth a transition as possible when the contract expires. The specific

[3] *According to this regulation, the consumer is able to offset with any claim when the company is insolvent; irrespective of this, he can compensate with claims that have a legal association with those of the company; and finally with claims that are determined to be legally binding and recognised by the company.*

duration of grace periods depends heavily on the circumstances of individual cases. They must, however, be balanced and satisfy the interests of both parties. It is also possible to agree different notice periods for the contractual parties. A single-sided or mutually limited cancellation waiver is often selected as a ″safety period″.

**Extraordinary termination** is a right that cannot be excluded in the contract and whose exercising is effective immediately. It can be deferred if fair conditions are in place. Extraordinary cancellation is always applicable when major parts of the contract are not complied with or when an objectively substantiated loss of trust in the contractual partner has arisen, i.e. continuation of the contract to the next ordinary termination date or the limited contract expiry is not reasonable. But it can also be agreed contractually for certain breaches of the contract.

Particular attention must be paid at the end of every contract to what happens to the data in the power of disposal of the service provider and what alternative software is provided for continuation of the service. Because it is mainly personal data that is stored at the provider, the **transfer in full** of this data to the customer must be regulated explicitly and meticulously. Furthermore, **a legal obligation to erase data** on the part of the provider must be agreed for all this data. The erasure must be performed by the provider by a certain deadline (to be agreed), and verification thereof must be provided to the customer. This is critical for all data in the backup because it is commonly stored on tapes, DVDs and similar media. Its erasure is usually time-consuming and laborious, but is an absolute legal requirement nevertheless (see → 2.3.2). Checking to see whether data has really been erased requires a high level of expertise and so should be left to a professional organisation. The costs arising for data erasure are part of the provider service but should still be regulated explicitly in the contract.

The German Data Protection Act 2000 stipulates that all customer data must be transferred and erased when the contract expires.

If the provider goes bankrupt (according to new insolvency legislation), the customer will have to bear the costs of data erasure himself because the provider will not be able to follow a regulated procedure in this situation. The customer should take steps immediately to ensure erasure of the data.

### 1.2.15 Obligations to confidentiality

A contractual obligation to confidentiality is expedient, but its scope should be realistic and not overstretched.

It is of course in the interests of customers that their data does not end up in the public domain or even in the wrong hands. Obligations to confidentiality are already governed in various laws. It is nevertheless advisable to regulate confidentiality in the contract (whilst also bearing in mind that people always make mistakes). The effects of these mistakes could be serious or amount to nothing. Sanctions must be agreed accordingly. Commonly used, all-encompassing confidentiality to "eternity" (which implies the lifetime of the obligated party ) with rigid sanctions often goes far beyond the intention. A **contractual penalty**, including compensation extending beyond this, is usually agreed as a sanction to protect against confidentiality breaches.

Employees on both sides must commit explicitly and verifiably to confidentiality.

Whilst this contractual penalty is difficult to transfer to **employees** in light of the Employee Liability Law, it is still very important that employees on both sides also conclude appropriate agreements in writing, preferably with the subject matter stated specifically. This guarantees their attention and adherence to the conditions. **Time limiting** these obligations is wise because, especially when an employee leaves the company, attention to the matter fades and after a time the situation is no longer viable. A longer timeframe for confidentially is only reasonable for particularly critical or sensitive data.

### 1.2.16 Particular rights and obligations

Agreements in the implementation can give rise to contract changes.

Every agreement contains conditions requiring particular attention. These could be agreed maintenance cycles or software releases for example. Practical management on implementation level may give rise to changes to contractual rights and obligations (by agreeing on specific procedures or accepting them by implication). Changes and specific implementations should therefore be checked at regular periods in meetings, and be brought into line with the contract. For these agreements not to bring about unintended contract changes unexpectedly, it is practical to qualify such understandings between the parties as mere implementation and not as changes to the contract.

A high level of security is offered by forming a "Coordination committee" that is not involved in direct implementation and to which regular reports are submitted. Its remit is to monitor the alignment of the actual reality with the contractual reality. Note that the agreement on contract changes in writing, for example, cannot help here – even a relevant clause can itself be waived in the event of non-compliance in practise (also see → 1.2.24).

### 1.2.17 Development machine

It may be the case in exceptional circumstances that a separate development machine is necessary for certain software developments so as to avoid interrupting ongoing operation with test runs. This must be explicitly agreed however. In terms of content, this corresponds to an additional, separate service contract for these kinds of foreseeable time-based processes. The issues to be regulated would be who makes the machine available when and where, and with which capacity, and how it may be used.

### 1.2.18 Data protection register reports

A reporting obligation to the data protection register must be clarified and its implementation regulated.

As described in more detail in → 1.2.5, the data processed in the SaaS model is usually personal data for which the Data Protection Act has defined rules. Reporting of data processing to the data protection register may be redundant if certain conditions are in place (see § 17 ☞ DSG 2000). Reporting is required in all other cases. Because a certain level of expertise is required for this report (§ 19 DSG 2000) that is not available everywhere, entrusting the specialists with reporting to the data protection register is recommended. However, these must also assume compensation and administrative law liability in the event of erroneous reports. The register reports must be sent electronically in the future (over the Internet). Examples can be found on the Data Protection Commission (DSK) website (www.dsk.gv.at).

### 1.2.19 Warranty

The provider must guarantee a service that is free of deficiencies. Deficiencies must first and foremost be rectified free of charge.

The contractual warranty is governed in §§ 922ff ☞ GENERAL CIVIC CODE and determines the liability of contractual partners for the **defectiveness of the service rendered**. A defect is understood to be a departure of the service rendered from the properties due contractually or normally presupposed (see → 2.1.4). Warranty obligations are of course also in place for new developments and development versions.

Austrian warranty law is a **two-stage system**. Primarily, the provider providing a poor service is given the opportunity for improvement within an appropriate timeframe, the overhead for which must already be included in the payment for the service. If this is not possible because the deficiency cannot be rectified[4], secondary warranty mechanisms are applied: **Price reduction** or **annulment of contract**.

Annulment is only possible for "non-neglibable[5]" defects. Only a price reduction can be demanded for negligible defects.

In Austria, warranty obligation is two years for moveable items. The warranty period starts when the service is delivered in full.

Restrictions of the warranty obligation are only justifiable objectively in exceptional cases.

The restriction, or even exclusion, of the warranty is virtually the rule in IT contracts. The warranty restrictions are often skilfully disguised in the ☞ GENERAL TERMS AND CONDITIONS of the contract[6]. The methods used here range from the forthright restriction, ideological-rhetorical arguments, introduction of different fault and deficiencies terms, division of the software into maintenance classes & reclassification to constraint

[4] *A fault is also non-rectifiable when it can only be improved with disproportionately high overhead or the obligated party does not rectify the defect.*

[5] *Traditionally a deficiency is defined as "non-negligible" when it prevents the usual or expressly agreed usage of the item in question, or the item in question does not have an agreed feature.*

[6] *Details in Ertl/Wolf, Die Software im österreichischen Zivilrecht (Software in Austrian Civil Law), 225ff, 304ff; Ertl, Allgemeine Geschäftsbedingungen der Softwareverträge, in EDV&Recht (General terms of business of software contracts, in IT and law) 1/94, 19ff; Staudegger, Rechtsfragen bei Individualsoftware (Points of law for customer software), 1995, 102 ff.*

of legal redress and replacement of fault rectification with new releases. This type is particularly popular for standardised software. These kinds of limitations of the warrant obligation are immoral in many cases, and hence not valid.

In practise, difficulties arise in determining the scope of the warranty because certain software packages are excluded from maintenance (because for example they have yet to be successfully introduced into the overall software product). The service provider is well advised to expressly exclude such components from the main liability, and hence also from the warranty. This is of particular importance when the software does not come from the provider, and features are promised in the documentation that cannot be implemented without fundamental modifications to the software. The effects of such an exclusion on other parts of the software are often unpredictable however.

One of the particular difficulties in SaaS contracts is the interleaving between continuing obligation and short-term contract. The higher-level framework is the continuing obligation, but individual services can be short-term contracts. The legal warranty consequences are sometimes different. In order to determine the correct assignment, a check must be carried out on how a fault effects these two different obligation structures. There are for example mistakes in the framework contract (continuing obligation) that appear as mistakes in the individual service. Conversely, not every mistake in an individual service need be a mistake in the framework contract.

Non-rectifiable deficiencies in the continuing obligation can be compensated to a certain extent by reducing payment (in the same way as interest reduction in § 1096 General Civil Code[7]). This only applies for negligible non-rectifiable deficiencies however. If the fault is not

[7] *§ 1096 para. 1, 2nd sentence in General Civil Code: "If the item in question is deficient on transfer, or it becomes deficient during the period in question through no fault of the receiver to such an extent that it is unfit for the use stipulated, the receiver is exonerated from the payment of interest over the period in which, and to the extent to which, it is rendered unusable."*

negligible, only an extraordinary termination or potential compensation claim remains. Reducing the payment to zero cannot be expected of the service provider, however, because the service obligation would then remain free-of-charge for the contract term.

| Deficiency | Overall service | Individual service | Legal consequence | Comment |
|---|---|---|---|---|
| **Non-rectifiable** | Non-negligible | Non-negligible | Annulment of the individual service, extraordinary termination of the overall contract | The specific value of the individual service must be determined |
|  | Negligible | Non-negligible | Annulment of the individual service and reduction in price of continuous service | Determination of the specific payment reduction for the continuous service is often difficult when the individual service is omitted |
|  | Negligible | Negligible | Payment reduction | Assessment of the individual service in money, and reduction of payment for continuous service (see above) |
| **Rectifiable** | Non-negligible | Non-negligible | Rectification obligation and payment reduction until improvement | Payment reduction by packages; assessment of the individual service can be difficult here too |
|  | Negligible | Non-negligible |  |  |
|  | Negligible | Negligible |  |  |

Non-negligible, non-rectifiable faults generally lead to annulment of the contract.

