EuroCloud
TRUSTED DIGITAL COMPETENCE PLATFORM

CLOUD COMPUTING & ENTERPRISE MOBILITY MANAGEMENT



Market, products and technical approaches;
relevant organisational and legal aspects

PROVIDED BY EUROCLOUD
CLOUD KNOW HOW
knowhow.eurocloud.org
TRUSTED DIGITAL COMPETENCE PLATFORM

09

EuroCloud Europe a.s.b.l.
L1013 Luxembourg
7, Rue Alcide de Gasperi. Luxembourg

E-Mail: contact@eurocloud.org
Web: https://.eurocloud.org
Copyright: EuroCloud Europe 2016



FOREWORD



Almost exactly three years ago, EuroCloud published the first Mobility & Cloud handbook – only a few years after the first iPad was introduced. As usual, Steve Jobs knew before anyone else what functionality many people would appreciate. And although this new type of device was initially criticised and even ridiculed, with many finding it difficult to imagine what such a device could be good for, we are now buying more of these practical little gadgets than we are PCs or laptops. Despite their small size, consumers have now come to expect convenience and ease of use combined with high performance for professional and personal use from tablets.

Indeed, the distinction between occupational and private use of devices is becoming more and more blurred – which simultaneously means that the associated technical, organisational and legal challenges are becoming ever more complex.

This handbook covers all topics relevant to mobile computing (technology, legislation, organisation and processes) and provides checklists and procedure models as well as a market overview.

This "Enterprise Mobility Management" handbook was compiled by the following authors: Reinhard Travniček, Gerald Haidvogl and Christoph Lang-Muhr (technology), Árpád Geréd (legal aspects), and Tobias Höllwarth (organisation and processes).

If you are considering an Enterprise Mobility project for your company, we would be happy to welcome you at one of our introductory planning workshops.

Dr. Tobias Höllwarth
Vienna, May 2016



TABLE OF CONTENTS

1 INTRODUCTION 5
2 MARKET OVERVIEW 6
3 DETERMINING REQUIREMENTS 10
4 MDM AND MAM: PRACTICAL IMPLEMENTATION AND FUNCTIONALITY 11
5 ORGANISATIONAL MEASURES 20
6 LEGAL ASPECTS 24
7 VENDOR LISTING – MANAGEMENT PRODUCTS 29
8 VENDOR LISTING – MIM AND EFSS 32
9 GLOSSARY 34
10 STARAUDIT 37
11 CLOUD COMPUTING GLOSSARY 42
12 LEGAL NOTES 48
13 AUTORS 50



1 INTRODUCTION

The previous edition of this mobility handbook stated that there were seven billion people in the world in 2012, and six billion mobile phone contracts. By comparison, there were less than two billion credit card contracts at that time. By the year 2015, the number of mobile phone contracts had grown to seven billion.[1]

These numbers clearly show that the market for mobile devices is growing. Modern employees often have not just a mobile phone with which they can call and text, but a smartphone that provides them with access to a plethora of company data and services on the go. And for more substantial work, a tablet PC is often used in addition. 47 percent of these devices are equipped with mobile broadband Internet access,[2] which once again shows how essential the mobile world has become.

For this reason, most businesses have come to understand the need for management solutions for devices and data, subsumed under the term Enterprise Mobility Management (EMM).

1 - http://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2015.pdf
2 - http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

2 MARKET OVERVIEW

2.1 THE PROVIDERS

According to Gartner, the significant players in the market have not changed much in the past few years. What has changed is ownership: Good Technology was acquired by BlackBerry, for example, and AirWatch by VMware.



Fig 1: © Gartner, May 2015

None of the companies in the leader quadrant see themselves as MDM/MAM manufacturers with a narrow product focus anymore. Rather, many of them have begun to diversify into important areas of EMM – like file sharing and synchronisation (EFSS) or content management – through development or acquisition. After all, customers are no longer looking for the functions categorised under the term MDM/MAM alone. A detailed market analysis can be found in "Enterprise Mobility Management Smackdown" by consultants PQR.[3]

For more MxM acronyms, please see the glossary at the end of this handbook.

Many manufacturers have only recently begun to enter the important fields of file sharing/synchronisation and content management through development or acquisition.

3 - http://www.pqr.com/downloadfiles/Whitepaper_EMM_smackdown.pdf



2.2 PRODUCT VARIANTS

Until fairly recently, one of the pivotal questions was which of the available mobile platforms would support a particular mobile management solution – and to what degree. In the meantime, however, the number of business-relevant mobile operating systems has decreased: according to surveys, almost 90 percent of all mobile end devices in companies are now equipped with iOS or Android. The dominant approach in the market is currently MDM, which mostly represents a continuation of the laptop operating model for different end devices and with different tools. The main concerns seem to be configuring the respective devices, installing desired software, creating an inventory, enforcing security policies, and being able to take appropriate measures in case of loss or theft.

The mobile operating systems relevant to business applications are iOS and Android.

The most common approach is currently MDM – basically a continuation of the laptop model for different end devices.

The individual choice of an MDM solution is often based on the security requirements of the respective institution. Virtualisation implementations featuring a strict separation between private and professional operating system on a single device, such as those offered by VMware for Android, are particularly interesting for insurance companies, banks or military applications.

Classic agent-based MDM systems represent the majority of solutions currently in use throughout the market. Depending on the operating system, they offer adequate (Android) to very good (iOS) security features.



Fig. 2: Device life cycle in classic MDM

While the MDM approach is well-suited to CODs (Company-owned Devices), employees will likely not be willing to abandon full control over their own end devices in the BYOD (Bring Your Own Device) segment.

For this reason, approaches known as MAM (Mobile Application Management) are seeing increasing use on the market. MAM solutions – for which Good Technology was a pioneer – are usually agent-less systems (and thus well-suited to BYOD) with a focus on the application and data levels; they generally lack functionality in regard to inventorying and helpdesk services, however.

What questions transcending the classic device management approach can be answered by MAM?

Employees are unwilling to abandon control over their own mobile end device – this is the setting for MAM.

Question	Product choice significance - if YES:
Are you worried that company data are not safe on a mobile device?	Distribute company data only to secure data containers.
Do you want to protect email attachments without using a separate company email application on mobile devices?	Encrypt the attachments prior to sending them to the mobile device so that they can only be opened by the authorized MDM client on the specific device.
Do some of your applications require access to the company LAN and do you consider full-fledged VPN embedment to be too risky?	Choose a product that supports app-specific VPNs. This means that a VPN connection is established only between your company network and the specific application, not with the entire device.
Do you require an application portal for your users to choose applications they want or need?	Choose a product featuring a portal and provisioning function.
Should intranet pages be externally accessible on mobile devices?	Choose a product that includes its own web browser.
Do you require an application portal for your users to choose applications they want or need?	Choose a product featuring a portal and provisioning function.

A further factor in deciding which mobile management product (MAM or MDM) is the “right” one



should always be whether existing infrastructure like Citrix, Microsoft or Symantec is compatible with the potential new system.

2.3 REQUIRED FUNCTIONALITY

The features required in a mobile management product can be separated into six categories:

2.3.1 CATEGORISATION INTO SIX FUNCTION GROUPS:

Mobile Security Management: passwords, lock screens, remote deleting, local data encryption, virus scanner.

Mobile Software Management: private app store, OS updates and patching, backup and restore functions.

Mobile Information Management: data synchronisation and backup, file sharing, data distribution to user groups, rights management in applications.

Policy: enforcement and compliance: recognition of "rooted" or "jailbroken" devices, separation of personal from company data, observation of encryption rules, passwords and lock screens, SIM card change.

Analytics: dashboard views, various reports, analysis of application usage, documentation of access rights.

Scalability: deals with the number of manageable devices, high availability, and the way in which the system is restarted in the case of disastrous failure.

