Secure cloud collaboration for companies in accordance with the EU GDPR

TeamDrive Systems GmbH
Max-Brauer-Allee 50
22765 Hamburg
Germany
Phone +49 40 607709 300
Email: info@teamdrive.com
Web: www.teamdrive.com

February 2018

Contents

1 Executive summary

The cloud is an abstract concept for many businesses and users. Today, instead of exclusively saving their data to internal servers, many companies also store data and documents in the cloud. But no two cloud services are the same and there are a range of options for saving data and documents to the cloud. Equally, no two providers are the same and, as a result, whenever a company decides to store data in the cloud as opposed to on its own servers, many questions arise:

- Where is my data stored?
- Who can access my data?
- How secure is my data?
- What data protection legislation must I observe?

No two pieces of application software are the same either, with solutions that enable users to synchronise data and share data and documents differing in terms of their "look and feel", features, user-friendliness and, above all, security aspects.
IT security and data protection are of crucial importance to companies that store and process data, documents and client data in the cloud – and rightly so. The objective of IT security is to reliably protect data and documents on local computers, during data transfer and in data centres from unauthorised access by third parties (e.g. as a result of cyber attacks), viruses, ransomware and Trojans. This requires certain guidelines and laws to be observed, such as the privacy rights laid down in the German Federal Data Protection Act (Bundesdatenschutzgesetz), European directives and companies' internal data protection policies. German cloud providers such as TeamDrive Systems GmbH with data centres in Germany are subject to very strict data protection requirements.

Besides cloud security, close attention needs to be paid to ensuring the secure transmission of data and secure data integrity processes. In TeamDrive's Sync&Share software, the data communication between local computers, mobile devices and the servers in the provider's data centre is always protected by end-to-end encryption. All keys remain under the user's exclusive control. Thanks to its new point-in-time recovery (PiTR) security solution, TeamDrive also creates regular back-ups known as snapshots. If you lose your data, e.g. as a result of a faulty hard drive or a virus, you can access these snapshots at any time and use them to recover a version of your data quickly and easily. In addition to snapshots, TeamDrive creates complete, redundant data back-ups in the cloud.

After almost four years of debates, the European Council, the European Parliament and the European Commission have agreed on the final contents of the new EU General Data Protection Regulation (GDPR). The new regulation came into effect on 25 May 2016 and replaces the EU Data Protection Directive (Directive 95/46/EC) in place since 1995. The regulation provides for a two-year transition period and will be mandatory across the European Union from 25 May 2018.
The enforcement of the EU GDPR on 25 May 2018 will bring with it various changes to how personal data is used and stored. From this date, companies will be required to introduce data protection management procedures in order to keep personal data secure. Any company found breaching the provisions laid down in the GDPR will face hefty penalties, which will not only result in financial losses but will also seriously affect the company's reputation. Anyone who comes into contact with the personal data of third parties in a professional capacity would be well advised to familiarise themselves with the new provisions and to adjust their business practices in line with the future requirements in order to avoid a heavy fine. The end-to-end encryption used in TeamDrive reduces the risk of incurring penalties and means companies are less likely to be obliged to report cases of loss. TeamDrive will therefore not only protect your data, but your data controllers and managing directors as well.

2 Cloud computing – the future of data management

2.1 Unfounded fear of the cloud

These days, cyber attacks are fairly commonplace and are far from unique to the cloud. For instance, on 25 September 2017, it was uncovered that hackers had gained access to databases belonging to Deloitte Limited through an administrator account that had presumably not been sufficiently protected. It would seem that the hacked administrator account had only been secured with a single password and not with two-factor authentication, which is normally the case for accounts that have such a bearing on security. As reported in the Guardian[1], the hackers were able to gain access to passwords, usernames, health information and other sensitive data belonging to the management consultancy's blue-chip clients. The perpetrators are said to have been stealing data on a large scale for months.

At the start of September 2017, it was discovered that Equifax Corporation, the largest of the three major credit reporting agencies, had fallen victim to data theft in the USA. Between May 2017 until the breach was discovered on 29 July 2017, unauthorised parties had gained unlawful access to sensitive data belonging to 143 million Americans. This accounted for 44% of the US population and there were further victims in Canada, Great Britain and Northern Ireland. The hackers obtained access to personal data such as social security numbers, dates of birth, addresses and credit card and driving licence numbers.[2]

The attack on Equifax Corporation represents the greatest case of theft of social security numbers to date. It was made possible by a security hole in one of the company's web applications built into its website. The total extent of the damage not to mention the loss of reputation suffered by Equifax Corporation is still unclear.