Deficiencies in individual services (deficiency rectification or changes and updates to the software package) have different legal consequences depending on the deficiency. Non-negligible, non-rectifiable faults generally result in annulment of the contract (whereby payment reduction can always be chosen by the party entitled to the warranty). However, termination of the contract via the individual service is not immediately possible or sensible for an SaaS agreement. This way an individual service not rendered often reduces the overall contractual service without the overall contract being terminated for this reason at the same time. Limitation of the legal consequences to the individual service agreed may therefore not be sufficient, but direct expansion to the overall contract on the other hand would be going too far. To clarify the legal consequences, the importance of the specific individual service within the overall structure of the software package and the agreed and expected effect on the overall service package must be assessed. The table above shows an overview of the potential scenarios and their effects.

Annulment of the individual service is problematic because in the rescission of the individual service the customer "...may not benefit from the loss or damage suffered by the other party.", in accordance with the second sentence of § 921 of the General Civil Code. This means however that the payment already received must be paid back to the service customer. Because usually an ongoing payment must be made in SaaS contracts, a part of the payment cannot be assigned directly to the individual service. This may lead to disputes. Discussing these scenarios in contract negotiations and including a payment determination formula in the contract are therefore strongly advised. An anticipatory regulation can help to settle the conflicting interests in a way that is fair to both arties and does not entail legal proceedings.

It is important to remember that this is a **no-fault** warranty. If either party is culpable for a fault, the provider is liable beyond the legal consequences of the warranty (also for the encumbered loss, such as to other material property or customer assets). § 1298 of the General Civil Code states that the provider must prove there is no blame on his part for the fault.

Moreover, the provider is considered an authority as laid down in § 1299 of the General Civil Code, and is therefore liable in accordance with the knowledge and skills pre-supposed, even if the provider does not possess these personally[8].

[8] *§ 1299 of the General Civil Code leaves no doubt: "All those taking up an office, an art, a trade or a profession, or voluntarily taking over a business without a situation of hardship, whose execution requires expertise or extraordinary diligence indicate by doing so that they believe that they have the necessary diligence and required specialist knowledge; Those in question must therefore take responsibility for deficiencies. [...]*

### 1.2.20 Compensation

Massive restrictions in compensation claims are contrary to a balanced contractual relationship.

Compensation claims are often subjected to massive restrictions in software contracts, be they exclude specific levels of blame (such as negligence) or by limitations to particular kinds of loss/damage. This is contrary to a balanced contractual relationship.

Restrictions to compensation liability are generally permissible by jurisdiction for cases of slight negligence (see also § 6 para. 2 Z 5 Consumer Protection Act[9] Legislation is heavily dependent on the individual case for gross negligence. Full liability, also for slight negligence, is commensurate with the law and is the fairest solution. This liability should only be restricted in well-justified cases and only on the basis of an adequate service in return. The non-usual exclusion of financial loss normally affects the main service in SaaS contracts and therefore means the exclusion of any liability. This results in gross discrimination of the service customer and would therefore be null and void according to § 879 para. 3 of the General Civil Code[10].

In the event of damage or loss, the liable party must always prove that it is not at fault for the damage in the event of contract breaches.

One should also consider that, according to legislation from the ☞ OGH (SUPREME COURT), a large company which receives legal advice and still includes illegal clauses in its contract, becomes liable for compensation regardless of the clauses in question[11] .

It is also appropriate to consider the case in which third parties, in conjunction with the contract, assert compensation claims against a contractual party. Requiring clarification here is whether and how any compensation for loss between the two parties is regulated in such a case.

[9] *In consumer transactions, a restriction or exclusion of compensation obligations is only permitted when the businessperson proves that these have been specifically negotiated individually.*

[10] *§ 879 para. 3 of the General Civil Code: A contractual regulation contained in the general terms of business or contract forms that does not lay down one of the mutual main services is always null and void when it grossly discriminates one side in due consideration of all the case facts.*

[11] *10 Ob 23/04m (JBL 2005, 443 = ecolex 2005/205)*

## 1.2.21 Service exemptions and force majeure

The scope of services obligation is defined in the subject matter of the contract. Certain areas therein can then be specifically excluded. Anticipated forms force majeure should be included for clarification (see → 1.2.1).

Legal regulations are inevitably not always appropriate for certain areas of the business world[12]. This is particularly true for cases of force majeure, i.e. causes and factors on which none of the contractual parties can reasonably be expected to have any influence. These must be defined adequately for specific cases and be regulated in the contract as force majeure (see also → 2.1.9).

A term for force majeure that is applicable in the same way for all fields of law, and that is explicitly stipulated by law, does not exist however. The parties must therefore go through the process of localising and formulating when drawing up a contract. The more the conditions for force majeure are narrowed down, the higher the price because this increases the risk of a loss occurring which is not categorised as force majeure. The insurability of these risks and their costs are a useful reference to the higher risk.

## 1.2.22 Company transfer

The newspapers are full of company mergers and acquisitions, be they hostile or friendly. In many cases however, these kinds of undertakings can mean a considerable disadvantage for one of the two contractual parties, especially when competitors suddenly get dangerously close. In such cases it is necessary to agree on a duty to inform the other contractual partner promptly and an extraordinary termination right.

In the event of a company transfer, agree on a requirement to provide information and an extraordinary termination right!

[12] *Provided the list of provisions does not become so long that it is unclear and contradictory, the law can only consider standard cases and must leave settlement to the contractual parties on a case-by-case basis.*

### 1.2.23 Insolvency and liquidation

Contracts can only be terminated for important reasons during the restructuring process; insolvency itself does not count.

The insolvency law amendment in 2010 replaced former potential "compensation" with the **restructuring process**. This saw major expansion and additions. From now on, contractual relationships can only be terminated during the restructuring phase by contractual partners of the insolvent company **for an important reason** (when termination of the contract is not essential to avert serious personal or financial disadvantage). A deterioration of the economic situation and arrears in payments which became due prior to starting the insolvency process expressly do not provide entitlement to cancellation. This cannot be subject to different contractual regulations. It is only when restructuring fails that bankruptcy is declared and bankruptcy rules then apply, albeit in a somewhat stricter form than previously.

**Bankruptcy** is always a disadvantage for the contractual partner because its entitlements in the event of insolvency are always valued in terms of money, and are settled at a rate less than 20% (if at all). Then come the additional costs for assertion of the claims. Conflicting contractual clauses are generally ineffective because the other debtees are almost always disadvantaged. This is tantamount to a contract at the expense of third parties.

Bankruptcy of the service provider is particularly problematic because the customer runs the risk of losing control of its data – and possibly of also being dragged itself into bankruptcy. This must be guarded against contractually (see → 1.4.1).

**Liquidation** of the provider is generally less risky unless it occurs abruptly without any notice. But because there is always a possibility of this happening, the same measures as those adopted in bankruptcy are conducive to achieving the desired outcome.

## 1.2.24 Miscellaneous

Generally grouped under ″Miscellaneous″ are all remaining clauses that cannot be assigned to any other section of the contract.

Arbitration court instead of public jurisdiction?

Typically agreed here for example is that disputes are heard by an arbitration panel instead of a public court. The benefits of arbitration panels are that they sit in closed sessions and that their arbitration awards are recognised and enforceable in virtually every country. In straightforward cases they can also be faster than a public court. However, if a case is complicated and requires specialist expert knowledge, the process can take just as long as the public process. Also cited sometimes as a benefit is the fact that skilled arbitrators can be chosen. In practise, however, special expertise of an arbitrator is uncommon and so should not be relied upon. Also the arbitrator cannot really be asked about the kind of expert witness by the parties.

The opportunity for parties to have a strong influence over the code of procedure of the arbitration court, introduced in the civil process amendment in 2006, enables arbitration proceedings to be conducted more quickly. Adherence to the major parts of the legal system of the country in which the arbitration award is to be enforced is a requirement however. Otherwise the arbitration award is not enforceable due to infringement of the ″☞ ORDRE PUBLIC″.

Downsides of an arbitration court: higher costs, non-transparent legal position, lack of coercive means.

The downsides of an arbitration court are usually higher costs and, because of the closed sessions, broad non-transparency of the legal position. Also, no coercive measures can be taken in the evidence taking procedure, such as in regard to the statements of witnesses or the publishing of third party documents. Arbitration proceedings can therefore put the weaker party at a disadvantage. A just and valid arbitration clause is necessary in the contract for effectual arbitration proceedings to be held.

