DLA PIPER

WHITE PAPER

Meeting European Data Protection and Security Requirements with CipherCloud Solutions

TABLE OF CONTENTS

This white paper contains data and information up to date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore DLA Piper UK LLP cannot give any guarantees relating to the content of this white paper. Ultimate responsibility for all interpretations of, use of, data information and commentary in this report remains with you. DLA Piper UK LLP will not be liable for any interpretations or decisions made by you. © DLA Piper UK LLP.

1. EXECUTIVE SUMMARY

In this white paper, DLA Piper investigates the ways in which encryption and tokenization of data can help companies that are subject to EU data protection and general security laws adopt cloud-based solutions and remain in legal compliance.

The first part of this paper outlines the most relevant, applicable data privacy rules and policy initiatives throughout the European Union, as well as key legal challenges that may result for companies considering cloud services. Three main issues are investigated:

1. The regulatory requirements of processing "personal data" in the cloud
2. The security of personal and other types of data
3. The protection of data processed in the cloud from seizure or any other kind of access by third country law enforcement agencies

This paper also discusses the current debate and most recent European guidelines on whether encryption or tokenization of data constitutes anonymization of the data.

The second part of the paper analyzes how encryption and tokenization techniques, as offered by CipherCloud, can address the challenges presented.

We conclude that for several jurisdictions, a sufficient level of encryption or tokenization of data before sending it to the cloud could avoid the legal barriers created by data protection laws. For stricter jurisdictions, encryption and tokenization techniques can still offer substantial benefits for achieving legal compliance from a data protection point of view, both under current and future EU data protection laws (as proposed at the time of writing this document).

Also from the perspective of general security requirements and protection against unwanted access to the data, CipherCloud security products, when implemented properly, offer an excellent tool to achieve a high level of compliance.

2.

ADOPTING CLOUD SOLUTIONS: WHAT ARE THE KEY LEGAL CHALLENGES?

When considering whether to adopt the cloud, many companies face similar barriers. Not all of these issues are legal in the sense that they are subject to specific regulatory requirements, and some of them depend on the contractual negotiations between the cloud provider and the cloud customer. Examples of these non-legal issues include: the level of internal control, whether the cloud customer has a say in how the cloud technology is deployed to process data, service levels guarantees, and availability of core services, as well as changes in corporate structure or control by the cloud provider.

However, several other recurring issues are indeed legal and are further discussed below. Companies falling under the realm of EU laws typically face legal issues related to regulatory requirements of processing personal data, overall security of data, and access to cloud data by foreign law enforcement agencies.

2.1 Data protection: am I processing personal data in the cloud?

Context: Given the shifting legal landscape in the European Union and growing awareness of privacy and data protection issues (for citizens, companies and governments), one of the first questions companies must answer before going into the cloud is whether this will involve the processing of personal data.

These considerations are especially important when large quantities of data are being processed or when data is considered sensitive by law, such as healthcare data, or sensitive by general sentiment, such as personal financial or location data.

Legal basis: The primary EU legal basis for the processing of personal data is set out in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive"). It applies to **processing** (which involves any level of the information processing flow) of **personal data** (broadly defined as any information relating to an identified or identifiable natural person) by automatic means, by a **data controller** (i.e. the entity determining the "purposes" and "means" of the processing), in the context of its activities as a Europe-based establishment, or when making use of equipment situated on the territory of an EU Member State.

In practice, when a company transfers data that is considered personal to a cloud service, the company is likely to be seen as a data controller, and the cloud provider is in principle likely to be qualified as a data processor.

Key legal challenges: Application of the legal principles set out in the Data Protection Directive, as subsequently implemented by the EU Member States, gives rise to a number of regulatory requirements to take into account. When companies decide to go to the cloud, these requirements include that:

- The company can invoke a legal basis to process data via cloud-based services;
- Data subjects are sufficiently informed in accordance with legal requirements;
- There are strict limitations on transferring data outside of the European Economic Area, which in a cloud context may be very hard to achieve;
- The company, as cloud customer, should take appropriate technical and organizational measures in order to protect the data, taking into account the current state of the art, cost, risk level and nature of the data processed;
- Cloud customers must also assess whether a cloud provider offers sufficient guarantees in respect to technical and organizational measures, and this (together with certain liability provisions) must be laid down in a written contract.

Encryption and tokenization tools, when implemented properly, can help a cloud customer subject to data protection laws comply with some of these legal requirements.

Below, we describe how encryption and tokenization tools, when implemented properly, can help a cloud customer subject to data protection laws comply with some of these legal requirements.

What about anonymous data? The legal requirements described above only apply under the condition the data processed effectively constitute "personal data" as defined by Data Protection Directive. This is not the case when the data could be qualified as "anonymous" data. In order to be considered anonymous, it must be rendered in such a way that the data subject is no longer directly or indirectly identifiable.