3 DETERMINING REQUIREMENTS

More than ever before, it is necessary for mobile devices to be properly integrated within a company. The increasing number of devices and device types is making it more and more difficult to correctly configure individual devices and ensure that nobody is skirting policies – as a matter of fact, it is not realistically possible even for small numbers of devices.

In the ideal case, the administrator does not need to do anything more once the required policies and basic device configurations have been defined. The user "unrolls" the device himself, it is automatically integrated into the company infrastructure and the policies are applied. Examples for these automated processes are the configuration of email accounts, the security levels for encryption, or blacklists and whitelists for applications. Scanning by the obligatory antivirus application – especially on Android devices – is another example for essential policies.

In the previous edition, we mentioned that the more devices an enterprise uses, the earlier an investment into an MDM or MAM system pays off. This statement still holds true. We would also like to mention, however, that current MAM systems are able to generate significant additional value for companies: Employees are more flexible and can react more quickly, for example by opening a link included in an email directly on the smartphone since the MAM service can establish a VPN tunnel to the company intranet. This allows changes to be made to presentations easily on the go or sales staff to access up-to-date statistics, to name just two examples.



4 MDM AND MAM: PRACTICAL IMPLEMENTATION AND FUNCTIONALITY

4.1 PURE MDM, PURE MAM, OR MDM + MAM?

This is a very common question, and the answer depends on the administrator's opinions on the topics of security, maintenance and support, as well as on ownership of the actual end devices. In general, it is safe to say that companies giving out mobile devices to their employees will likely want to, or have to, take full responsibility and control over those devices. This usually makes an MDM solution the best choice in such cases. Businesses that wish to support COPE (Company-Owned – Personally-Enabled) or BYOD solutions will generally only require control over company data, emails and access to the company network. Their focus will therefore be on data leak prevention and application management, functions provided in MAM solutions by most manufacturers.

If COPE or BYOD are supported, the emphasis will be on data leak protection and application management.

4.2 ON-PREMISE OR AS A CLOUD SERVICE, INSTALLATION OR APPLIANCE?

So, which variant is best suited to your needs? There is no straightforward answer, as many factors come into play to determine your requirements. For example, companies that operate their IT on-site will likely prefer to have their mobile management implemented locally as well. Besides installation costs, this also entails operating costs for servers, power supply, cooling, personnel, etc.). An appliance solution generally reduces base installation costs and, to a lesser degree, operating and support costs as well. Cloud variants offer greater flexibility, especially for small businesses, to establish an initial setup quickly and inexpensively. Finally, hybrid systems – which leave certain elements like email or access filtering within the corporate network – should also be mentioned.

4.3 THE DRAWBACKS OF ANDROID

The advantage of Android devices in the eyes of many users is the large number of different types available. Precisely this variety can become a problem for the administrator, however: there are several versions of Android with significant disparities between them, and the issue is compounded by the myriad device-specific configurations implemented by manufacturers. This multiplicity of configurations heavily restricts the administrator's possibilities. Some manufacturers offer proprietary APIs to provide the MDM/MAM suppliers with additional options. This means, for example, that Exchange accounts can be configured on some Android devices only if a separate license for special email accounts is purchased. Older Android

versions do not support encryption. The ideal solution for these problems would be to limit the use of Android products within a company to a particular version by a particular manufacturer. This is not always possible in practice, however; a system designed with the multitude of Android variants in mind should therefore be chosen to provide more safety and flexibility. Solutions exist that check which version of Android is installed on a specific device and make the correct configurations according to predefined policies.

4.4 LICENSE TYPES

Manufacturers generally differentiate between perpetual (purchase) and subscription licenses. Either users or end devices can be licensed. For businesses whose users operate more than one device (e.g. smartphone and tablet), user licensing is usually more economical. Companies with high employee turnover rates should generally choose a device license model. Some suppliers, including some of the well-known ones, even offer freeware solutions with limited functionality, user or device contingents.

4.5 REQUIRED INFRASTRUCTURE

The infrastructure requirements depend upon the chosen installation variant. On-premise installations generally consist of the actual MDM/MAM server and a database. The MDM/MAM server is usually placed in the DMZ (Demilitarized Zone) in order to facilitate communication with the end devices. The database server, on the other hand, should always be located within the corporate LAN in order to meet security requirements.

A cloud installation will require fewer components; in the simplest case, nothing needs to be installed within the corporate network, and all functionality is provided via the cloud. Businesses should make sure that the connection to the cloud MDM/MAM service is appropriately secure and that all transmissions are encrypted. Most manufacturers offer various possibilities to do so, with SSL encryption being the most common method. VPN solutions are used less frequently. Many enterprises do not want their email data stored in the cloud; a hybrid system is often the best solution for such requirements. In such a setup, a filter mechanism that receives relevant parameters (which devices are compliant and which are not, who must be blocked, who must be cleared) from the MDM/MAM server in the cloud – and then enforces those parameters locally – is integrated into the corporate systems as a plug-in. Thus the system only communicates with the cloud server to obtain configuration information, while all other data and communication remains internal.

This type of filter mechanism is usually implemented as a proxy to the corporate email system,



and therefore often entails the use of an additional server or gateway system.

Besides the required infrastructure, appropriate ports need to be configured in the firewall so that the MDM/MAM components can provide their functionality. Once again, the systems available on the market differ from each other significantly in this regard: some require only a few ports to be opened, while others need more.

4.6 FURTHER REQUIREMENTS

4.6.1 CERTIFICATES AND PKI

All MDM products and most MAM products must be integrated into a certificate infrastructure so that appropriate access certificates can be distributed to the mobile end devices. Several public web server certificates are usually required to secure the access points towards the outside.

4.6.2 APPLE DEVELOPER ENTERPRISE

MAM products generally encase applications in a so-called "wrapper" managed by the MAM. This avoids the need for applications to be reprogrammed for every MAM solution. This wrapping process usually requires an Apple operating system (Mac OS) and an Apple Developer Enterprise Account – even for Android apps, which are likewise wrapped using this setup.

4.6.3 APPLE ID

Devices using iOS 5 and up can be activated without an Apple ID. Because users have to install an appropriate client available only from the App Store for many MDM/MAM systems, however, Apple IDs are currently still required in most cases. If a device can be integrated without a client, the administrator can push apps installed locally on the MDM/MAM server to the device. For apps that need to be installed from the App Store, however (via an installation link or a "suggestion" link sent to the device), users must have an Apple ID in order to access the store and get the app.

The same applies to the administrator: Most MDM/MAM systems use APNS (Apple Push Notification Services) to prompt the device to communicate with the MDM/MAM server. In order to use this service, the MDM/MAM server requires an APNS certificate which can only be obtained with a valid Apple ID. It is highly recommended to create a separate Apple ID for the server instead of using the administrator's personal Apple ID so that nothing has to be changed if the administrator leaves the company.

The VPP (Volume Purchase Program) licenses, which provide businesses with the option of purchasing licenses for apps and making them available to their employees, would solve the Apple ID problem very elegantly. Unfortunately, this service is not yet available everywhere in Europe, and Apple has hitherto provided no information on when they plan to expand the program's coverage.

4.6.4 GOOGLE ID

Just like with Apple devices, a Google account is not required to activate an Android device. If a user wants to access the Play Store, however, he or she must have a Google ID. The same principle as above applies: The administrator can install applications from the MDM/MAM server, but if a link to the Google Play Store is involved, the user must have a valid Google account to get the corresponding app.