SaaS contracts are often cross-border contracts. In addition to the ☞ GENERAL CIVIL CODE and the ☞ UGB (AUSTRIAN CORPORATE CODE), the **UN Convention on the International Sale of Goods (UN CISG)** and EU ordinances **Rom I** (for contractual relationships) and **Rom II** (for non-contractual obligations) may then be applicable, unless they have been expressly and intentionally excluded. The contractual parties must decide which choice of law they opt for (whereby the choice of legal system can not be expected to benefit either party in any particular dispute). The inclusion of these transnational regulations always presupposes knowledge and viable application of them however. In particular, inclusion can be beneficial when the potential foreign legal system is broadly unknown or when it differs greatly and unfavourably from national law. The United Nations CISG always applies in international contracts if not expressly excluded. The EU enforcement ordinance simplifies and greatly accelerates execution within the EU. This should be taken into consideration in contract negotiations.

The very popular ″severability clause″, stating that any lapse of a contract provision leaves the other provisions unaffected, and that the invalid clause must be replaced by a valid clause which comes as close as possible to pursuing the purpose of the invalid clause, is useless in many cases. Firstly, both public courts and arbitration courts must generally draw up the contract such that it can be upheld (design that preserves contract validity). Secondly, replacing an invalid clause with another valid regulation that is approximate or comparable is generally not feasible because it undermines legal invalidity regulations (including § 879 para. 1 ABGB (General Civil Code)[13] and § 6 para. 3 of KSchG (Consumer Protection Act[14])·

It is therefore not permitted by courts. So the severability clause is generally useless because it feigns something that cannot be implemented.

[13] *§ 879 para. 1 of the General Civil Code: ″″A contract that violates legal prohibitions or good morals is null and void.*

[14] *§ 6 para. 3 of the Consumer Protection Act: A contractual regulation contained in the general terms of business or contract forms is ineffective if its formulation is unclear or incomprehensible.*

The severability clause is however used in a very targeted manner in many cases. For example, it is not common in ☞ GENERAL TERMS AND CONDITIONS to include standards that are very obviously against public policy, such as an almost all out disclaiming of liability from warranty and compensation obligations. Just how far such a contractual liability exclusion goes is often contentious, but the creator of the general terms and conditions has not even made an effort to find a formulation that could come near satisfying the demands of the courts. Rather, the very general formulation should consciously incriminate the contractual partner with an artificially created legal uncertainty risk.

Agreement of the **contract in the written form** is almost always a matter of course. It states that all agreements and changes to the contract must be concluded in writing for them to become effective. However, this proviso does not have the absolute effectiveness it is often assumed to have because, according to Austrian civil law, such contracts are not subject to formal requirements. This means that the parties can depart by mutual agreement at any time from the proviso agreed – even verbally! This departure need not even be explicit and can also be implicit. However, the ☞ SUPREME COURT would take a very critical view of the departure from the proviso on the basis on non-explicit declarations and would arrive at a strict judgement. Because of the improvement in the body of evidence, the strong recommendation is to conclude contracts, and all additions and changes, in writing.

Departure from a contractually agreed written form understanding is possible at any time by mutual consent – even verbally!

## 1.3 Disputes

### 1.3.1 Procedure for extrajudicial settlement

If disputes arise between the parties, it is important for both sides to resolve these as quickly and as smoothly as possible. A public court or an agreed arbitration court can be used for this (→ 1.2.24). Beforehand, however, it may be expedient to appoint a **mediator** who does not pronounce a judgement but instead helps both parties to approach the other and to end the conflict amicably. There is a risk of procrastination here however.

In the American legal system in particular, different procedures have arisen to avert judicial proceedings in which the two sides require each other to collate the evidence pertaining to the dispute and available, and to submit it to the opposing party. Both management teams then get together and attempt to resolve the dispute amicably with appropriate legal consultation. The matter can be brought before a court if agreement cannot be reached. Both parties however commit to limiting themselves to the evidence that has been collated and submitted and to justifying any evidence extending beyond this and explaining why it was not submitted before.

## 1.4 Insolvency

### 1.4.1 Access to data irrespective of procedure

Bankruptcy of one contractual partner is always disadvantageous to the other. A particularly critical situation would be if a service provider were to go bankrupt because the full power of disposal over company data and programmes passes over to the insolvency administrator or **liquidator.**

In the event of bankruptcy, it is important to ensure that company data and programmes can continue to be accessed.

The insolvency administrator or liquidator represents solely the interests of the company debtees and they can be completely different to those of the original company and now common debtor – especially in the case where the company is not continuing. The insolvency administrator is also not very likely to have experience in the IT business.

Clarification is therefore required between the two parties as to how provision is to be secured in the event of provider insolvency. The solution agreed must ensure that, in the event of bankruptcy, company data and programmes used can be accessed at short notice. Whilst a foresighted contractual solution for the insolvency should be attempted, it must be taken into consideration that insolvency law is extensively mandatory law and cannot be bypassed with a contract. This difficulty was intensified with the insolvency law amendment in 2010.

The best protection can be provided if the customer's data remains its **property** and as such identifiable within the domain of the service provider. However, this presupposes that it can be physically separated (own server) and that it can be made available to the customer in one form or another, preferably daily or at least once a week (recovery of the used and processed data as a backup). Because the data by itself is not enough for continued use, a foresighted agreement must also be reached on the used and current processing software. This can be implemented by keeping the most recent version, including installation and user guides, at a trustworthy location such that the customer, in the event of bankruptcy, is able to continue processing its data within a reasonable period of time at either the customer site or another provider.

Another option for precluding problems in the event of bankruptcy of the SaaS provider is a **three party solution**. Another contract is then concluded with another SaaS provider in addition to the actual contractual partner. Agreed in this contract are regular transfer of data and continuation of the service in the event of specific kinds of failure at the primary provider.

In a three party solution, an additional contractual partner guarantees continuation of the service when the SaaS provider fails to deliver.

A contract specifying the modalities of the transfer of data and service is also concluded between the two providers. This solution is currently not very widespread, but could be offered as a standardised solution by SaaS providers operating in reciprocal alliance with others. This enables the reliability and security of the software service to be increased enormously at a relatively low additional cost.

Without such agreements in place, it can easily be the case that the service provider, in the event of its bankruptcy, drags with it one or more customers into insolvency, or at least damnifies them, without an equivalent compensation claim being enforceable.

Another risk arises when a debtee of the provider, through a court, initiates **execution** of individual provider items. The provider is only able to actively prevent this by making clear to the debtee, and potentially also to the bailiff and insolvency administrator, that this entails accessing third party items, or items carrying third party rights. The contract should therefore also contain an obligation on the part of the provider, in the event of executive access to

Put into place a duty to furnish information on the part of the provider in the event of execution.

items, data and programmes belonging to the customer or that greatly affect the scope of service between provider and customer, to immediately point out the risk to an insolvency administrator, debtee and bailiff and also to inform the customer of this event. At the enforcement court, the customer can then take action against this execution, and possibly avert it, with the nullity proceedings as laid down in § 37 of the Enforcement directive.

## 1.5 Compliance

In many industrial nations, the actions of many companies over recent years have resulted in considerable negative spin-offs and unfavourable economic consequences. These have heightened the demands made by society and politics of leaders of multinational organisations, or "compliance", to keep to **legal regulations** and to observe **ethnic principles**.

This should in itself be a matter of course. Nevertheless, the legal systems of internationally operating companies, very similar in execution yet different in individual issues, represent a temptation to capitalise on the differences (to the detriment of customer and financial authorities) to gain an advantage for companies. The compliance requirements made of these companies are now aimed at preventing this.

The stipulations of the USA within the **Sarbanes-Oxley Act (SOX)** and the lending guidelines of **Basel II** must be regarded critically for an Austrian SaaS provider or SaaS customer. For example, the SOX demands that companies trading on the stock exchange in the USA pass on data of third parties (such as customer, supplier and personal data). These demands are inconsistent with EU directives on data protection. The lending guidelines as laid down in Basel II are mandatory for the EU and must therefore be followed.

The compliance requirements are of course also targeted at **SaaS**

**providers and customers** who must familiarise themselves with these requirements and take them into account in their business policies, and hence also in two-way contractual relationships. A more detailed guide is not possible here because specific requirements considerably vary from case to case.

Both providers and customers must adhere to compliance requirements.

# 2.0

# Data protection and data security

# 2.1 Technical security

## 2.1.1 Redundant memory networks

Increasing of fail safety from RAID level 1.

The mass storage devices on which operative data is kept must be safeguarded against the harmful effects of a technical component failing. Hard drives are generally used for this. These are made fail-safe through **redundancy concepts**. One popular concept is the organisation of multiple physical hard drives into an array of hard drives (☞ RAID). The number following "RAID" is the **RAID level**, i.e. the internal structure of the memory network. The individual types differ in regard to their behaviour under read and write loading, and in regard to the gross to net capacity ratio. Note that the system reliability is not increased until RAID level 1 and higher. RAID 0 does not offer redundancy. A higher RAID level does not necessarily provide more security. Memory networks with RAID level 5 are common at the moment, RAID level 6 provides additional redundancy (two units can fail without data loss occurring).