However, this is not the first case of large-scale data theft. Back in 2013, the retail chain Target Corporation was hacked, resulting in the theft of 40 million credit card numbers. The total damage was estimated at around 300 million US dollars. Target's Canadian subsidiary was unable to recover from the ensuing loss of reputation and was forced to file for insolvency.

Despite all these cases, many companies continue to rely on on-premise solutions by storing data on their own property. Above all, it is security and data protection concerns that cause a feeling of unease among data controllers and deter companies from hybrid data storage. However, with the right security solutions, sensitive data can be sufficiently protected in the cloud thanks to standardised back-up procedures and defined service level agreements.

Besides security fears, companies also worry about becoming dependent on a single provider. This anxiety is completely unjustified, however, as cloud suppliers are now firmly established, there are numerous benefits of cloud computing and data migration between cloud providers has become a tried-and-tested process that is possible with virtually no downtime. According to recent figures, almost two thirds of small and medium-sized businesses (SMEs) in Germany took advantage of cloud computing in 2016[3], and the trend is growing.

[1] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails?CMP=twt_gu
[2] https://www.extremetech.com/internet/255311-equifax-fine-print-keeps-getting-longer-situation-mostly-gets-worse?utm_source=email&utm_campaign=dailynews&utm_medium=image
[3] https://www.heise.de/forum/heise-online/News-Kommentare/Hacker-Jackpot-Credit-Bureau-Equifax-gehackt/forum-387653/comment/

2.2 Security – the pros and cons of cloud computing

When asked about what deters them from using the cloud, data controllers often cite security concerns, claiming that transferring data to data centres over the internet is too insecure. However, the precise opposite is true. After all, what small or medium-sized business is capable of taking security measures comparable to those implemented by certified providers and their data centres? Such security measures include an uninterrupted power supply, elaborate precautions against fire and back-up solutions in different locations, not to mention a continuously up-to-date firewall and the latest encryption technology.

According to the 2016 Global Cloud Data Security Study, 54% of the companies questioned regard their own security strategies as insufficient.[4] Companies live with the understandable fear of sensitive data being shared carelessly with business partners or clients. This is compounded by the fact that almost half of all data in the cloud is not managed and controlled by IT departments, but rather by other areas within a company. Similar figures are cited by Bitkom Research. Its Cloud Monitor 2017 representative study found that the proportion of cloud users rose to 65% in 2016, which marks an increase of 11% compared to the previous year.[5] What's more, 24% of companies are planning to or considering whether to switch to the cloud in the future. Companies in the chemical and pharmaceutical industry are leading the way in this respect, with 88% of them already using cloud services such as software as a service (SaaS).

Dr Axel Pols, Managing Director of Bitkom Research, summarised the results: "Cloud computing has become widely established and has developed into a fundamental technology behind digitalisation in just a few years. The use of IT services over data networks in line with demand offers a tremendous range of advantages."

2.3 Choice of provider

No two cloud services are the same. The main distinguishing features are the location of the data centres, the level of control over the flow of data and the services offered. Location is a crucial factor because data protection legislation differs from country to country. After Edward Snowden's revelations, it became clearly apparent that the large external data centres managed by Microsoft and Google are not as secure as made out.[6] Moreover, US authorities have confirmed that European data protection laws do not apply to American firms operating in Europe. Application software produced by American companies, such as Microsoft OneDrive for Business, Dropbox Business or Box Business, are subject to US law, meaning that personal and company data saved using these services are not protected from access by US authorities regardless of the location of the servers. Therefore, anyone who wants to play it safe should choose a provider with servers in their home country. TeamDrive only ever stores client data in German data centres.

Anyone considering using the cloud should compare services carefully, in particular in terms of the origin of the provider and the location of the cloud server. If the provider's headquarters and data centre are located in Germany, the cloud is subject to German data protection laws and German legislation.

2.4 Outstanding level of security

Cloud computing is a matter of trust. Certification provides evidence that a provider of cloud services follows security and quality management processes as well as observes specific data protection guidelines.