In short, if a cloud customer can bring forward sound arguments to state that the encrypted or tokenized data transferred into and processed by means of the cloud does not constitute "personal data," the above described **requirements for data protection would not apply.** This can provide a high level of comfort from a compliance point of view.

We indicate further below that at least in a number of jurisdictions, competent administrative authorities, and even courts, are not adverse to this argument.

2.2 Security of the data: is my data sufficiently secured?

Context: Surveys indicate that the issue of data security is a top concern for companies from a legal, commercial, and operational perspective. The issue of data security touches a wide range of elements.

While it may be important that personal data is secured (and specific legal requirements apply), even when data does not qualify as personal, security may be one of the most important issues as companies do not want business-critical information to be subject to data breaches, hacking or other unauthorized forms of access. Most companies need to ensure the availability of their services and continuity of service delivery, and do not want their data altered or modified by unauthorized parties. Adequately securing data has effectively become a business-critical issue.

Policy initiatives: Given the importance of data security, the European Commission in its Communication titled "*Unleashing the Potential of Cloud Computing in Europe*" has made it one of its key action points to set up security standards and adopt certification schemes.

The initial action of the European Commission has resulted in the establishment by the European Telecommunications Standards Institute (ETSI) of a "Cloud Standards Coordination" report. This document provides an overview of ongoing standardization initiatives in cloud security.

Related to this framework, the European Union Agency for Network and Information Security ("ENISA") lists on its website the existing cloud computing certification schemes, including the International Organization for Standardization (ISO) and PCI Data Security Standards.

Below, we discuss how the tools CipherCloud offers fit in with these and other certification schemes.

2.3 Can foreign law enforcement agencies access my data?

Context: The Snowden revelations and on-going media coverage surrounding this and subsequent leaks have placed the protection of data (whether personal data or not) from actions of foreign law enforcement agencies high on the agenda.

European companies must be aware of these considerations when "transferring" data in any way to a third party located in territories outside of the European Economic Area. This can apply to both data stored outside the EU, or local servers that can be accessed remotely. The importance of this was highlighted recently by the Microsoft Ireland judgment. In this case a New York court ruled that even though data was stored on servers located outside of the United States, in this case Ireland, Microsoft was still ordered to comply with a US law enforcement agency's request to hand over data stored on those servers. Microsoft is appealing the ruling and has chosen to be in contempt of court while it challenges the court's order.

One of the first questions companies must answer before going into the cloud is whether this will involve the processing of personal data.

3. IMPACT OF ENCRYPTION AND TOKENIZATION ON DATA PROTECTION REQUIREMENTS

In the below sections, each of the key legal challenges mentioned above are assessed from the point of view of a cloud customer applying encryption or tokenization solutions before placing the data into the cloud.

3.1 Key question: does the data I process constitute personal data?

The central question is whether personal data is being processed in the cloud. If one argues that encryption or tokenization make the data effectively anonymous, the data processed in the cloud is no longer personal data, hence the legal requirements in this respect do not apply.

Although the specific circumstances should be assessed on a case-by-case basis, in several jurisdictions in the European Union, for example, the United Kingdom, Spain, Czech Republic, there is a good chance this position can be convincingly defended. The reasoning behind this is that the entity receiving the secured data does not have access to its actual content, and thus cannot reasonably be considered a processor of personal data.

Two elements are important to successfully invoking this position:

- The encryption keys or token mapping tables are securely kept from the receiving third-party entity. CipherCloud's products are based on the storing of the keys or mapping tables exclusively with the cloud customer without access by the cloud provider (or CipherCloud for that matter). This seems a very strong argument to defend this position, at least in the jurisdictions that are favorable towards this argument.
- When data is secured and in this way, the remaining unsecured data does not directly or indirectly allow for the singling out of the individual in question. Guidance and training with respect to the level of encryption or tokenization, as offered by CipherCloud, may offer additional safeguards in this respect.

3.2 What if secured data still constitutes personal data?

In some stricter jurisdictions, there is a possibility that even highly secured data will still be regarded as personal data when stored in the cloud, even though the cloud provider has no possibility to decrypt or de-tokenize the data without access to the keys or mapping table. This stricter interpretation may result from the position held by the Article 29 Working Party ("WP 29"), a European advisory body on data protection laws that issued an opinion on anonymization techniques. In this opinion, encryption and tokenization are categorized as "pseudonymization" techniques which do not result in truly anonymized datasets.

Although these opinions have a certain moral authority, they are not binding for administrative bodies, such as data protection authorities or courts, but are nonetheless followed by some regulators.