4.7 MOBILE INFORMATION MANAGEMENT (MIM)

Besides email, contacts and appointments, files will be the resource used most frequently by employees. Mobile file sharing is easily achievable for enterprises these days, with many different products on offer that meet the most common requirements. Not all available solutions are capable of digital rights management (DRM) and data leak protection, however. A good enterprise file sharing product has to cooperate closely with the MDM/MAM solution in order to allow centralised management. It is important to keep in mind as well that files are not the only type of data on mobile end devices that require protection. Many apps such as Facebook and Evernote store data on the device as well, though not in the typical file format.

If such a product is used in a BYOD environment, functions like "Delete" and "Block" within the product itself are indispensable – as it will not be possible to delete or reset an entire device in a BYOD environment. Depending on data content and compliance requirements, it may be necessary for all data to be stored on-premise. Non-critical data (see Data Classification) can be stored in any cloud product without hesitation.

A good MIM product must work closely with the MDM/MAM solution to facilitate centralised management.

If users are not provided with any "official" means of file sharing, they will inevitably make use of products they can install themselves – and over which the corporate IT infrastructure has no control.

The minimum feature set of a MIM product should include:



Function	Included	Missing
Data storage location satisfies compliance rules		
Service provider observes compliance rules for certain areas, e.g. U.S. Securities and Exchange Commission, Independent Securities Regulator FINRA, or HIPAA Business Associate Agreement		
Access control		
Active Directory integration		
User groups and folder mapping		
Granular administration		
Differentiation between access by employees and access from outside		
Possibility of on-premise data storage		
Protection against data loss from synchronisation errors		
Administrator control over data on the mobile devices (wipe, lock)		
Data backup and restore at item level		
Enforcement of policies on the mobile device		
Data encryption on the mobile device		
Integrity test on the mobile device (rooted, jailbroken)		
Comprehensive (revision-secure) reporting		
Documentation of data access (type, duration, etc.)		
Reporting of access rights of individual persons		

The following features are optional, but desirable:

Function	Included	Missing
View-only document access		
Automatic time-controlled deletion		
Versioning of documents		
Recycle bin function		
Single-Sign-On		
Two-factor authentication		
Digital rights management (DRM)		
Data leak prevention		
SharePoint access		
Access to general CIFS shares		



4.8 MOBILE DEVICE SECURITY

The increasing use of mobile devices in the corporate environment naturally raises concerns about the security of the employed devices and the data stored on them. The familiar data protection goals of confidentiality, integrity and availability apply to this device class just as they do to others.

In order to achieve these goals, one must first be aware of the risk potentials associated with mobile devices, which differ significantly from the threat vectors on a Windows PC.

The danger of conventional attacks (e.g. malware) is greatly reduced due to the security mechanisms like app sandboxing integrated into the leading mobile operating systems and the MAM solution. Mobile devices are susceptible to other issues, however.

4.8.1 DEVICE LOSS

Loss or theft of devices and the sensitive data stored on them (from contacts and emails to saved passwords and files) is one of the biggest dangers associated with mobile devices.

In order to protect data stored on mobile devices, an access lock/screen lock using a PIN or password is indispensable. Furthermore, all sensitive data on the device must be encrypted to prevent extraction by means of forensic tools or hackers. These two measures protect data immediately after the loss or theft of a device. To keep the time period available for potential attacks to a minimum, any lost or stolen device should be cleared as quickly as possible via a "remote wipe", thus making it useless to the attacker.

Most EMM solutions offer one or both of the following remote wipe options:

1. Enterprise Wipe – only sensitive corporate data are deleted.

This variant of remote deletion is sensible for BYOD scenarios, since no private data belonging to the employee or former employee are deleted.

2. Device Wipe – all data on the device are deleted, and it can even be made completely inoperative, preventing any future use (depending on the operating system).

4.8.2 DATA LEAKAGE

Data leakage/data loss through the use of cloud services like Dropbox, Google Drive, Apple iCloud or Microsoft OneDrive.

The often very deep integration of these services with operating systems can make it difficult to control data flow to them. The storage of data in popular cloud services is firmly in the hands of U.S.-based companies, and European data protection laws therefore apply only within limits. By employing of an EMM system, these apps can be deactivated or their use restricted. Newer EFSS systems support digital rights management and DLP systems.

4.8.3 MANIPULATION OF DEVICES

Device manipulations like rooting or jailbreaking (i.e. gaining administrator privileges) can compromise the implemented security mechanisms and in worst cases make the device accessible to malware.

Furthermore, EMM policies can no longer be reliably rolled out to such manipulated devices. EMM systems therefore generally include a jailbreak and root detection mechanism that excludes such devices from the corporate network once recognized.

4.8.4 MALICIOUS SOFTWARE

A further danger is the installation of apps from non-authorized sources instead of from the manufacturer app stores. The official stores operated e.g. by Apple, Google, Amazon or Microsoft check apps for damaging code prior to publishing. This sort of verification usually does not occur on third-party app stores, however (e.g. Android – Galaxy Apps, F-Droid or Slide ME). These stores may or may not feature reliable security checks and should therefore not be used.

Malicious apps can also come in the shape of freeware like screensavers, games, etc. that tap sensitive data on the device in the background and send them to the app manufacturer. Such apps can be recognized by the permissions that they request during installation, e.g. access to the address book, location data, etc. Users should always be aware that free apps are usually not actually free, but instead paid for with the user's data.

4.8.5 ALWAYS-ON CONNECTIVITY

Mobile devices are permanently online and exchange data via frequently insecure connections, like Wi-Fi hotspots without encryption. These data transfers are susceptible to a variety of attacks which can intercept or tamper with the transmitted data, e.g. man-in-the-middle attacks. Therefore, an additional security layer like a VPN or SSL encryption should be employed for such unprotected networks and connections.



4.8.6 PHISHING

This form of attack is currently experiencing a renaissance on mobile devices because the small displays and mobile web browsers and email clients make it more difficult to discern manipulated or fake websites from their official counterparts.

4.8.7 MISSING UPDATES

Depending on the manufacturer of a device, updates and security fixes are rolled out at different times; support for older devices can also be discontinued without warning. This requires the EMM solution to recognize outdated or unpatched devices and isolate them from the corporate network, and ideally reintegrate them once they fulfil the compliance rules.

5 ORGANISATIONAL MEASURES

Besides the obvious need to determine the technically optimal solution for an EMM system, the planning and implementation of such a system should also always take into consideration the legal (see next chapter) and organisational measures and implications. In order for Enterprise Mobility to work flawlessly and with as few manual interventions as possible, the following questions should be addressed in due course between the affected parties and answered authoritatively.

5.1 DISTRIBUTION AND MAINTENANCE OF DEVICES

Most users of mobile devices are used to handling the purchase, configuration, maintenance, repair, replacement and security of their devices themselves. For CODs (Company-owned Devices), this responsibility generally lay with the corporate IT department, and users only needed to adhere to the agreed terms of use. The more complex usage scenarios of BYOD or COD with private use likewise require the introduction of clear and comprehensible procedures and rules.

Clear procedures for device request, approval, issuing, repairs, changes, return, and loss.

This applies in particular to questions of backing up of private data and the procedures relating to updates that might have consequences for private-use-only applications.

Clear procedures for requesting, approving and issuing devices; handling device defects or failures (including data transfer and replacement devices); changes to devices; device return in case of changes to the employment contract; device accessories and device loss (particularly in foreign countries) must be established, discussed with all stakeholders, and mutually agreed upon.

5.2 HELPDESK SERVICES

Another indispensable aspect is the comprehensive definition of services to be provided by an internal or outsourced helpdesk as part of the EMM concept. These services, particularly regarding user requests and inquiries relating to problems with devices and their handling, should not be underestimated and can entail significant costs. Especially for a BYOD approach, it is vital to determine what type of service the user (who is used to receiving full support from a central source in the case of a company PC) can expect from the helpdesk. The question of what level of helpdesk comfort (e.g. remote control) to provide to users of mobile devices as compared to laptop users should also be clarified.