## 2.1.2 Up-to-date information

When backups of operative data are created, how often these copies are generated determines how up-to-date the information is when it is recovered. Whether or not information is up-to-date is particularly important when data is lost as a result of user error or because of major and harmful incidents. This is because minor incidents can be caught by redundancy concepts (such as the failure of a hard drive, see → 2.1.1).

Making daily backups is a minimum requirement.

How up-to-date information the information needs to be depends on the type of data and how often changes are made. The creation of a **daily copy** is currently regarded as the most basic of measures.

## 2.1.3 Data recovery

When a loss occurs that necessitates the recovery of operative data, the time period required for it is a key parameter. The time is measured from the point the data loss is reported to the service provider up to when the data from the last backup is put into operation. This time should of course be as short as possible – specific requirements are heavily dependent on the particular application.

A decision must be made on whether all of the data needs to be recovered or whether only parts are affected. Data recovery usually means recovery of the entire data file. Depending on the provider's application and set-up, selective recoveries can be made by assigning version numbers to data files.

### 2.1.4 Recovery from a particular day

In data archiving, backups are stored even after the next backup run is performed. The number of archived backups and the timing are dependent on the type of application. Mixed concepts are often used which make the storage medium cheaper but slower as the information gets older and which reduce the number of copies with age.

Recovery from particular days is particularly necessary for statutory disclosure.

Recovery from particular days is particularly necessary for **statutory disclosure** (in accordance with § 26 ☞ DSG 2000) in cases when it must be specified to the affected data subject when and how long certain information was stored and when it was erased. Providing incomplete or incorrect information may result in the Data Protection Commission issuing administrative penalties. Tax related information is also a typical application for recoveries from particular days. The form of recovery is usually essential in such cases. A mandatory obligation to preserve information for seven years is in place for such cases. To satisfy this requirement, it is usually necessary to keep available the database as well as the application that first enabled the information to be read.

### 2.1.5 Continual monitoring of systems

To respond to any malfunctions of systems, they must be continually monitored. Fault events are usually detected using **automatic**

**monitoring systems** – the kind and selection of system states monitored for different quality levels, and the risks averted as a result, must be stated. The specific system states that require monitoring depend on the level of security required/desired. Monitoring of the system hardware, and general availability of the system, must always be considered a matter of course. The monitoring of individual services may also be necessary depending on application.

Continual monitoring of the system hardware and general availability of systems are a matter of course.

Attention must also be paid to the timeframe in which operating personnel are informed of faults and the timeframe in which it is possible to respond to it.

### 2.1.6 Physical separation

To prevent data loss in the event of a **major incident** (such as fire, flooding or earthquake), it is necessary to store backups in separate areas.

Under the terms of § 14 para. 1 ☞ DSG 2000, "In consideration of the technical options and economic viability, it must be guaranteed that information is protected from random and unlawful destruction, and from loss, that its use is proper and that information is not accessible to unauthorised persons". In this regard, paragraph 2 substantiates this norm under Section 4: "Access authorisation to customer and service provider facilities must be regulated".

With this, the legislative authority is implicitly stipulating that data processing, regardless of who performs it, must be organised such that data loss, unauthorised access to information and its destruction can be prevented. However, implementing this norm in practise means storing a copy of the data and the programmes in a safe environment, away from the normal processing area.

This is generally only possible with strict physical separation.
The extent to which this physical separation is required depends on specific circumstances. It certainly does not mean that the distance has to be many kilometres, but also does not imply that a simple sheet metal cabinet in the server room will be sufficient.

### 2.1.7 Protection against malware

Protection from malware is a commitment from both sides.

The use of anti-virus software to provide protection from threats such as computer viruses, Trojans and worms is standard today. Differences may arise in update management and relevant employee training. The protection of systems from malware is a **commitment from both sides** and cannot be limited to one firewall and one anti-virus programme. Access from inside the company to data processing systems running on external servers and access from outside the company to internal servers must be subject to specific and continually updated **rules** to prevent (as far as possible) the infiltration of malware or at least to detect it with regular checks. The use of Intrusion Prevention Systems (☞ IPS) is becoming increasingly common – these monitor data traffic at protocol level as well as at network level.

It is generally recognised that the company's in-house staff and the service provider's staff present the **greatest risk through incorrect operation**. Attacks from external sources are however also becoming increasingly severe, sophisticated and complex. It is therefore essential to remain alert to these threats and to keep an adequate log of such attacks.

### 2.1.8 Network security

Networks must also be safeguarded against faults and failure.

Just as servers and peripherals require protection from malware, attacks and manipulation from inside and outside, networks and their individual components must also be safeguarded from these kinds of threats as well as from faults and failure. This requires technical and organisational regulations, as well as monitoring actions that need regular checking and logging.

Firewalls and other active network components must be kept up-to-date in terms of operating software. Access to these elements requires strict regulation to help prevent manipulation. Only encrypted access should be used if possible and authentication should be based on certificates.

### 2.1.9 Security of technical equipment

For the security mechanisms mentioned above to be effective against loss and destruction of information, appropriate structural, electrical and organisational regulations must be followed and continually updated in setting up and operating an IT installation (that also renders services for third parties).

Structurally, these measures include **adhering to the minimum standards** for walls, floors and ceilings to provide protection from fire, water and burglary.

The entire IT network must also be protected from lightning strikes and electrical surges from the power supply. The prerequisite here is a proper lightning protection system for the building and correct earthing (star grounding of all earth conductors at one point). This is not enough however. Also, the lines of the internal network in the server room and those routed outside or to peripheral equipment must be laid such that there are no loop areas that could absorb the high-frequency oscillations of a lightning strike. This could result in irreparable damage to sensitive electronic equipment.

The protection of the server room from high water and fire-fighting water (for an external fire) must be planned in advance and guaranteed. Extinguishing equipment and fire alarm systems are indispensable in the server room.

To what extent video surveillance can be implemented for access to the server room and within the server room must be decided on a case-by-case basis (in light of the necessary permission from the Data Protection Commission). Intrusion protection must be in place in rooms housing critical network components (switches, routers and distributors), as well as for the server room itself.

# 2.2 Organisational security

## 2.2.1 Protection from access by unauthorised persons

Caution - protection from unauthorised access must also include the backups

**How passwords are treated**, the type of **authentication**, the **access regulations** and the **classification of information** by confidentiality and integrity must be taken into account when protecting the access to data. Do not forget that these protective measures must always include the backups as well.

To be clarified as overriding priorities:

- Who has what access to what information when?
- Is there a ☞ SECURITY POLICY in place (known internally)?
- Is there log information about every access?
- What protective measures are in place to protect against third party access?

Access authorisations must be regulated in a transparent and non-ambiguous manner. This also applies for employees at the customer site.

As shown → 1.2.5, most company information is covered by DSG 2000 even if it is not information about physical people (e.g. assets accounting information). Therefore practically all the information a company processes is subject to data protection laws and therefore requires protection and confidentiality. Data access must be regulated in an appropriately transparent and non-ambiguous manner. This also applies for employees at the customer site. Access authorisations must be safeguarded with appropriate measures (e.g. secure authentication and logging with digital signatures). It is essential to create an overall concept that defines and monitors both access and authentication by the customer's staff and the provider's staff.

Zur Verdeutlichung sei an dieser Stelle § 14 Abs. 1 und Abs. 2 DSG 2000 vollständig zitiert:

### Data Security Measures

§ 14 (1) Any unit of the client or service provider's organisation that use data must take measures to ensure data protection. Depending on the kind of data used as well as the extent and purpose of the use and considering the state of technical options and economic feasibility, it shall be ensured that the data is protected against accidental or intentional destruction or loss, that it is properly used and is not accessible to unauthorised persons.

(2) In particular, the following measures are to be taken insofar as necessary with regard to the last sentence of para 1:

1. The distribution of functions between organisational units as well as employees regarding the use of data shall be laid down expressly
2. The use of data must be tied to valid orders of the authorised organisational units or employees
3. Every employee shall be instructed on his obligations in accordance with this Federal Act and the internal data protection regulations, including data security regulations
4. The right of access to the premises at the client or service provider shall be regulated
5. The right of access to data and programmes, as well as the protection of storage media, shall be regulated to protect against access and use by unauthorised persons
6. The authorisation to operate data processing equipment shall be specified and every device shall be safeguarded from unauthorised operation by taking precautionary measures for the machines and programmes used
7. Logs shall be kept so that processing steps actually taken, as well as modifications, queries and transmissions in particular, can be traced to the extent necessary with regard to permissibility
8. Documentation shall be kept on the measures taken pursuant to subparas. 1 to 7 so as to facilitate control and conservation of evidence

These measures must, in due consideration of the technology available and the costs incurred in their implementation, safeguard a level of data protection appropriate to the risks arising from the use and the type of data to be protected.

### 2.2.2 Patch management

☞ PATCH management specifies the patches to be applied to which system at a particular time. It is to be used for the server software as well as for any client software potentially used. The use of supporting software enables the overview of version revisions and the chronological sequence of the changeover to be simplified and partially automated. Irrespective of this, these processes must be defined and the authorisations governing who may introduce which patches and where must be clearly managed.

### 2.2.3 Separation of development and production

Separation of productive and test systems is an absolute requirement.