For example, the Deutsche Anwaltverein e. V, an association for lawyers in Germany, worked with TeamDrive Systems GmbH to develop a cloud data storage solution especially for lawyers. Thanks to the system's end-to-end encryption

[4] https://safenet.gemalto.com/resources/data-protection/cloud-security-study-2016-report/
[5] https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/03-Maerz/Bitkom-KPMG-Charts-PK-Cloud-Monitor-14032017.pdf
[6] http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-macht-das-internet-sicherer-1.1984638

and guaranteed server hosting security standards, the Deutsche Anwaltverein e. V recommends to its approximately 68,000 members this state-of-the-art solution for storing, synchronising and sharing data and documents, which meets the specific requirements placed on members of this profession as persons entrusted with secrets in accordance with Section 203 of the German Criminal Code (StGB) and the German Federal Data Protection Act (BDSG). The solution gives law firms and lawyers the assurance that they are not unintentionally violating the interests of their clients when storing, synchronising and sharing data. Users of TeamDrive can rest assured at all times that confidential data is only transferred in an encrypted form and is always stored in a dedicated highly secure data centre in Germany under clearly defined conditions.

The TeamDrive software has been awarded the Data Protection Seal of Privacy of the Regional Centre for Data Protection of Schleswig-Holstein in accordance with Section 4 Paragraph 2 of the Regional Data Protection Act (LDSG) in conjunction with the Data Protection Audit Regulation (DSAVO).

The multi-award winning data centres are certified in accordance with ISO/IEC 20000-1 and ISO 27001 on the basis of the IT baseline protection approach from the German Federal Office for Information Security (BSI).

Gartner, Inc., one of the world's largest IT consultancies and analysts, included TeamDrive in its Cool Vendor for Privacy 2013 list.

2.5 Trust is good, control is better

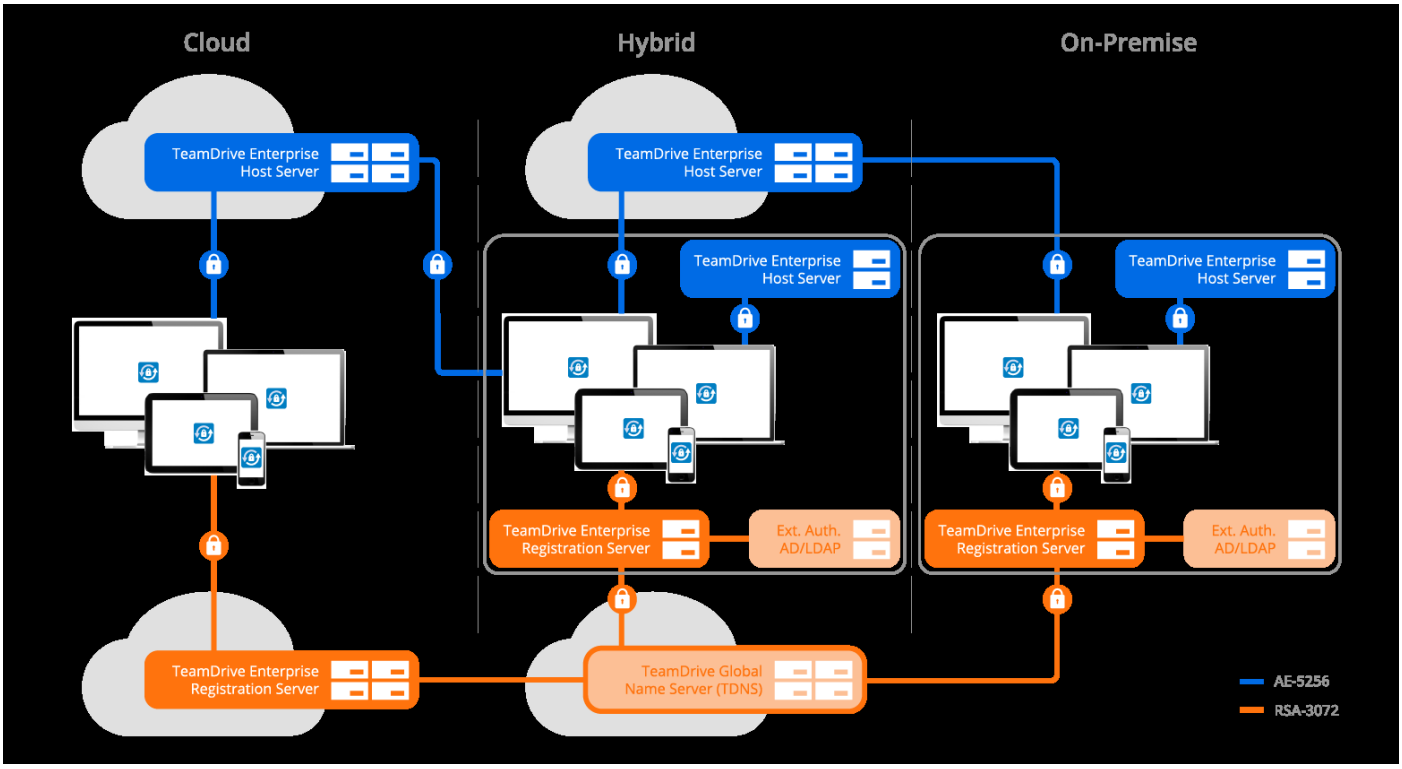
The issues of data protection and data security are among the most important criteria when choosing a cloud model. Data storage is a matter of trust. In contrast to non-transparent public cloud solutions such as Box, Dropbox and Microsoft OneDrive, TeamDrive Systems GmbH offers its clients complete end-to-end encryption (256-bit AES) for their data and documents as well as storage in dedicated data centres in Germany (private cloud).