Especially in BYOD scenarios, it must be clear what helpdesk services users can expect.

5.3 PASSWORD RESET AND DEVICE WIPING

As in the classic PC environment, it is essential to establish a simple yet secure process for resetting passwords. Passwords are sometimes forgotten by users, need to be changed regularly, and must be reset quickly if there is suspicion of abuse. Ideally, users can reset their own passwords using a portal, thus reducing necessary helpdesk costs.

In the case of device loss, a quick and simple set of procedures must be established for the user and IT department to execute in order to prevent unauthorized access to the data on the device as much as possible. While the technical infrastructure and the device naturally must support this procedure, it is the immediate steps to be taken by the user that determine whether data loss can be prevented quickly and successfully.

A quick set of procedures must be established for execution by the user and IT department in the case of device loss.

Ideally, backups of the data on all devices are so complete and frequent that the user does not need to fear remote wiping of the device even when there is only the suspicion that it has been lost (e.g. user cannot find their device). This also requires the restoring of data to the device (if it is found again) or its replacement to be a quick and uncomplicated process.

5.4 FLEXIBLE WORKING HOURS

Despite their obvious advantages, permanent reachability and uninterrupted access to data and emails are also increasingly becoming a burden for people everywhere. This is especially true when flexible working hours are taken to the extreme, with weekends and vacations suffering from permanent reminders of a person's work life. There are many organisational and technical measures that can be applied here, some of which can have significant consequences for certain businesses (e.g. no email delivery on weekends, email deletion or automatic forwarding during vacation). Obviously, an acceptable balance must be found depending on responsibility, urgency, and industry sector, and this balance can only be found and implemented in close coordination between all stakeholders.

Mobility as a burden.

5.5 DATA CLASSIFICATION

One of the most complex organisational and technical challenges is the classification of data and the respective security requirements. Obviously, general and publicly accessible product data, price lists, etc. do not require the same level of protection (internally as well as on the mobile end device) as technical or other classified product information, customer data or internal calculations. Only if a comprehensible data classification scheme and associated designations have been established can technical systems as well as users adhere to a systematics requiring different handling and storage spaces depending on the respective data class. It should be kept in mind that such a classification can be an elaborate and lengthy process, and that excessive complexity may result in the affected users – or even the technical systems – being unable to properly comply with the scheme. An onion layer model (lowest protection requirement on the outside, highest security level on the inside) can help to illustrate the differentiation of data in an understandable fashion.

An onion layer model can help to make a data classification scheme more easily understandable.

5.6 TRAINING COURSES

While the statement "Everyone has to learn to protect themselves" is principally correct, it should realistically read "Everyone needs help to learn to protect themselves." The implementation of a repeatable and expandable training concept for all users is of pivotal importance. A training plan featuring a series of courses, information material and individual briefings helps to create a natural awareness regarding the allowed and possible uses of devices and applications among employees. The goal of such a program should be to establish a healthy balance between the possible risks of an Enterprise Mobility concept on the one hand, and its many benefits and potentials on the other.

Everyone needs help to learn to protect themselves.

5.7 BALANCING VARIOUS DIFFERING INTERESTS

In order to ensure that an Enterprise Mobility Concept can be successfully implemented in the long term, it is important to seek – starting in the earliest planning stages – a balance between the different vested interests that is accepted and supported by all stakeholders. This applies particularly to aspects of the required protection of corporate and personal data versus day-to-day usability and convenience of the employed devices. A requirement of complete device encryption, for example, will usually entail the use of complex passwords on smartphone lock screens, which in turn may uncomfortably impede everyday use of the telephone.



5.8 REVIEW OF ORGANISATIONAL RULES AND PROCESSES

Review and corresponding adaptation of organisational concepts and procedures should be an ongoing process. It is recommended, however, to schedule mandatory reviews including all stakeholders after three and twelve months.

Schedule mandatory reviews including all stakeholders.

6 LEGAL ASPECTS

6.1 POINT OF DEPARTURE

Although the topic of MDM is not entirely new in a legal sense, the BYOD concept in particular creates novel challenges. While the first legal aspect that comes to mind is usually "data protection", data protection laws are in fact only of secondary importance in the field of Enterprise Mobility. Labour law is far more significantly affected.

Although no specific regulations concerning EMM exist in current labour law, there are several basic principles which provide orientation for answering certain questions.

The most important of these are the fiduciary duties legally imposed on the employer and employee respectively. In short, these rules mandate fair and considerate interaction between employer and employee as well as mutual respect for and observation of each other's interests. The focus of the employer's fiduciary duties lies on the personal rights of the employee, while the employee's duties mostly regard the economic interests of the employer.

Legal regulations mandate fair and considerate interaction between employer and employee as well as mutual respect for and observation of each other's interests.

Regulations and court rulings based on these principles exist in regard to the use of devices – and communication systems like telephones and the Internet in particular – provided by the employer. In general, the employer may not completely forbid all private use of such provided infrastructure, e.g. private telephone calls or reading private emails during working hours. On the other hand, the employee is required to limit private use to a minimum, with failure to do so constituting grounds for dismissal under certain circumstances.

Hence companies travel relatively well-established paths in regard to COD even with mobile devices. It is nevertheless essential for employees to be comprehensively informed about their rights and duties, preferably in writing, and that those rights and duties are compliant with all applicable laws and regulations (which cannot be discussed in detail here).

6.1.1 PARTICULARITIES RELATING TO BYOD

Different conditions apply to private devices used by employees for business purposes, for while devices provided by the employer are to be used primarily for business (and employers are therefore legally entitled to restrict employee's usage rights through technical measures), private devices are primarily intended for private, non-business use.



Therefore, the employer must ensure that such devices can be used for private purposes, especially outside of normal working hours. There is currently no clear legislation on whether maintaining certain restrictions in regard to the possibility of installing applications is permissible under such conditions, however. The best course of action at this time is certainly to clarify from the outset the needs of employer and employees, which can differ greatly from setting to setting and company to company, in order to avoid possible conflicts later on.

The employer must ensure that privately-owned devices can be used for private purposes, especially outside of normal working hours.

It is likewise important to keep in mind that in BYOD settings, the respective company will always be handling private data of its employees as well. Whether these data are "personal data" as governed by data protection laws, i.e. whether they can be correlated to a particular individual, makes no difference in this regard. Special care must therefore be taken to ensure that these data are properly protected and can be restored in case of loss. It is recommended to design backup and restore systems in such a way that individual data (e.g. photos or texts) cannot be viewed.

Data protection laws can indeed become relevant in this circumstance, however, particularly in terms of handling if the data represent "personal data" as defined by applicable data protection laws. This is because these laws not only govern the ways in which personal data may legally be acquired and used, but also stipulate that such data must be corrected or deleted at the request of the individual to whom they refer.

If the private use of mobile devices is allowed and the company conducts backup procedures incorporating all mobile data, the situation can thus arise that the company possesses backups of private files and data which may already have been deleted elsewhere, or which belong to former employees. In order to avoid such situations and their potential consequences, it is therefore advisable to take appropriate technical and/or organisational precautions: for example, corporate data can be backed up separately to allow private data to be easily deleted. In organisational terms, employees can be instructed to transfer corporate data and files from their mobile device to the appropriate permanent storage systems at regular intervals so that the personal mobile devices can be reset or wiped without data loss.

6.1.2 PARTICULARITIES IN REGARD TO CLOUD SERVICES

If cloud services are used, it is important to make sure that the employed service and its provider comply with company-internal regulations and policies. This applies in particular to backups of private data in the cloud.

In the course of the initial implementation of cloud-based MDM/MAM, the basic technical and legal conditions should therefore be discussed with the cloud service provider at an early stage. When migrating an existing MDM/MAM solution into the cloud, the technical and legal compatibility as well as possibly required adaptations to existing company policies and regulations should be analysed.