The separation of productive and test systems is an absolute necessity. Only with comprehensive testing on a separate system that is virtually identical to the productive system can modifications and upgrades to applications be tested realistically and with a high degree of reliability.

The type and scope of testing should be documented, as should the results. Automatic test environments simplify the testing process and guarantee a constant quality level.

### 2.2.4 Using live data in test mode

Adherence to data protection when testing with live data.

Systematic test data should be used primarily for applications tests. This approach is not adequate in many cases and live data, or extracts thereof, must be used for testing. Adherence to data protection is required in this case. Also, the rights and possibilities for testers must be aligned to the heightened security level. Similarly, the logging of accesses must conform to a higher security level.

# 2.3 General

## 2.3.1 Data availability when the software service is not available

It is important to consider how available the information processed in the SaaS model is in case the software service becomes unavailable. A short-term failure of the service resulting in a lack of information usually only inhibits the operating processes within a company. Such a shortfall is not so serious and compensation can be agreed in the payment. It is however far more problematic for the company when data is unavailable for a prolonged period of time.

The requirements made of how up-to-date available information is, and the type of provision, vary from case to case and can only be defined in these specific circumstances. These should certainly be topics up for discussion.

A prerequisite for software-independent data availability is essentially an **Export function** that makes available data such that it can be read with generally available software. It is advisable to define in the contract which specific software should be used to read the data.

Software-independent data availability must be guaranteed with an Export function.

The situation becomes particularly critical if the service provider becomes insolvent because the power of disposal over the company's data and programmes is then transferred to the insolvency administrator (also see → 1.4.1).

## 2.3.2 Erasure of data

A service provider **can be required to erase data** at the customer's request or on the basis of mandatory obligations. Depending on the instruction, this can mean erasing just the up-to-date data or all the data stored in the archive. A distinction must also be made on whether this is erasure of all customer data or just some defined data.

A service provider can be required to erase data.

This means that an erasure request can sometimes entail **considerable overhead** for the provider. The recommendation therefore is prior clarification of the requirements that are technically possible and the overhead with which they are associated. Potential legal conditions may have to be observed here, such as the mandatory obligation to preserve information in accordance with § 14 para. 1 (see → 2.2.1) or § 27 para. 3 to 7 DSG 2000 (Data Protection Act).

The strict obligation in DSG 2000 to irrevocable data erasure also includes all backups.

For statutory erasure requests (§ 27 and § 28 of DSG 2000), it is not enough just to delete the data in the usual way, i.e with a simple system command. According to the law, there must be guarantees in place that the information has been erased irrevocably and that it cannot be recovered by any means at all. Note that this requirement also includes the backups that are normally available. It is also necessary to provide legally recognised verification of the erasure, such as in the form of a signed ☞ LOG FILE.

### 2.3.3 Data protection

Adherence to the regulations in ☞ DSG 2000 (DATA PROTECTION ACT) is a requirement for data protection. In this regard, the customer and provider must check the type of data to be processed and familiarise themselves with potential legal restrictions as regards processing and access.

Everyone has the right to information on data pertaining to himself.

DSG 2000 gives the data subject the constitutionally guaranteed right to obtain information at any time on the data processed pertaining to that person, its origin, the transmission recipients and the purpose of the processing and its legal bases in an understandable form (§ 26). This information must be available free of charge once a year. Associated with this is the right to have processed data corrected and erased. Technical and organisational regulations must be in place for this information to be issued in the first place.They are laid down abstractly in § 14 DSG (see → 2.2.1) and must be observed at all times. Otherwise inspections and recommendations from the Data Protection Commission, unfavourable judgements from civil courts (e.g. on compensation obligations) and administration penalties may follow.

# 3.0

# System reliability

## 3.1 Clarification from the supplier

In the negotiation phase, the service provider has the duty to address the subject of system reliability, to explain the major conditions and to synchronise the specific requirement with the customer. The provider must as a minimum provide information on what has been agreed in comparable cases, i.e. what is "standard". This disclosure is of fundamental importance. The provider is subjected to a **pre-contractual duty of disclosure** in this regard. The provider must ascertain the significance of the service to the customer to then determine the required availability. Failure to comply can entail liability for damages.

The provider is subject to a (pre-contractual) duty of disclosure.

## 3.2 Agreement of permissible downtimes

The required **operating times**, the **measurement time period** (month/year/quarter), the **availability as a percentage** within the measurement time period and the operating times must be determined as a minimum to satisfy this criterion.

Ascertainment of operating times, measurement time period and availability (in %).

An example is used to show how different interpretations and perceptions have a bearing on downtime values:

An availability rate of 99% is agreed between provider and customer (without specifying the measurement period).
In the first two months, the software is not available for a total of 84 hours during customer's critical hours, i.e. from 8:00 to 18:00 hrs. From the viewpoint of the customer, this means that the availability rate of the software service is just 80% because the measurement is taken over the critical 420 business hours (10 hours per each of the 21 workdays over a 2-month period).

The provider can rightly claim that the agreed availability target has been met if the measurement period is taken as one year with ″around the clock operation″. The 84 hours downtime figure means in this calculation an availability of 99.041%, measured over a total of 8760 hours (365 days, 24 hours per day). In this calculation however, the service may only fail for a maximum of 3.6 hours in the following 10 months.

The example highlights the different interpretations when no measurement periods are agreed. Had business hours from 8:00 to 18:00 hrs during an average month with 21 workdays been agreed, i.e. a time span of 210 hours in total, then an availability rate of 99% would mean a downtime of 2.1 hours and would therefore still be acceptable.

The requirements made of availability can vary greatly depending on the type of workplace and service.

It must also be noted in the contract agreement that the requirements made of availability can **greatly vary** depending on workplace and service. For example, the service hours for particular workplaces can be restricted to 8:00 to 18:00 hrs on weekdays, with an average downtime of 2 hours per month being acceptable and the availability corresponding to about 99.1%. The lower limit stands at around 97%, meaning a downtime of about 6.6 hours per month. On the other hand, for services critical to the company, availability from Monday to Saturday from 7:00 to 20:00 hrs (so a total of 318 hours a month) may be necessary with a possible downtime of about a quarter of an hour per month on average. This corresponds to an availability of 99.93% per month. The lower level is at 99.5%, so about 1.7 hours a month for these services. If services are rendered across multiple time zones, the availability necessary for these services quickly rises to 99.95% per month and more. Very sophisticated concepts with managed maintenance windows, schedules and notice periods need to be developed for these scenarios.

It may be advisable in some circumstances to go beyond the minimum requirement of the contractual specification of an overall availability rate and to introduce different ″failure″ categories, such as ″complete failure″, ″partial failure″ and ″minor reduction″.

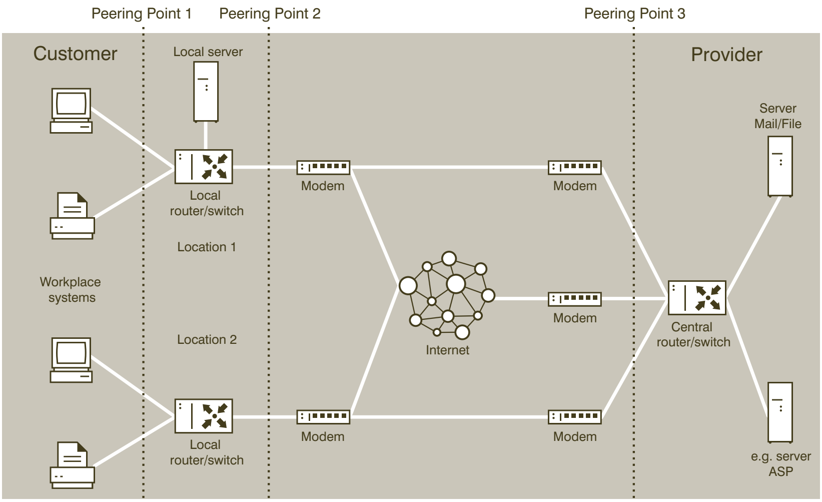
# 3.3 Determining the methods for ascertaining failures

It is advisable to define how a failure is actually ascertained and what measures should then be taken. The measurement depends on the specific service. If ″fulfilment on site″ has been agreed for example, the measurement must also include the availability of the local internet. To prevent such a proliferation, it is advisable to agree on availability up to a certain **Peering Point**.

It is best to agree on availability up to a certain Peering Point.

There are multiple variants for where the Peering Point is located and what areas it includes. The following diagram shows the different options.

Example of an SaaS service



The most favourable solution for the software provider is a Peering Point at the exit of the central router (Peering Point 3). The provider then only assumes liability for the components under the provider's immediate control, namely server, central router and the cabling in between. The customer on the other hand has to deal with the sourcing and setting up of all components such as modems, lines, routers, firewalls, any local servers and PCs, as well as the cabling in between, and has to ensure that everything stays up and running smoothly.

The most favourable solution for the customer is when the Peering Point is immediately next to the customer equipment with which the software service is used (Peering Point 1). This is because the provider then has to assume responsibility for sourcing, setting up and keeping all the components up and running (from the server to the end user equipment at the customer's site). This is a particularly viable solution for the customer when the customer has little or no expert knowledge of IT equipment and its operation (provided of course that the provider can render these services in the first place).