Above all, sectors that are required to handle large quantities of sensitive data have until now chosen to place their trust in the tried-and-tested private cloud model. In the private cloud, users are given an adequate IT environment all to themselves. The private cloud is either hosted within the user's own data centre or externally in the service provider's data centre – where, however, it is kept separate from those of other clients.

In recent years, the hybrid cloud[7] concept has emerged as a popular, forward-looking model. The term "hybrid cloud" describes a cloud environment in which companies manage some of their IT resources on site (on-premise), while their remaining data is hosted by a service provider.
TeamDrive supports the use of a hybrid cloud and – unlike Box, Dropbox or Microsoft OneDrive – not only offers cloud services, but provides a free choice of servers as well. You can choose to save your data exclusively on servers hosted by TeamDrive, on your own servers or on servers belonging to a service provider chosen by you. The TeamDrive security layer offers additional protection through your company's existing infrastructure.

[7] https://digitales-wirtschaftswunder.de/Crisp-QSC-Multi-Cloud-Studie.pdf

Figure 1: Using a hybrid cloud with TeamDrive



3 Countdown to the GDPR

3.1 Implications of the enforcement of the GDPR

In the future, natural persons will be able to access their data more easily. This means that every natural person will have the right to find out what data has been collected and stored about them. In addition, every natural person will be entitled to receive clear information about who is using or processing their data and for what purpose.

As part of this, in the future, it will be necessary to provide natural persons with more detailed information in the event of unauthorised parties gaining access to their data. The aim of this is to give all natural persons the opportunity to take steps to protect themselves in good time.

Personal data always belongs to the natural person to whom it relates and not to the internet service processing it.

The launch of the new GDPR will entitle every natural person to transfer their data from one internet service provider to another. In addition, the "right to be forgotten" will be stepped up by giving natural persons the chance to request that any information ever published about them be deleted.

TeamDrive – as a German company – offers crucial benefits over Box, Dropbox, Microsoft OneDrive, Google Drive or Amazon AWS, as it only uses data centres in Germany to store data in Europe for its European clients. Your data is subject to the data protection regulations laid down in the German Federal Data Protection Act (BDSG). Storage space is allocated automatically during registration depending on your IP address when you sign up. After this, the server allocated does not change while you are using the service, regardless of from where you are accessing it.

3.2 What are the exact implications for your company?

Section 9 of the German Federal Data Protection Act (BDSG) states the following: "Public and private bodies collecting, processing or using personal data either on their own behalf or on behalf of others shall take the technical and organisational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act."

The annex to Section 9 BDSG demands that the access to and the transmission of personal data be controlled. It must also be possible to control whether and by whom personal data is inputted, modified or removed. Finally, it must be guaranteed that

- personal data is only processed in accordance with the instructions of the client
- personal data is protected from accidental destruction or loss and
- data collected for different purposes can be processed separately.

The use of state-of-the-art encryption procedures is explicitly recommended.

3.3 The German IT Security Act (ITSiG)

In 2014, German Minister of the Interior Thomas de Maizière stated in the Frankfurter Allgemeine Zeitung (FAZ) that "Anyone who creates risks for others through the use of IT must be held accountable by providing protection against these risks,"[8] adding that the more serious the risks, the tighter the safeguards required. De Maizière went on to write that "It is no longer sufficient for services and initiatives available in this area to be used on a voluntary basis" and the state must therefore introduce "a safety belt for the IT systems used in critical infrastructures".

[8] http://www.faz.net/aktuell/politik/inland/de-maiziere-ueber-die-digitale-agenda-deutschland-wird-it-vorreiter-13103217.html

The German Federal Office for Information Security (BSI) refers to the objectives of the EU and the German government as “Resilience against cyber attacks”:

1. Drastically reducing cybercrime
2. Developing a cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
3. Developing the industrial and technological resources for cyber security
4. Establishing a coherent international cyberspace policy for the EU and promoting core EU values.