When migrating an existing MDM/MAM solution into the cloud, adaptations to existing company policies and regulations may be required.

Compliance with these company-internal regulations as well as any ancillary duties of the cloud service provider and its restrictions in regard to private data (depending on the scope of the service and the required access possibilities) should be contractually agreed between the service provider and recipient, i.e. the company.

Furthermore, compliance with data protection laws should be verified separately in such cloud configurations, as they commonly entail the passing on of personal data in the legal sense to a third party, i.e. the cloud service provider. This requires, among other measures, the conclusion of an appropriate data protection agreement. The relevant data protection authorities provide sample agreements for such purposes, thus keeping the required additional effort to a minimum

6.2 DATA DELETION

If a device is lost or a user leaves the company, it is essential for the employer to be able to quickly and completely delete all data stored on the device.

COD poses no new challenges in this case. So long as it is agreed that no private data may be stored on the device, complete device wipe is legally permissible – as is the withdrawal of the device from the user.

It is not permissible, however, to demand that a user turn over a private device used within the corporate infrastructure. In regard to deletion, the rights and duties agreed between the company and the user are the determining factor. These can include an obligation for the employer to regularly back up his or her private data as long as such backups are technically possible. If such an obligation is not agreed upon, the employer – if he wishes to be able to wipe the device completely – is responsible for creating regular and timely backups of the user's personal data as well.

Restricting mobile device usage to models which allow several user accounts to be maintained in parallel (e.g. BlackBerry 10 or Android from version

Under certain circumstances, the employer can be responsible for backing up private data as well as corporate data.



4.2 upwards) is advantageous in such situations.

6.3 REMUNERATION FOR MOBILE WORK OUTSIDE OF CORE TIME

Although extra working hours and overtime have to be authorized by the employer ahead of time in principle, the practical implementation of this rule is at best difficult in a mobile working environment.

There are various approaches to this issue: flexible working hours, pre-approved contingents of extra hours and overtime hours, a general ban on mobile work during weekends or vacations, etc. There is no single solution that works equally well for every company, however.

It is therefore important for the employer to analyse which solution is the optimal one for his needs, and to come to a legally binding agreement with his employees prior to the introduction of the MDM/MAM solution.

A legally binding agreement governing mobile work outside of core time is essential.

6.4 INVOLVEMENT OF A WORKERS' COUNCIL

Aside from legal requirements regarding approval by the workers' council for the introduction of certain technical systems (for control measures according to ArbVG § 96 Section 1 Line 3), the involvement of an existing workers' council beyond the legal requirements can be advantageous for COD as well as BYOD configurations.

For example, technical freedoms and restrictions for the use of mobile end devices, as well as rules for their business-related usage outside of working hours, can be discussed with representatives of the workers' council. It is advisable to develop a concept as a basis for discussion prior to consulting the council, however.

Even if the coordinated requirements cannot be cast into a binding company-wide agreement, the support of an existing workers' council for the introduction and implementation of the required measures can prove invaluable.

6.5 CHECKLIST

- COD, BYOD or both?
- Should BYOD be restricted to certain devices?
- Should the use of mobile devices be restricted to certain persons or groups of persons?
- What usage options and/or restrictions should there be?

- How should backups be handled, and who should execute them?
- Is at least the regular deletion of backups of private data ensured?
- How should such deletion occur?
- Should external providers (e.g. cloud service providers) be involved?
- If yes: Are the duties of these providers agreed upon in accordance with applicable laws?
- Was the workers' council consulted?
- Have the conditions for use been agreed upon with the employees in writing and in accordance with applicable laws?
- Have the conditions for use outside of core time been agreed upon with the employees in writing and in accordance with applicable laws?



7 VENDOR LISTING – MANAGEMENT PRODUCTS

Manufacturer	Product	Website
7P	7P MDM	www.7p-group.com/enterprise-mobility/seven-principles/
Absolut Software	Absolut Management	http://www.absolutemanage.com/en/manage/mdm
AirWatch	AirWatch	www.air-watch.com/de
Alcatel	Motive Device Management	www.alcatel-lucent.com/solutions/device-management
Amtel	Mobile Device Security	www.amtelnet.com
Apperian	Mobile Application Management	www.apperian.com/mobile-application-management-platform/mobile-application-management/
Baramundi	Mobile Device Management	www.baramundi.de/loesungen/mobile-device-management
Capricode	SyncShield	www.capricode.com/
CA Technologies	XenMobile MDM	www.citrix.de/products/xenmobile-mdm/overview.html
Cortado	Workplace	corporateserver.cortado.com/de-de/
Dell	Mobility Software	www.dell.com/us/business/p/enterprise-mobility-management?~ck=anav

Manufacturer	Product	Website
equinux	Tarmac Mobile Device Management	www.tower-one.net/de/
Excitor	EMM	www.excitor.com/enterprise-mobility-management
FancyFon Software	Famoc	www.fancyfon.com/
Good Technologie	Mobile Device Management	www.good.com
Kaseya	Mobile Device Management	www.kaseya.com/products/enterprise-mobility-management
LANDesk	Management Suite	www.landesk.com/products/mobility-manager.aspx
Matrix42	Mobile Device Management	www.matrix42.com/de/produkte/matrix42-mobile-apps/
Microsoft	Enterprise Mobility	www.microsoft.com/en-us/server-cloud/enterprise-mobility/overview.aspx
Microsoft	Intune	www.microsoft.com/en-us/windows/windowsintune/explore.aspx
Microsoft	Office 365	Mobile Device Management for Office 365
Mobile Active Defense	Mobile Enterprise/ Security Server	www.mobileactivedefense.com/
MobileIron	Mobile Device Management	www.mobileiron.com/en/solutions
OpenPeak		www.openpeak.com/mdm.php



Manufacturer	Product	Website
Relution	Enterprise Mobility Platform	www.relution.io/de/
RIM	Blackberry	de.blackberry.com/enterprise/solutions/emm.html
SAP		go.sap.com/germany/solution/platform-technology/enterprise-mobility-management.html
Sophos	Mobile Control	www.sophos.com/de-de/products/mobile.aspx
SOTI	MobiControl	www.soti.net/solutions/enterprise-mobility-management/
Symantec	Mobile Management	www.symantec.com/mobile-device-management
Tangoe	Matrix	www.tangoe.com/products-services/managed-mobility-services-matrixmobile/enterprise-mobility-management/
Trend Micro	Mobile Security	www.trendmicro.de/produkte/mobile-security/index.html
universit		universitplatform.com/
Wavelink	Avalanche	www.wavelink.com/products/avalanche/

8 VENDOR LISTING – MIM AND EFSS

Manufacturer	Product	Website
Accellion		www.accellion.com/solutions/online-file-sharing/file-sync
AirWatch		www.air-watch.com/solutions/mobile-content-management
Amazon	Amazon Cloud Drive	www.amazon.de/clouddrive/home
Apple	iCloud	www.icloud.com
Appsense	DATANOW	www.appsense.com/products/datanow
box		www.box.com
Carbonite		www.carbonite.com
Citrix	Sharefile Enterprise	www.sharefile.com/enterprise/
Cloudme		www.crashplan.com/enterprise/mobile.html
Cortado	Workplace	corporateserver.cortado.com/de-de/
CTERA		www.ctera.com/solutions/by-business-need/enterprise-file-sync-share-efss
Cubby (LogMeIn)		www.cubby.com
DROPBOX	Dropbox for Business	www.dropbox.com/business
EGNYTE		www.egnyte.com
EMC	Syncplicity	www.syncplicity.com