Peering Point 2 represents a compromise. The provider is then responsible for data transmission to the customer, and provides and supports the leased line and also the internet service to the customer. Local networking is then up to the customer.

The series connection of the individual components (from the diagram) must be taken into account when determining the availability of the software service. Connection of equipment in parallel is also used for redundancy concepts. The resulting reliability and availability can be calculated for each of these connection concepts. The calculation becomes complicated for a mixture of series and parallel connections. Reference is made to the "**Reliability analysis**" literature for the determination of availability for all three concepts.

## 3.4 Defined follow-up actions

To avert disputes, it is important to specify which actions are to be taken by the service provider and potentially by the customer in the event of non-availability of the software service. It is important first and foremost to agree a specific approach (see also → 1.2.4). For example:

A specific approach should be agreed in the event of non-availability.

- A measurement is taken on the customer's computer in response to a fault report by the customer (agree on contacts for rectifying faults).
- Escalation management: Defined for this are the hierarchical contacts on the side assuming responsibility who are approached when the preceding contacts are unable to rectify the fault.
- Which mutual obligations must be satisfied by the contractual parties in order to restore the contractually agreed state?

## 3.5 Agreement of a (financial) sanction when agreed thresholds are exceeded

Sanctions must be agreed for when agreed downtimes are exceeded. There are essentially two options here: **Payment reduction** or **penalty payment** (flat-rate compensation).

Customers are subject to a duty to avert, minimise or mitigate loss

Note here however that the customer has a duty to avert, minimise or mitigate loss. This means the customer must take reasonable steps to keep the losses arising from the failure as low as possible. Objections to this can be argued by the provider in dispute proceedings.

Caution – provider may be required to give warning in the event of an extraordinary fault even if this has not been agreed explicitly. Its default can constitute a liability for damages on the part of the provider.

# 4.0

# In-service behaviour

# 4.1 Response time behaviour

## 4.1.1 (Pre-)contractual clarification from the supplier

The submissions in → 3.1 apply in the same way. In the negotiation phase, the service provider has the duty to actively reference the subject of response time behaviour, to explain the major conditions and to coordinate the specific requirement with the customer. Failure to comply with the pre-contractual duty of clarification may lead to legal compensation consequences.

## 4.1.2 Determination of response time behaviour parameters

The term "response time behaviour" is often paraphrased as the **performance** of a service, but the former is more accurate and is hence used here as the preference.

Longer response times can amount to considerable waiting times.

**Response time behaviour** is generally understood to be the time interval between initiating a request and the displaying of the response on the screen or beginning of the required reaction on a PC. Experience has shown that this time should not be longer than one second on average for screen work. This is because longer times result in considerable waiting periods when taken over a month. For example, bookkeeping work involves the entering of up to 300 requests or accountancy records a day. An average waiting time of two seconds would mean a total of 600 seconds per day. For an average of 21 workdays in a month, this would mean 12,600 seconds or 3.5 hours per month...

The response time is generally measured with system software on the PC. A continuous log should be kept for verification purposes. This also enables the content of the Service Level Agreement to be monitored.

The response time can be planned using an appropriately applied ☞ QUEUEING THEORY. The telecommunications industry has for decades developped and published appropriate formulae and tables that can also be applied to IT components.

The average response time, the percentage to be attained and the measurement period must be defined.

The commitment by the provider should include **average response time**, the **percentage** to be attained and the **measurement period**. This period should include the primary traffic hour determined with a measurement over at least a week. This measurement must be repeated more often because this hour can change as a result of organisational modifications and other employees.

One example agreement as regards response time behaviour could take on the following form:

- Response time maximum 0.9 seconds; the response is therefore on the screen after 0.9 seconds or earlier
- Percentage: 95%; the maximum response time 0.9 seconds is observed for 95% of all cases (or in other words only 5% of the response times take longer than 0.9 seconds)
- Measurement period: 10:15 to 11:15 hrs; the values specified are attained within this period in which generally the highest levels of traffic occur.

### 4.1.3 Determination of the measurement methods

Agreement on the definitive measurement point is important.

The provider should offer appropriate measurement software for this. Some measurement methods have established themselves.

It is also important here to define the measurement location (see also → 3.3 and the diagram). This must be specified depending on the scope of the service agreed in the contract. A verification option on a PC can also be offered.

### 4.1.4 Defined follow-up actions

As mentioned in more detail in → 3.4, specific measures to be taken in the event of delayed response times should be agreed between provider and customer.

### 4.1.5 (Financial) sanction when agreed thresholds are exceeded

Agreeing a financial sanction is a viable measure to guarantee compliance with the agreed parameters. The adverse effect caused by exceeding the permitted waiting time agreed is simple to ascertain. Reimbursement for exceeding the permitted waiting time must be provided, either in the form of **payment reduction** or flat-rate **compensation**.

The actual adverse affect is often difficult to ascertain and could be detrimental to both contractual partners. The purpose therefore is to agree a fair level of compensation.

The objective is fair compensation for incurred losses.

### 4.1.6 Protection of the overall system from sporadic overload

Which precautions the service provider has in place for **load peaks** can play a major role in the smooth operation of a software service. In many cases, it is wise for the service provider to contractually agree the option to protect the system from overload with partial restriction of the service (i.e. of computing capacity) – especially when it is caused by maloperation on the part of the customer or by them exceeding the maximum agreed load.

## 4.2 Organisational & technical scalability

### 4.2.1 Disclosure of system-related parameters by the provider

The service provider must be able to provide information on the load thresholds of the system. The specific scalability requirements naturally depend heavily on the specific customer requirements.

It must be possible to provide information on the system's load thresholds.

# 5.0

# Glossary

# Glossary

## ABGB

″Allgemeines Bürgerliches Gesetzbuch″ or General Civil Code – the most important codification of civil right in Austria, effective since 1812 and therefore the oldest applicable law code in the German-speaking world.

## AGB

″Allgemeine Geschäftsbedingungen″ or General Terms and Conditions; pre-formulated contractual conditions of the service provider (colloquially also called the ″small print″)

## Application Service Providing (ASP)

Original common term for ″Software as a Service (SaaS)″, now broadly used synonymously

## Consumer transactions

According to § 1 para. 1 of the Consumer Protection Act (KSchG), these are legal transactions in which, on the one hand, a party is involved for whom the transaction is part of running the business and, on the other hand, a party for whom this does not apply (the ″consumer″). The common business term for this is ″B2C″ (″Business to Consumer″).

## Continuing obligation

Contractual relationship created for a prolonged period, i.e. does not expire after a one-off service exchange (e.g. rental, employment status); Target (or goal) obligation: The service content is already defined on contract conclusion (in full) or is at least determinable (e.g. purchasing contract and work & services contract).

### DSG 2000

The Data Protection Law applicable in Austria

### Intrusion Prevention System (IPS)

An IPS is a protection and monitoring system integrated in a data line that monitors all incoming and outgoing traffic (similar to a firewall). When an IPS detects a suspicious data packet, it is blocked immediately and not allowed to enter the network.

### ITIL

"IT Infrastructure Library"; a collection of Good Practices in a series of publications defining possible implementation of IT Service Management (ITSM) and now a de-facto international standard. Described in the set of rules and definitions are the processes, structure organisation and tools necessary for operation of an IT infrastructure. The ITIL is based on the commercial value-add to be attained by the customer through operating an IT system. Topics covered are the planning, rendering, support and efficiency optimisation of IT services with regard to their benefit as relevant factors in meeting the business objectives of a company. (source: Wikipedia)

### KSchG

Austrian Consumer Protection Law

### Log data / log file

Automatic logging of all or specific actions in a computer system

### OGH

"Oberster Gerichtshof" or Supreme Court; the highest instance in civil and criminal cases in Austria, and therefore authoritative in the formation of legal entities.

### Ordre public

(French for public order), understood to be the "fundamental assessments of a legal order". In essence, the general rules state that a foreign ruling is not recognised, and is therefore not enforceable, if it is obviously inconsistent with the endorsement of public order (ordre public) in the state in which it is being brought to execution.

Within the EU, application of the ″Ordre public″ has been rendered inoperable to a large extent by the EU Enforcement Order. This decrees that a court or arbitration panel judgement to be enforced from an EU member state may no longer be reviewed in this regard. The underlying thought here is that the fundamental judgements of the legal systems of EU member states are harmonised with each other and with the EU Charter of Basic Rights.

## Patch

A patch is understood to be the provision of a (small) software package that is used for example to plug security loopholes, to rectify software bugs or to enhance programme functionality.

## Prohibition of assignment

Here one or both contractual partners are prohibited from transferring claims from the contract to a third party. The most common scenario is the sale of claims to a ″factor bank″. A claim for amount x is then sold at (immediately payable) price y (lower than x). This can be useful when you are experiencing liquidity shortfalls because amount y is received, and can be accessed, for claim x even though payment y is not yet due.

## Queueing theory

As an area of telecommunication engineering, queueing theory explores the behaviour of message sources and their interaction with telecommunication systems. The queueing theory enables systems to be configured such that blocking due to overloading does not extend beyond a reasonable limit. The legalities ascertained also apply to data traffic to a limited extent.