In the FAZ, de Maizière also announced the new German IT Security Act, which – in addition to the healthcare sector – classifies the energy, information technology and telecommunications, traffic and transport, water, food and financial and insurance sectors as “critical infrastructures”. He commented that it would be particularly responsible of providers if they were to take the necessary technical and organisational measures before these were required by law.

3.4 Hefty penalties for breaching the EU GDPR

The European General Data Protection Regulation will be enforced on 25 May 2018. From this date, companies will be required to introduce data protection management procedures in order to keep personal data secure.

To date, violations of the GDPR have frequently been treated as trivial offences and the penalties have been accordingly lenient. However, this approach is soon set to change: Article 83 defines “General conditions for imposing administrative fines”: “Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.” In other words, “According to the new regulations, effective, proportionate and dissuasive fines must be enforced in each individual case.”
Anyone who comes into contact with the personal data of third parties in a professional capacity would be well advised to familiarise themselves with the new provisions and to adjust their business practices in line with the future requirements in order to avoid a heavy fine.”
The objective is to ensure the “security of processing” (Article 32) – including by third parties. The controller and the processor should implement appropriate technical and organisational measures to ensure “a level of security appropriate to the risk”. In doing so, the state of the art, nature, scope, context and purpose of the processing and the likelihood and the severity of the risk to the rights and freedoms of natural persons should be taken into account. In plain English, this means that if personal data goes missing, the supervisory authority will have to be informed of this within 72 hours. Furthermore, all parties affected must be informed of the data loss immediately, unless the loss of data does not pose a high level of risk. This is the case when the data is encrypted using state-of-the-art technology.

!

According to Article 33 GDPR, the competent supervisory authority and the data subjects (Article 34 GDPR) must be informed of a breach immediately and no later than within 72 hours of knowledge of the breach being obtained.

According to Article 34.3 (a), you are not required to report a personal data breach that is likely to severely endanger the rights of natural persons if the data was encrypted. By using TeamDrive, you can guarantee that this protection is in place.

The fine is hefty. According to Article 83, anyone who breaches the regulation puts themselves at risk of an administrative fine, which as stated in the law "shall in each individual case be effective, proportionate and dissuasive". This means that it could amount to "up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher". It is important to note that the German Insurance Association (GDV) has ruled out the possibility of insurance policies that cover the risk of administrative fines due to fears of such policies being viewed as "unethical". This means that the responsible party will have to foot the bill themselves! It is also possible that breaches of the requirements will result in claims for compensation for the material and non-material damage referred to in the regulation (Article 82). The GDPR also gives associations the right to lodge complaints (Article 80). According to this Article, "each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject". In addition, the supervisory authority shall have the power to prohibit the infringer from processing data (Article 58). An equally serious consequence of breaching the regulation is the resulting loss of reputation, as if a company were to fall victim to cyber attacks on multiple occasions, trust in this company would begin to wane. In fact, around one in three people would be prepared to switch products or brands in such cases.

As warned by the Organisation for Economic Co-operation and Development (OECD) in 2016, security holes and data attacks on the one hand and administrative fines and claims for damages on the other could put a company's very existence at risk. According to the OECD, data attacks are becoming ever greater in terms of effectiveness, quantity and severity and are therefore capable of undermining an SME's capacity for innovation and market position. Any company without the financial means to pay for legal advice, forensic investigations, the notification requirements, the recovery measures, the administrative fines and court rulings risks being quickly forced out of the market.

A study by service provider Veritas[9] has found that fewer than 10% of companies with 1,000 employees or more have currently implemented the regulation. Under certain circumstances, this could partly be caused by companies failing to properly understand the concept of what actually constitutes the state of the art. One of the reasons for this is the lack of understanding among managers responsible for information security. The situation is, however, worsened by the fact that according to market research company Frost & Sullivan the shortage of security specialists is expected to rise by 20% by 2022 compared with 2015[10]. It is anticipated that small and medium-sized companies will suffer especially as a result.

May 2018 is right around the corner and small companies, in particular, have a huge mountain to climb. Until now, there was no need for companies with fewer than ten employees to even appoint a data protection officer (Section 4e German Federal Data Protection Act – BDSG). It is not inconceivable that some small companies have also failed to keep a register of proceedings to date (Section 4d BDSG). This raises the question of how small companies will manage to put in place the information security requirements by May 2018. As 25 May 2018 draws closer (the date from which the GDPR must be applied by companies), it is expected to become increasingly difficult for these companies to even find a consultant who can support them to implement the legal requirements.