Manufacturer	Product	Website
Excitor	Excitor DME™ File Browser	www.excitor.com
Google	Google Drive	drive.google.com
Hightail	Yousendit	www.hightail.com
Huddle		www.huddle.com
Insync	Google Drive AddOn	www.insynchq.com
JustCloud		www.livedrive.com
Microsoft	OneDrive	onedrive.live.com/about/de-at/
Microsoft	Office 365	Mobile Device Management for Office 365
Mozy	Mobil	mozy.com/mobile
OpenDrive		www.opendrive.com
OwnCloud		owncloud.com/products/enterprise
PowerFolder		www.powerfolder.com
Primadesk	Unifyle	www.unifyle.co
SpiderOak		spideroak.com
SOONR (Autotask)		www.soonr.com
SugarSync		www.sugarsync.com
TeamDrive		www.teamdrive.com
TeamPlace		www.teamplace.net/de-de/
Trend Micro	SafeSync	www.trendmicro.com/us/home/products/storage-backup/safesync
Unwired Revolution	DocLink	www.unwiredrevolution.com/products/

9 GLOSSARY

Abbreviation	Full term	Explanation
Agent	Agent	Software component that needs to be installed on a mobile device in order to allow management of certain functions.
Android	Android	Smartphone operating system by Google
BYOA	Bring Your Own Application	Employees are permitted to use applications of their choice for business purposes so long as they conform to predetermined license, security and data compatibility requirements.
BYOD	Bring Your Own Device	Employees are permitted to use private devices for business purposes. This usage variant is often promoted and supported by companies.
Cloud	Cloud	Synonym for various data or application services obtained by users from the Internet. For precise definitions, see "Cloud Migration", ISBN 978-3-8266-9261-1
COD	Company-owned Device	Devices owned by the company. Enforcement of policies and regulations is generally easier with such devices than in BYOD environments.
COPE	Company-owned – Personally Enabled	The device is owned and provided by the company, but operated entirely by the user. Basically, BYOD with the advantage that devices are restricted to certain types or models.
DLP	Data Loss Prevention	DLP is one of the measures supporting the protection of data confidentiality. "Data loss prevention" and "data leakage prevention" are generally used synonymously.
EFSS	Enterprise File Sharing and Sync	See under MFM.
EM	Executive Mobility	See under MFM.



Abbreviation	Full term	Explanation
EMM	Enterprise Mobility Management	A comprehensive approach to allowing and safeguarding the use of smartphones and tablets by employees. A strong EMM strategy not only addresses questions of security, but also supports employees in increasing their productivity. Employees are provided with the necessary tools enabling them to execute work tasks on mobile devices.
IOS	IOS	Operating system of Apple's iPhone smartphones and iPad tablets.
MAM	Mobile Application Management	Deals with software on mobile end devices. MAM supports administrators in the provision, licensing, configuration, application lifecycle management (ALM) and usage analysis of mobile applications. Many mobile application managers can also verify compliance with defined company regulations and control and/or limit the exchange of corporate data between mobile apps. An important requirement for the use of MAM software is that it gives administrators the possibility to remotely delete corporate mobile apps and/or data on users' end devices.
MDM	Mobile Device Management	Refers to the centralised management of mobile devices like smartphones, sub-notebooks, PDAs or tablet computers by one or more administrators with the help of special software. Management functions include inventorying of hardware within organisations, software and hardware distribution and data protection on all existing devices.
MFM	Mobile File Management	Refers to products that allow files to be safely stored on mobile devices, synchronised with other devices and/ or transferred to cloud storage. Not to be confused with MIM, which deals with the data content in applications like Facebook, Evernote, etc.

Abbreviation	Full term	Explanation
MIM	Mobile Information Management	Is the next step of management and goes so far as to direct applications on how to handle certain data (depending on type, source and/or content). Some existing applications already support rights management, and certain email software (iOS) can distinguish between private and business-related settings.
MMP	Mobile Management Product	Products for managing mobile devices and the data stored on them.
Mobile Device	Mobile Management Product	Smartphones, tablet computers, handheld devices (PDAs).
Off-Premise	Off-Premise	IT services which are not provided from a company-internal location are called off-premise.
On-Premise		IT services provided by the company itself from a company location or locations are called on-premise.



10 STARAUDIT

The organisation EuroCloud offers a cloud certification scheme under the name "StarAudit". The certification process is specifically geared to the areas of IaaS, PaaS and SaaS, and features defined criteria regarding various control elements which must be met to certain degrees in order to be certified as a Trusted Cloud Service Provider.

Comprehensive expertise is necessary in order to verify compliance with the individual requirements resulting from service guarantees in the areas of data security, technical operation and organisational processes. Therefore, certificates providing a compact overview of security aspects and reliability of the service provider are generally used for this purpose.

EuroCloud has developed a special quality seal subsuming the abovementioned contractual, technical and organisational requirements. For providers to be allowed to display this seal, the fundamental requirements for the provision of their cloud services must be verified by trained auditors and confirmed with a certificate. A catalogue of testing criteria was developed in close coordination with public institutions, research centres, cloud providers, legal experts and auditing organisations.

The following categories are encompassed by the StarAudit process:

- Supplier profile
- Contract and compliance
- Security
- Operation of infrastructure
- Operational processes
- Application
- Implementation

Based on a point-awarding system and the specification of minimum criteria, providers can achieve different quality levels (one to five stars).

At the core of the certification process are legal aspects, the reliable provision of technical services, data protection, data security, and compliance with basic standards for operational processes and application design. The provider is required to provide concrete evidence for its declarations in the audit and is obliged to report significant changes to frame conditions (e.g.

location of service provision, changes to subcontracting agreements) as well as critical events without delay.

The following three quality levels can be awarded depending on the degree of realization:

- Trusted Cloud Service – three stars
- Trusted Cloud Service Advanced – four stars
- Trusted Cloud Service Advanced HA (High Availability) – five stars

10.1 ONE-STAR CERTIFICATION

The provider has met the following compulsory criteria:

- The provider is registered in the EU commercial register.
- Technical operation of the application occurs within an infrastructure suitable for the provision of web-based services.
- This includes:
  - An enclosed area for the employed hardware components
  - Redundant power supplies with UPS guaranteed for at least 20 minutes
  - Redundant Internet connections
  - Access control
  - Basic area security
- The contractual agreements are compliant with the data protection requirements according to the German Federal Data Protection Act.
- Comprehensible contract termination clauses exist.
- Clear agreements regarding to customer data exist that debar any right of retention by the service provider.
- Contractual clauses exist which clearly specify data export interfaces for the return and deletion of customer data upon termination of the service agreement.

10.2 TWO-STAR CERTIFICATION

The following compulsory criteria are met in addition to the abovementioned requirements:

- The provider issues comprehensible specifications on the assured service level in regard to



availability and speed of the application. Appropriate reporting functions for verification of these service commitments exist.

- Technical operation satisfies the minimum standards of a computing centre in terms of redundant configuration of fundamental technical logistics. Area risks and building security are confirmed by provider documentation.
- The export formats for customer data are fully documented and available for migration into other environments.

10.3 THREE-STAR CERTIFICATION

The following compulsory criteria are met in addition to all abovementioned requirements:

- The customer is given the choice of national jurisdiction by the provider, or the provider offers the contract directly in accordance with the customer's national laws.
- The provider supplies comprehensive documentation and training material on the use of the service. A hotline number is available during the customer's normal working hours. Issues can be reported using an electronic ticketing system. The provider has established processes with guaranteed procedures and the required internal applications; this applies not only to the provider itself but also to its own suppliers.
- The commitments made in regard to service management and technical provision have been verified on location by trained auditors.