## RAID

″Redundant Array of Independent Disks″, originally ″Redundant Array of Inexpensive Disks″; In RAID systems, multiple physical hard drives are organised into an array such that a part of the disc capacity is used for the storage of similar kinds of information. Data can then be recovered in the event of a failure, and high transfer rates can be attained. RAID systems provide the option of swapping out (failed) hard drives during live operation. The individual configurations are known as RAID levels.

### Software as a Service (SaaS)

Software as a Service (SaaS) is the name given to the provision of applications and programme functionality for use over a computer network. An Application Service Provider makes available either standard software or software developed specially for this purpose, as well as the infrastructure required. The application is normally used by a number of users. Payment is generally based on a service contract, e.g. dependent on the number of transactions made or as a fixed monthly amount. The SaaS provider takes care of software licenses, maintenance and updates. Support is provided for users in an appropriate form.

### Security Policy

This is understood to be the internal company security guidelines. The purpose of the security policy is to safeguard the availability, integrity, confidentiality and authenticity of information, and it must be acknowledged, understood and followed by all employees.

### UGB

″Unternehmensgesetzbuch″ or Austrian Commercial Code; a version of the old code, modernised in many areas, superseded this on 1.1.2005.

### Usability

The level of user friendliness of a system from the viewpoint of the user. A high usability level is reflected in simply manageable and intuitively understandable interaction.

# 6.0

# Useful aids for contract negotiations

# Overview of issues for negotiation preparation

Download overview: http://saas.clusterwien.at/5560579.0

Before you start talks with the potential contractual partner, it is sensible to define your own expectations based on the following points. Even if the required service does not offer any flexibility in the formation of the contract, it will be possible to gain a better assessment of existing risks by comparing your own expectations with the terms and conditions. And where clarity is not achieved due to a lack of precise information from the supplier, you should try to assess the possible consequences particularly carefully.

- □ Which software (features)?
- □ How is it provided (availability, measurement period)?
- □ How are faults/problems reported and rectified?
- □ Anti-virus and malware protection (who, how and update period)?
- □ What is the data backup like?
- □ How is data protection guaranteed?
- □ What are the requirements (who and how many people have been prepared for this contract and then actively involved)? What hardware and what software is available for the connection to the supplier? Which of the requirements listed above and below are covered by my company as complementary performance?
- □ How are service changes/upgrades reported and handled by myself/the contractual partner?
- □ What is the documentation for the software like and what requirements are placed on the training level of your own personnel?
- □ What training is required and how will this be given?

□ What is the term definition for the service?

□ What notice periods are in place?

□ What requirements, timeframes and penalties are specified under the confidentiality obligations?

□ Is a non-disclosure agreement necessary?

□ Are there any particular rights and obligations in place for the contractual partner and myself? (Notification obligations, service provision, legal matters and services, operational services)

□ How are new developments and updates carried out and put into live operation?

□ Who creates data processing register reports and how? (Fulfilment of the Austrian DSG 2000 and potentially EU Directive 95/46/EC and EU Directive 2002/58/EC)

□ What is the warranty like?

□ What compensation regulations are necessary and feasible?

□ Which service exemptions can be agreed under the provisions of force majeure?

□ How are disputes resolved?

□ How will the company's own interests be safeguarded if the contractual partner goes bankrupt?

If you have clarified your own expectations for each point then you are ready for preparatory contract negotiations.

Download overview: http://saas.clusterwien.at/5560579.0

# Checklist for contract negotiations

Download checklist from: http://saas.clusterwien.at/5560582.0

This checklist is intended for simpler cases of SaaS contract negotiations. If it is not adequate for your purposes, a **comprehensive questionnaire** is available for download from http://saas.clusterwien.at/5560585.0

It makes most sense for both contractual parties to use the checklist together as the basis for negotiation talks. As these talks can often last for several days, the individual points that have been successfully finalised should be ticked and dated. The results on each point should be recorded in writing in an essential accompanying report. The accompanying report and the questionnaire shall be signed by both parties and will be used as evidence and an appendix to the SaaS contract. This increases the chances that the key sticking points will be clarified before the contract is concluded and implemented.

| No. | Description | ☞ SAAS GUIDE | ☑ | Date |
|---|---|---|---|---|

# Performance and remuneration

| | | | | |
|---|---|---|---|---|
| | 1.1 Subject of the contract | | | |
| 1 | Are the key properties of the software/hardware to be used known (functions, memory capacity, user numbers, transaction volume, response time behaviour etc.)? | → 1.2.1<br>→ 1.2.3<br>→ 1.2.12<br>→ 4.1 | □ | |
| 2 | Definitions clarified and specified (glossary and list of abbreviations)? | → 1.2.2 | □ | |
| | 1.2 Provision, operation and support | | | |
| 3 | When can test operation and live operation be started? | → 1.2.3<br>→ 1.2.9 | □ | |

| No. | Description | ☞ SAAS GUIDE | ☑ | Date |
|---|---|---|---|---|
| 4 | How are existing data transferred at the start of operation (media, formats, structures)? | | □ | |
| 5 | Can operating times and requirements be achieved? | → 1.2.3 | □ | |
| | 1.3 Availability of overall service | | | |
| 6 | What availability can the supplier promise for its services and for what assessment period and at what cost? | → 1.2.12<br>→ 3.2<br>→ 3.3 | □ | |
| | 1.4 Customer-specific developments | | | |
| 7 | What further supplements/enhancements are already planned? | → 1.2.7<br>→ 1.2.8 | □ | |
| 8 | If supplements/enhancements are mandatory, to what extent is the supplier prepared to grant the customer a right of termination? | → 1.2.7<br>→ 1.2.14 | □ | |
| | 1.5 Data protection and data backup | | | |
| 9 | What is the data backup like? | → 1.2.5 | □ | |
| 10 | How is data protection ensured and how is the Data Protection Act implemented? | → 1.2.5<br>→ 1.2.18 | □ | |
| 11 | What is access to the data backups like (also in relation to necessary changes or deletions, § 27 DSG [Data Protection Act] 2000) | → 2.1.4 | □ | |
| | 1.6 System requirements for the customer | | | |
| 12 | What system requirements (hardware and software) are needed from the customer? | → 1.2.6 | □ | |
| 13 | What update cycles are absolutely necessary for hardware and software? | → 1.2.7 | □ | |
| 14 | What network requirements (bandwidth, router, protocols, network addresses) are expected and can be achieved? | → 2.1.8 | □ | |
| 15 | Who is responsible for the network on the customer's premises? | → 3.3 | □ | |

| No. | Description | ☞ SAAS GUIDE | ☑ | Date |
|---|---|---|---|---|
| | 1.7 Training and support | | | |
| 16 | What training can the supplier offer/carry out? What content will be covered and how many people can be trained? | → 1.2.11 | □ | |
| 17 | What requirements must staff meet before they are trained? | → 1.2.11 | □ | |
| 18 | Costs and time for training (per person and module)? | → 1.2.11<br>→ 1.2.13 | □ | |
| | 1.8 Remuneration and payment conditions | | | |
| 19 | How will the supplier's services be invoiced (individually, at a flat rate, according to time or according to use of components)? | → 1.2.13 | □ | |
| | 1.9 Term and cancellation | | | |
| 20 | What contract term is the supplier aiming to achieve (unlimited, limited, waiver of entitlement to termination for one or both parties)? | → 1.2.14 | □ | |
| 21 | What regulations (data transfer and deletion etc.) are provided for the end of the contract? | → 1.2.14<br>→ 2.3.1 | □ | |
| 22 | How and in what period of time can the supplier reliably conduct and document the deletion of backups after the end of the contract? | → 1.2.14 | □ | |
| | 1.10 Warranty | | | |
| 23 | To what extent is the supplier prepared to undertake the statutory warranty for its services (as per §§ 922-933 and §§ 1096-1097 ABGB [General Civil Code])? | → 1.2.19 | □ | |
| 24 | What deadlines are agreed for the reporting of deficiencies? | → 1.2.19 | □ | |

| No. | Description | ☞ SAAS GUIDE | ☑ | Date |
|---|---|---|---|---|
| | 1.11 Compensation | | | |
| 25 | To what extent are the supplier and the customer prepared to be liable even for slight negligence? | → 1.2.20 | □ | |
| 26 | How will the settlement be carried out between the parties in relation to claims for compensation from third parties (infringement of third party rights by one of the parties)? | → 1.2.20 | □ | |
| | 1.12 Exemption from performance and force majeure | | | |
| 27 | What events are seen as force majeure and what other external influences will be included as reasons for exemption from performance? | → 1.2.21 | □ | |
| | 1.13 Company transfer | | | |
| 28 | Which companies are at least currently not acceptable for the customer/supplier if they conduct a friendly or hostile takeover of the supplier/customer or a merger is imminent between them and the supplier/customer or they are able to exert a significant influence over the supplier/customer? | → 1.2.22 | □ | |
| | 1.14 Bankruptcy | | | |
| 29 | What precautions have been implemented so that the customer will have access to its data if the supplier goes bankrupt? | → 1.4 | □ | |
| 30 | Is a backup of the customer's data and the software used by the supplier outside of the supplier's domain possible and at what cost? | → 1.4 | □ | |
| 31 | Is an alternative supplier conceivable in the event of bankruptcy and can the supplier name a supplier who is authorised as per insolvency law? | → 1.4 | □ | |

| No. | Description | ☞ SAAS GUIDE | ☑ | Date |
|---|---|---|---|---|
| | 1.15 Compliance | | | |
| 32 | Does the supplier comply with the Austrian Corporate Governance rules? | → 1.5 | □ | |
| 33 | If the customer has to comply with the Sarbanes-Oxley Act (USA, SOX), is the supplier prepared for this and does it consent to US-certified specialists inspecting its services for conformity with the SOX? | → 1.5 | □ | |