Besides an administrative fine, companies could also face claims for damages. Article 82 of the regulation says: "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

[9] Veritas: Germany is lagging behind: companies feel poorly prepared for the GDPR, 25 April 2017, https://www.veritas.com/de/de/news-releases/2017-04-25-veritas-study-organizations-worldwidefear-non-compliance-with-new-european-union-data-regulation-could-put-them-out-of-business

[10] https://www.computerwoche.de/a/grosser-mangel-an-it-sicherheitsfachkraeften,3331095

3.5 IT security and data protection have a lot of catching up to do

Timotheus Höttges, CEO of Deutsche Telekom, strongly believes that "everything that can be digitalised will be digitalised. And everything that can be connected will be connected."[11] Besides communication and processes, consumer goods can also be digitalised. For example, consumables can be automatically reordered when they are low in stock, smart metering components can be controlled and evaluated remotely, and vehicles can be located and hired using an app. This growing level of interconnections is a consequence of the internet of things, which is seeing suppliers connecting with manufacturers and retailers, hospitals and medical practices connecting with health insurance companies, and architects connecting with engineers, building authorities and property managers. This enables a "real-time economy". However, not everyone who gains access to information is entitled to it. According to a study by memory products manufacturer Kingston, 95% of companies store their corporate data on USB devices and more than half of these do so without using encryption[12]. In addition, 39% of employees claim to have lost these storage devices at least once. More than half of the companies questioned by Kingston were found to have "inadequately" secured their mobile storage products.

> **!** **Only four in ten small and medium-sized business encrypt data and hard drives. As claimed by the manufacturer of antivirus software Kaspersky, employees are believed to cover up security leaks in 40% of SMEs. The situation is no better in corporate networks, as 33% of large companies are said to be unaware of where their data is physically stored.**

According to information available to Gartner, 55% of companies worldwide have an identity and access management system. Conversely, however, this means that 45% of companies do not know who has access to what information. Dirk Kretzschmar, Managing Director of TÜV Informationstechnik (TÜViT), believes that only 3% of companies are prepared for data attacks. At the same time, risk experts warn that a tough cyber security programme is "essential for survival" in our computer age.

3.6 GDPR requires evidence of data security measures

To help avoid cyber attacks, the General Data Protection Regulation (GDPR) will apply in the European Union from 25 May 2018. Authorities and companies must be in a position to demonstrate at any time that their data processing activities are secure. According to Recital 78 of the regulation, the controller should "adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default." As laid down in Article 42, the easiest way in which the controller can demonstrate compliance with the requirements is by means of appropriate certification. TeamDrive already meets these requirements, as the quality of the company's data security is proven by a data protection seal from an institution closely associated with the authorities.

According to Article 32, the GDPR requires the following: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

The risks cited by the regulation (Recital 75) include physical, material or non-material damage, identity theft or fraud, financial loss, a loss of reputation, and economic or social disadvantages. Possible sabotage by employees or the infiltration of malware must also be considered in this context. These risks need to be identified and analysed. The

[11] https://www.heise.de/newsticker/meldung/Telekom-Chef-Alles-wird-vernetzt-2661572.html
[12] http://www.kingston.com/de/company/press/article/48111

German Federal Office for Information Security (BSI) recommends that this process be conducted using its Risk Management Standard 200-1.

3.7 GDPR demands state-of-the-art security measures

"State of the art is the state of the development of progressive processes, equipment and modes of operation, which in the prevailing opinion of leading experts appears to enable it to be guaranteed that statutory objectives can be met." As defined in a brochure on the state of the art by lawyers and computer scientists from the TeleTrusT – IT Security Association Germany, the technology and processes must have "proven themselves in practice" or – if this is not yet the case – "their operation must at the very least have been successfully tested".[13] The brochure adds that European Union law also uses the phrase "the best available techniques". In the view of the authors, these definitions correspond largely to the blanket phrase "state of the art".

3.8 The need for security is no reason not to use the cloud

The issue of security plays a very important role when data is transmitted, as ultimately personal data is sensitive information. Only a few companies are still deterred from using cloud technology. A few years ago, some clients still harboured concerns about cloud computing, especially in terms of security. This has since changed, however, with cloud computing developing into an established technology. Clients now appreciate the benefits of using the services of a public cloud provider compared with traditional on-premise hosting. Here, the high security standards in place in Germany are regarded as a benchmark.

Generally speaking, cloud providers are better placed to keep data secure than the companies making use of their services. In fact, small and medium-sized businesses in particular are frequently unable to cope with the requirements of secure data management.