10.4 FOUR-STAR CERTIFICATION

The following compulsory criteria are met in addition to all abovementioned requirements:

- The technical provision satisfies the standards of a professional computing centre provider. The communication links are provided in the shape of a direct and redundantly configured Internet exchange point (IX).
- The service processes satisfy the requirements of ITIL and ISO 27001 as applicable to an ISMS (Information Security Management System).
- The security functions and applications of encryption technologies are comprehensibly documented and satisfy normal IT security requirements. Protection measures against external attacks exist and satisfy the requirements of ISO 27001 at the time of the audit.
- Direct access by administrators is restricted, and individual transaction data is anonymised against the associated user profiles. Process documentation for this mechanism exists and can be made available to the customer upon request.

- If long-term archiving of customer data in accordance with the basic principles of data access and verifiability of digital records is not implemented through other measures, the provider is responsible for the archiving and provisioning of customer data in accordance with applicable legal requirements.

10.5 FIVE-STAR CERTIFICATION

The following compulsory criteria are met in addition to all abovementioned requirements:

- The provider offers redundant provisioning of the entire scope of the service, featuring at least two separate computing centres with an availability of at least 99.99 per cent and a highly fail-safe infrastructure.
- Emergency drills are conducted regularly (at least once per year) and documented according to BS 25999.
- Penetration tests for verification of the security functions are conducted regularly (at least once per year) and documented.
- The provider offers a variable pricing model and allows switching to a generally available, lower-priced service model even during an active contract period (Best-Price Option).

10.6 STARAUDIT

The StarAudit certification scheme is a best-practice approach designed to answer the most important management questions regarding the selection of a suitable cloud service provider. In contrast to pure security or data protection certification schemes, the StarAudit scheme takes all related aspects into consideration and confirms them in a clearly comprehensible verdict. Classic certification systems will doubtless continue to develop towards cloud assessment in the future. This process may take several more years, however, and fundamental questions require answers now, especially for SMEs.

Providers displaying the following seal are certified by EuroCloud to meet the criteria listed above:





10.7 STARAUDIT.ORG

Details on StarAudit, including the precise contents of the StarAudit catalogue of criteria and the StarAudit Assessment Tools (also for use in self-assessment), are available at no cost. at https://staraudit.org.



11 CLOUD COMPUTING GLOSSARY

11.1 WHAT DOES "CLOUD COMPUTING" ACTUALLY MEAN?

"Cloud computing is a model that allows network access, at any time and from any location, to a shared pool of configurable computing resources (e.g. networks, servers, storage systems, applications and services) which can be made available quickly and with minimal management effort or limited service provider interaction."[4]

According to the NIST definition,[5] the following five features characterize a cloud service:

- On-demand self service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

4 - https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html
5 - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf



11.2 PROVISIONING AND ACQUISITION FUNCTIONS OF CLOUD SERVICES

Various possibilities for supplying and obtaining cloud computing services, and the following roles should be differentiated:

(A) PROVISION

- Cloud service provider – Company that offers the cloud services to the customer as a contract party.
- Cloud service subcontractor – Supplier of cloud services that are integrated as sub-functions in the offering of the cloud service provider.
- Cloud service subcontractor supplying technical IT services representing classic IT outsourcing (computers, storage, network) that are not acquired as a fully-fledged cloud service.
- Co-location provider – Supplier of infrastructure components providing buildings, power, cooling and communication as basic services.
- Cloud service agent – Company that solicits customers for the cloud service provider (and in legal terms functions as a commercial agent).
- Cloud service reseller – Reseller of cloud services who makes no adaptations to the cloud service, but instead adopts all aspects of the service from the cloud service provider (and in legal terms represents an authorized dealer).
- Cloud solution provider – Cloud service reseller that bundles several cloud services and sells them as an integrated package.

The term "broker" is intentionally not used here, as it is applied to several distinct but not necessarily related roles within the market, i.e. in the sense of "agent" as well as in the sense of "solution provider".

The term "marketplace" is likewise used with different meanings within the market, i.e. in the sense of "agent" or "reseller".

(B) ACQUISITION

- Cloud service customer – Contract partner of the cloud service provide wishing to use the cloud service for business purposes.
- Cloud service user – Individual user of a cloud service, usually an employee of the cloud

service customer.

- Cloud service administrator – Specialist employee of the cloud service customer in charge of managing identities and usage options of the cloud service.

Within the market, the term "broker" is also sometimes used to refer to an internal function in the IT department of the cloud service customer that provides cloud-based solutions to the cloud service users.

11.3 CLOUD SERVICES AND THEIR FEATURES

The following features are typical aspects of many cloud services:

- Self-management of the service and the associated applications by the user.
- Technically unrestricted Internet access with standard applications (e.g. web browser) on the user device (e.g. laptop computer, smartphone).
- Multi-tenant use of technical resources, generally across entire computing centre areas or multiple computing centres as a resource pool.
- Immediate elasticity, i.e. automatic allocation of technical resources from the resource pool in case of peak performance requirements or increase in the number of users.
- Continuous measuring of the actual usage per customer and usage-based billing.

11.4 CLOUD SERVICES AND OPERATING MODELS

Two different planes must be distinguished in the provision of cloud services: the type of cloud service and the different operating models that can be freely combined.

(C) CLOUD SERVICES TYPES

Three fundamentally different types of cloud service can be distinguished:

- SaaS – Software as a Service

Refers to all offers of application software that meets the criteria of cloud computing. The spectrum of applications is practically limitless; examples for common services are contact data management, bookkeeping, word processing and collaboration applications.

- PaaS – Platform as a Service

A PaaS provider offers a complete software infrastructure, providing standardised interfaces for customer applications on a platform. Such a platform can include services for multi-

client capability, scalability, access control and database access. The customer generally has no access to the underlying layers (operating system, hardware), but can run proprietary applications on the platform, for the development of which the PaaS provider usually offers a toolset. Examples for PaaS services are force.com by manufacturer Salesforce or Azure by Microsoft.

- IaaS – Infrastructure as a Service

In IaaS configurations, IT resources such as computing power, data storage or networks are offered as a service. A cloud service customer can rent these virtualised and highly standardised services and construct proprietary services for internal or external use within them. A cloud service customer can thus rent computing power, RAM or data storage capacity and run an operating system with applications of its choice on those resources.

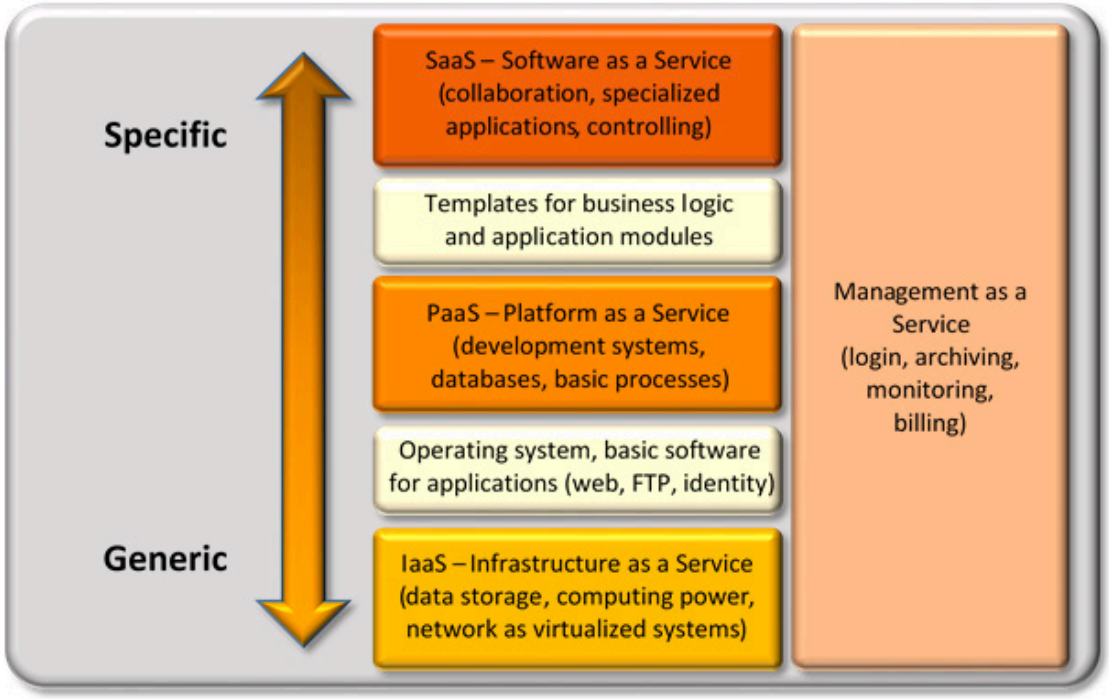


Fig. 3: Source: EuroCloud

Further special forms of cloud services exist, such as Security as a Service (aaS), Business Process aaS, Storage aaS, Monitoring aaS, or Communication aaS. These various concepts are often subsumed under the abbreviation "XaaS".