# Data protection and data security

| | | | | |
|---|---|---|---|---|
| | 2.1 Technical security | | | |
| | 2.1.1 Redundant memory networks | | | |
| 34 | Which redundancy concepts are applied or available? | → 2.1.1 | □ | |
| | 2.1.2 Up-to-date information | | | |
| 35 | How often is a data backup created (time interval/type)? | → 2.1.2 | □ | |
| 36 | Where is the backup data and is it physically secure? | | □ | |
| | 2.1.3 Data recovery | | | |
| 37 | How is data recovered following loss or damage? | → 2.1.3 | □ | |
| 38 | What time span has to be planned in for this? | → 2.1.3 | □ | |
| 39 | Is differentiation according to used data possible? | → 2.1.3 | □ | |
| 40 | Are data recovery tests also carried out and at what intervals? | | □ | |
| | 2.1.4 Protection against malware | | | |
| 41 | What safeguards does the supplier use against malware and which should the customer use? | → 2.1.7 | □ | |

| No. | Description | ☞ SAAS GUIDE | ☑ | Date |
|---|---|---|---|---|
| 42 | How often are these protection programs updated or should they be updated? | → 2.1.7 | □ | |
| | 2.2 Organisational security | | | |
| | 2.2.1 Protection against access by unauthorised persons | | | |
| 43 | What password security methods are proposed for the employees of the customer or the supplier? | → 2.2.1 | □ | |
| 44 | Do the databases allow differentiated access protection for data and datasets and for the programmes that are used? | → 2.2.1 | □ | |
| | 2.3 General | | | |
| | 2.3.1 Data availability when the software service is not available | | | |
| 45 | Can the supplier provide an export function which makes the customer's data available so that it can also be read and processed by other programs? | → 2.3.1 | □ | |
| 46 | Do these programs already have to be specifically named now? | → 2.3.1 | □ | |
| 47 | How often and in what way can the supplier legally provide the customer with its data so that even an executive intervention in relation to the supplier will not prevent the customer from accessing its data? | → 2.3.1 | □ | |
| 48 | How can the supplier ensure that the programs it uses will be available for the customer to use legally in the event of executive access to the supplier? | → 2.3.1 | □ | |

| No. | Description | ☞ SAAS GUIDE | ☑ | Date |
|---|---|---|---|---|
| | 2.3.2 Erasure of data | | | |
| 49 | Is it possible for individual pieces of data/entire datasets to be deleted on the request of the data subject and/or as a result of statutory requirements in all backups (§ 6(1)(5) DSG 2000)? | → 2.3.2 | □ | |
| 50 | Is it possible for datasets to be blocked for certain periods in the databases (§ 26(7) DSG 2000)? | → 2.3.2 | □ | |
| | 2.3.3 Data protection | | | |
| 51 | Are the supplier and its employees familiar with the Data Protection Act? | → 2.3.3 | □ | |
| 52 | Have its employees received corresponding instructions and have they signed written declarations? Can these be inspected? | → 2.3.3 | □ | |
| 53 | Have the databases provided to the customer been designed so that they can meet the requirements of §§ 6, 7, 9, 14 and 26 DSG 2000? | → 2.3.2<br>→ 2.3.3 | □ | |
| 54 | Is the supplier prepared to allow the Data Protection Commission or experts which it commissions to carry out the investigations required by law on its premises at any time? | → 2.3.3 | □ | |

# System reliability

| | | | | |
|---|---|---|---|---|
| | 3.1 Clarification from the supplier | | | |
| 55 | Is the supplier prepared to comprehensibly present and explain the matter of system reliability before the contract is concluded? | → 3.1 | □ | |

| No. | Description | ☞ SAAS GUIDE | ☑ | Date |
|---|---|---|---|---|
|  | 3.2 Agreement of the permitted downtimes |  |  |  |
| 56 | Has the customer given notification of its desired operating hours? Has it fully defined the percentage availabilities for all departments? | → 3.2 | □ |  |
| 57 | Have the corresponding measurement periods also been proposed? | → 3.2 | □ |  |
|  | 3.3 Specifying the methods for ascertaining failures |  |  |  |
| 58 | Have various failure scenarios been investigated and substantiated? | → 3.3 | □ |  |
| 59 | How are failures identified? | → 3.3 | □ |  |
| 60 | Have the responsibilities for this been clarified? | → 3.3 | □ |  |
| 61 | Have any possible external service providers also been included in this and have they been assigned acceptance of responsibilities? | → 3.3 | □ |  |
|  | 3.4 Defined follow-up actions |  |  |  |
| 62 | Have the reactions to an error notification from the customer been discussed and the measurement methods and organisational units for remedying by the supplier been defined? How does escalation work? | → 3.4 | □ |  |
| 63 | Have the mutual obligations to recover the contractual state been agreed? | → 3.4 | □ |  |

## Download as PDF

Overview:
http://saas.clusterwien.at/5560579.0

Checklist:
http://saas.clusterwien.at/5560582.0

List of questions:
http://saas.clusterwien.at/5560585.0

Complete guide:
http://saas.clusterwien.at/5560576.0

The second enhanced edition of the German guide „Software as a Service – Correct Conclusion of Contracts" is based on the Austrian Legal System and translated to English. This translation is oriented in both languages at both applied terminologies; however, one should take care at use, that behind the translated words are different legal systems. Therefore, it is impossible that these words or terms cover the same meaning in both languages. Moreover, they differ in the content of meaning in the same way as the used constructions of both legal systems. Admittedly, the results of interpretation in both legal systems could be very similar. However, for each single case the result could be very different and could lead to significant disadvantages for one party. Therefore, the choice of the legal system has effects that are more practical then a person of less juridical understanding expects in general. Unnecessary and ill-considered compliance could paralyse the legal department and company lawyer and legal knowledge have to be obtained in an expensive and complicated way from external sources. The choice of the legal system is only unimportant if the power difference between the contract parties is so enormous that the content of the contract has less meaning.

It is a wide spread fallacy that a jurist who has to assess a case according to a foreign legal system, he only has to look up in an other book or if needed in a dictionary. Additionally in English speaking nations, one has to consider that they have not only one but many different legal systems and terminologies. The more concrete a legal expression is the rougher the translation is in the strange legal terminology. The available translation of the German juridical text into English could and should offer only a general orientation. Otherwise, the remarks of the translator grow to a malice tumour of footnotes.

Legal notice:
Produced by the working group ″General conditions for Cloud Computing″
managed by Paul Meinl

Text:
Eike Wolf, Prof. Dr. Gunter Ertl and Paul Meinl

In collaboration with:
Helmut Maschek, Peter Ranisch, Dr. Ulrich Schönbaumsfeld, Rüdiger Schultz, Günter Wildmann

This publication has been made possible as a result of the intensive collaboration of the IT Cluster with several partner companies. Special thanks go to factline Webservices GmbH and Paul Meinl for the group management. The work also received significant support from the Austrian Computer Society (OCG) and the Data Processing Work Group (ADV).

For reasons of legibility, only the male form of address is used in this guide. All personal statements of course always apply to men and women in equal measure. Regrettably the male designation also reflects to a large extent the current state of affairs within the (Austrian) IT landscape, a fact attested to by the members making up our work group.

This guide was created in good faith and with great care and diligence. Nevertheless, ″Wirtschaftsagentur Wien″ assumes no liability for the completeness or correctness of information contained therein. Any compensation, warranty and/or liability claims made against ″Wirtschaftsagentur Wien″, regardless of type, caused by the application or usage of information provided or through the use of incorrect or incomplete information are therefore excluded in full. Despite all the care taken, the information is solely for non-binding general use and does not supersede any exhaustive individual consultation. The second enhanced edition of the German guide ″Software as a Service – Correct Conclusion of Contracts″ is based on the Austrian Legal System (Status 31.03.2012).

Design: November Design & PR GmbH, www.november.at
Print: gugler cross media
April 2012

Your opinion is important to us. Please send your emails to itcluster@wirtschaftsagentur.at.
″IT Cluster Vienna″ is a service from ″Wirtschaftsagentur Wien. Ein Fonds der Stadt Wien.″, short ″Wirtschaftsagentur Wien″.

Visit us online at:

http://saas.clusterwien.at

You will find here (mainly in German language):

- The updated version of the whole guide
- Useful contract negotiation aids ready for download
- Further information
- The opportunity to take part in a professional forum.

IT Cluster Vienna:
www.clusterwien.at/it

StaDt Wien
Wien ist anders.

EUROPÄISCHE UNION
Europäischer Fonds
für regionale Entwicklung
Mit Europa für Wien

eu.Wien.at