3.9 Germany's security standards make it a popular location for data centres

Numerous clients place immense value on their data remaining and being hosted in Germany. Data hosted in Germany must fulfil the data protection and security standards required under German law. Data and documents stored locally and on servers using TeamDrive software are always protected using end-to-end encryption (256-bit AES). This means that data and documents processed and synchronised with TeamDrive cannot be viewed by anyone at any time in accordance with the current state of the art.

[13] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

4 TeamDrive's Sync&Share software

4.1 About TeamDrive

TeamDrive is a sync and collaboration solution for multiple areas of use. Sync and collaboration solutions help teams to communicate as well as to create and archive documents.

TeamDrive gives users and user groups the chance to access shared stored data and make changes to documents. In TeamDrive, the stored data is always secured by end-to-end encryption (256-bit AES) and your data and documents are protected from unauthorised access by third parties.

With TeamDrive, users can share project-related data and documents with colleagues, clients, external service providers and partners. In TeamDrive, a shared work area is called a Space. A Space corresponds to a folder in a file system. You can save as many folders, subfolders and files as you wish in a Space. Files and documents can be added to a Space in TeamDrive or a folder in your file system using drag and drop.

You can use the authorisation system to specify who is entitled to perform certain actions in a Space. The Space administrator manages the team members. As the Space administrator, you can invite colleagues or partners to join a Space by email and give them pre-defined access to files and folders. You also have the option of turning a folder from your file system into a Space and managing it in TeamDrive. You can also work at the file system level within TeamDrive. In addition, it is possible to gain access to your stored data via a browser interface (web client).

A Space is on a TeamDrive hosting server, which is stored in the TeamDrive cloud, on a WebDAV server or on premise on one of your company's on-site servers.

TeamDrive monitors any number of local files and folders in the file system and in Spaces, synchronising them between the personally invited team members. TeamDrive can be used to synchronise files and folders between multiple computers and mobile devices. All files and documents are always available to all team members in the file system – including offline. By default, TeamDrive's server communication structure allows data to be automatically synchronised between the computers and mobile devices in use (this default setting can be deactivated if necessary). TeamDrive uses various intermediate servers to ensure the service remains available to teams and their members. During transfer between your computer and the server, the stored data is secured by end-to-end encryption (256-bit AES) at all times and the latest state-of-the-art technology is used to protect it from access by unauthorised third parties.

Thanks to its high level of data security, TeamDrive is especially suitable for companies and groups of professionals that store sensitive data, such as banks and insurance companies, universities, lawyers, notaries, medical professionals or those working in research and development.

The intermediate servers mean that you can use the secure cloud, your own servers or a compatible WebDAV server. The TeamDrive software's Personal Server can also be used for this purpose. If desired, you can choose to use services made available by commercial providers.

TeamDrive is compatible with the MS Windows, Mac OS X/macOS, Linux, iOS and Android operating systems and is available as a web client.

4.2 Audit trail

An audit trail is a chronological sequence of actions, events or system statuses that can be documented, tracked and retraced. An audit trail is used to check up on and/or monitor users and their activities.

The integrated audit trail enables modified data to be logged in TeamDrive and analysed. All changes to data and documents in TeamDrive can be described in detail in a consistent and comprehensible manner.

Every time data is changed in the system, this is recorded in a transaction log file. If a file is created, an entry with the document's global ID, the date, a time stamp, the user ID and device ID is added to the transaction log file. Changes, such as the renaming or moving of a file, the creation of a new document version or the deletion of a document, are stored in the transaction log alongside the details of the user (user ID) and the computer or mobile device used (device ID).

In addition, all details about the user and their rights are stored:

- When was a user invited and what rights were they given?
- When did a user accept the invitation?
- What data or which document did a user access and when?
- On what device did the user gain access?

An analysis of the audit trail can be exported as a CSV file.

The audit trail export file is encrypted with 256-bit AES. This means that it is not possible to subsequently edit or manipulate the export file. The transaction log file is saved to the TeamDrive hosting server and cannot be amended by the user.

4.3 Point-in-time recovery

One of TeamDrive's key features is its snapshot technology. Point-in-time recovery is used to back up and restore data from a snapshot. TeamDrive automatically creates regular (if desired, every 30 minutes) snapshots of the stored data for all of a user's computers. In the event of a loss of data (e.g. due to a hardware fault or a ransomware attack), the data can be completely restored in just a few simple steps. In the version for personal use, the backed-up data is deleted after 30 days. In order to meet legal requirements or contractual provisions, for example, the version for business use stores backed-up data for up to ten years.

5 Protective measures

5.1 Version control

In TeamDrive, all data – along with earlier versions – including metadata is saved to a server.