(D) CLOUD SERVICE OPERATING MODELS

Cloud service operating models are differentiated in terms of who is the operator and who has general access to the services:

Private Cloud: Exclusive provision of services for a defined customer using specific delimited hardware resources (i.e. individual computing centre/s, separate area/s within a computing centre) and network resources not simultaneously used by third parties.

Virtual Private Cloud: In contrast to the Private Cloud, customer delimitation occurs only on the logical network layer, while the actual hardware can be used by multiple customers.



Fig. 4: Source: EuroCloud

Public Cloud: General provision of services for an unlimited clientele using shared hardware resources. The cloud services utilized by individual customers are tracked via logical customer mapping.



Fig. 5: Source: EuroCloud

(E) FURTHER SPECIAL OPERATING MODELS:

- Community Cloud:

Combination of multiple cloud services for certain user groups. These combinations can be defined for areas like logistics, production, research and development, or industry cooperations. Access is not public and requires additional authorisation by the operators of the community cloud. The enterprises participating in a community cloud generally have similar requirements in terms of availability, compliance and security of the provided resources. Examples are banks or government institutions.

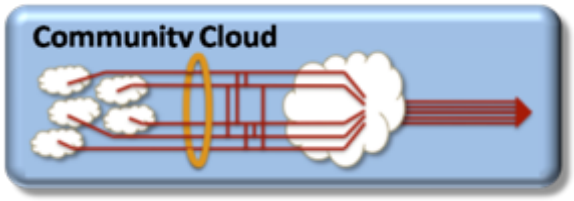


Fig. 6: Source: EuroCloud

- Hybrid Cloud:

Combination of Private and Public Cloud where elements from a private environment (e.g. an ERP system) and from a public environment (e.g. CRM) are merged. An example for the establishment of a Hybrid Cloud is the transfer of a publicly accessible corporate website from the Private Cloud into the Public Cloud. As the company website must be accessible from the Internet anyway, transferring it into the Public Cloud may actually help to improve security.

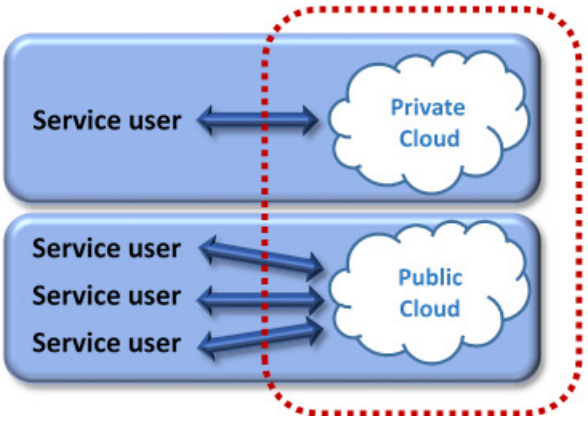


Fig. 7: Source: EuroCloud

11.5 CLOUD SERVICE MARKETPLACE

Various institutions offer their cloud services on a joint marketplace, and maybe even via a joint implementation platform in the cloud. These services can then be bundled into more complex added-value services in order to support business processes. Besides the providers and purchasers of these services, the service developers, and the process designers who compile the added-value services, the operator of the market place fulfils a central role as solution provider or reseller.

12 LEGAL NOTES

12.1 GENERAL INFORMATION

The information provided in this handbook serves for the general illustration of specific legal aspects in connection with cloud computing. The information does not constitute legal counsel, nor can it replace actual legal counsel since such counsel generally requires knowledge of all relevant circumstances, in particular the specific circumstances of the concrete individual case.

12.2 CONTENT OF THE HANDBOOK

The publisher and the authors assume no liability for the completeness, correctness or currentness of the provided information. This applies especially in regard to new developments in legislation or case law. Any liability claims against the publisher or the authors pertaining to material or non-material damages caused by the use of any part of the provided information, or the use of erroneous or incomplete information, are generally excluded.

12.3 REFERENCES AND LINKS

In regard to direct or indirect references to foreign content (e.g. web links) outside of the responsibility of the publisher / the authors, a liability obligation would arise only if the publisher / the authors had knowledge of the information and were technically able to, and could reasonably be expected to, prevent its use in the case of unlawful contents. The publisher / the authors hereby declare that no unlawful contents were recognizable on the linked webpages at the time of placement of the links. The publisher / the authors have no influence on the current or future design, contents, or authorship of the linked webpages. They explicitly distance themselves from all contents of the linked webpages that were changed after placement of the respective links. Only the offeror of the respective linked webpage is responsible for any unlawful, incorrect or incomplete contents, and in particular for any damages resulting from the use or disuse of information thus provided, and not the person referencing the webpage by way of web links.

12.4 COPYRIGHT

The content provided in this publication, including texts, graphics or images, is protected by Austrian copyright law. Contributions by third parties are identified as such. Any use not permitted by copyright law requires prior written consent by the publisher. This applies in particular to any duplication, editing, processing or reproduction of contents in databases or other electronic media. Unauthorised duplication or dissemination of the whole or any part



of this publication is explicitly prohibited. Individual and private use is excluded from this prohibition, though private use does not include the right to pass this handbook on to others. The same applies to publications or other documents.

12.5 COST

This handbook is provided to its addressees/recipients free of charge.

13 AUTORS

Reinhard Travniček
X-tech Handelsges.m.b.H.
Hauptstraße 157
2231 Strasshof, Österreich

E-Mail: reinhard.travnicek@x-tech.at
Web: www.x-tech.at



Dr. Tobias Höllwarth
Höllwarth Consulting
Gluckgasse 2
1010 Wien, Österreich

E-Mail: office@hoellwarth.at
Web: www.hoellwarth.at



Mag. Árpád Geréd
Maybach Görg Lenneis Geréd Zacherl
Rechtsanwälte GmbH
Museumstraße 5
1070 Wien, Österreich

E-Mail: a.gered@mglp.eu
Web: www.mglp.eu





Gerald Haidvogl
Fujitsu Technology Solutions
Guglgasse 15
1110 Wien, Österreich

E-Mail: gerald.haidvogl@ts.fujitsu.com
Web: http://www.fujitsu.com/at/



Dipl. Ing. Christoph Lang-Muhr
Fachhochschule St. Pölten GmbH
Institut für IT Sicherheitsforschung
Matthias-Corvinus-Straße 15
3100 St. Pölten, Österreich

E-Mail: clangmuhr@fhstp.ac.at
Web: www.fhstp.ac.at/de/studium-weiterbildung/informatik-security





EuroCloud Europe a.s.b.l.
L1013 Luxembourg
7, Rue Alcide de Gasperi. Luxembourg

E-Mail: contact@eurocloud.org
Web: https://.eurocloud.org
Copyright: EuroCloud Europe 2016