Automatic version control allows the latest version of a document to be accessed at all times. Detailed information on the author, version, previous version and the date the file was last edited is available for each version of a document. The version timeline shows all versions of a document and enables conflicts between versions to be resolved.

Data is never transferred unencrypted within the TeamDrive network. All documents are encrypted on the server before being saved and sent. Data can only be decrypted by team members in a Space.

5.2 Security

Data stored on your computer is generally unencrypted. All data stored and sent in TeamDrive is encrypted with 256-bit AES. To increase security further, TeamDrive can be installed and run on an encrypted partition (e.g. on a data storage device encrypted with VeraCrypt or PGP).

Table 1: a brief overview of the most important features

TeamDrive at a glance	Description
Anywhere in the world, flexible and fast	You can use TeamDrive anywhere in the world on your laptop, tablet or smartphone. Partners or service providers can gain access to a Space wherever they are, provided that they are a team member.
Operating systems	MS Windows, Mac OS X/macOS, Linux, iOS, Android (you can also use TeamDrive on any standard browser).
Encryption	Every Space has its own secure AES 256-bit key (the keys remain on your computer at all times).
Password and expiry date	You can protect files with a password and/or expiry date.
Encryption	Every Space has its own secure 256-bit AES key (the keys remain on your computer at all times).
Customised authorisation system	The creator of a Space is also its administrator. You can allocate customised user rights for each Space.
Team work	You can set up teams so that you can work on documents together.
Point-in-time recovery	You can restore data easily from a snapshot, e.g. in the event of a virus.

Hybrid cloud	You can use different types of server at the same time: on-premise, WebDAV, cloud computing or a combination.
Version control	Automatic version control for all documents.
Back-up	Automated back-up feature for your data.
Document editing	Offline editing with automatic synchronisation.
Synchronisation	You can synchronise as many folders and documents as you like (depending on the server space available).
Notification centre	You will be notified about new versions, comments, invitations, conflicts, errors, etc.
File formats	Support for all file formats for documents, photos, videos and programs.

6 Glossary

AES encryption
AES encryption is the end-to-end encryption of transmitted data. The data being transmitted is encrypted at the sender's end and is not decrypted until it reaches the recipient. The name of the type of AES being applied depends on the chosen length of the key. The higher the number, the higher the degree of encryption. TeamDrive uses a 256-bit AES key, which is currently the highest level of encryption.

Audit trail
An audit trail is a software-based process applied in operating systems, database systems or application and administration software, in which the user and their activities are monitored and logged for a specified period of time. The process is employed, on the one hand, to monitor user activities and, on the other hand, to make it easier to restore a system or data in the event of an incident.

CSV file
The abbreviation CSV stands for comma-separated values and refers to a type of text file used in data processing to help record, store and process large quantities of structured data.

Cloud
The cloud or cloud computing describes the provision of an IT infrastructure, such as storage space, computer power or application software, as a service over the internet. This is the type of service provided by TeamDrive Systems GmbH. The servers used by TeamDrive Systems GmbH for its European clients are located in Germany and are subject to German data protection regulations.

Host
In the original sense of the term, a host is a mainframe computer to which computers gain access in order to perform specific actions. Today, the term host is also used for servers in a data centre that provide storage space or application software for private individuals, companies or corporations.

Hyperlink
A hyperlink is a link within a document that leads to another place within the same document or to an external document or file. If a hyperlink is activated, the destination to which it links is automatically accessed.

Malware
The term malware is used to describe computer programs that are developed to perform undesired and harmful functions on computers and servers. There are various types of malware, including computer viruses, Trojans, ransomware and spyware.

On-premise
The term on-premise describes a licence and usage model for server-based computer programs. The software is either rented or bought and is operated at the user's own responsibility and in the user's own data centre.

Service level agreements
A service level agreement (SLA) refers to an agreement between a client and a service provider for specific services. The service level describes the agreed scope of the services, e.g. the availability of the provider and the coverage of their response in the event of it being necessary for a certain service to be restored.

URL

A URL (uniform resource locator) is a link to a complete path that can be opened using a standard browser (e.g. Microsoft Edge, Google Chrome, Mozilla Firefox). An example is https://www.teamdrive.com/en/.

VPN

VPN stands for virtual private network. VPN technology enables users to securely access resources in a private network from anywhere in the world. A VPN fully encrypts an internet connection from a computer to a VPN server in real time.

WebDAV server

WebDAV is an open standard for the provision of data online. Today, there are WebDAV solutions for every operating system that allow WebDAV servers (e.g. Deutsche Telekom AG's MagentaCLOUD™) to be implemented.