In these cases, where the rules on the processing of personal data still apply, the level of legal compliance can nonetheless be increased by using encryption and tokenization techniques. Several supporting points include:

- **Security of personal data:** One of the cornerstones of data protection laws is the **security of personal data** to protect it against accidental or unlawful destruction or accidental loss, alteration or any form of unauthorized access. This obligation is incumbent on the data controller, normally the cloud customer who should take "appropriate" measures, taking into account the current state of the art, cost, the nature of personal data to be protected and potential risks of exposure of such data. Although this analysis implies a balancing test and may further be subject to specific national requirements on the level of security, there are several key features in the products CipherCloud offers its customers to help meet the standard listed below.

- **Protected and locally stored keys:** Many international organizations as well as national regulators emphasize the importance of local storage of encryption keys as an extended security mechanism. This prevents intelligible data in transit or at rest from being disclosed (e.g. by the cloud provider), or being accessed in an illegal manner (e.g. hacking). Additionally, by providing services to its customers such as guidance on protection of keys and integration with third-party tools for key management, CipherCloud helps to obtain a high level of legal compliance in this respect.

- **Added layer of security:** Protecting data before it is stored in the cloud, by encryption or tokenization to a sufficient level, provides an added layer of security that is not in the hands of the processor (here, the cloud provider). This is a recommendation made by the Article 29 Working Party in its opinion on cloud computing.

- **High level of security:** The CipherCloud security solution uses standards-based AES 256-bit encryption and has been certified by independent and reputable institutions, including NIST FIPS 140-2 validation (certificate #2261, October 2014), and the solution meets several industry standards including NIST SP 800-57 standard and Requirement 3 of the PCI Data Security Standard. It is very likely that such certifications will lead to these security solutions being considered to comply with current state of the art.

- **Granular approach to security:** Where a customer can freely and granularly choose which data fields to secure and how to do this (via encryption or tokenization), this allows for fully taking into account the nature of specific data fields and the potential risk of their disclosure.

- **Transfer of Personal Data:** The Data Protection Directive stipulates a strict legal regime on the **transfer of personal data**, essentially prohibiting such transfer to countries outside of the European Economic Area and a list of approved countries (including U.S. Safe Harbor certified companies). If a transfer to other countries is contemplated, adequate safeguards, such as agreeing to model clauses, should be in place or the company should be able to invoke a specific (and exceptional) legal basis. Given that the notion "transfer" is very broad (e.g. encompassing access from a third country to data locally stored on a server in an EEA or approved country), it is clear that in a cloud computing context, it is very likely that such transfers will occur.

- **Local storage solutions:** To provide an answer to these concerns, many non-EU cloud providers offer specific solutions for Europe-based customers by physically storing data on servers located in an EEA (or approved) country. However, given the broad definition of "transfer" and the broad scope of the data transfer rules, such solutions may not offer complete compliance. For example, cloud provider support is often only available from non-EEA countries, and data may be mirrored or backed-up across multiple regions. In addition, the scope of foreign law enforcement agencies may well reach beyond national borders, as is shown in the Microsoft Ireland case, which is discussed further below.

- **Securing the data:** Although the securing of data itself may not offer sufficient compliance with data transfer rules (unless one argues that the data no longer constitutes personal data, see under section 3.1 of this white paper), securing the data may nonetheless offer an additional level of compliance.

  The combination of both local storage and an additional state-of-the-art security layer may provide sufficient arguments of compliance with data transfer rules.

- **Data Proccessing:** Data protection laws state specific legal requirements when **data processing is carried out by a processor** on behalf of a data controller. In essence, the controller must choose a processor providing and complying with "sufficient guarantees" in respect to technical and organizational measures and certain arrangements must be defined in the contract. The inherent fear is that personal data could be shared with third parties who do not always act in good faith.

- **Working with locally applied security solutions:** In a cloud computing context, the provisions on data processing requirements are likely to be relevant in the relationship between the cloud customer and the cloud provider, as well as any sub-processors. Additional requirements may exist when a third-party data security provider processes data on behalf of the cloud customer. However, in the case of CipherCloud, the security provider does not come in direct contact with the data of the cloud customer and these requirements would likely not apply.

- **Extended possibilities for the cloud customer:** Moreover, due to the added layer of security originating from the cloud customer itself, which may result in the cloud provider not being able to decipher or in any way use or misuse the data, the importance of the data processing legal provisions seem to decrease. Remember that in some jurisdictions, the cloud provider for this very reason does not qualify as a data processor as the data is not considered "personal" in the hands of the cloud provider. This may result in extended possibilities for cloud customers to choose appropriate cloud providers.

- **Basis for risk and privacy impact analysis:** Although not specifically stated in the provisions of the Data Protection Directive, one of the main conclusions of the opinion on cloud computing by the Article 29 Working Party is that potential customers of cloud computing services, as a first step, should perform a comprehensive and thorough risk analysis.

  Although this requirement is specifically aimed at the relation between the cloud customer and the cloud provider, a detailed risk assessment in the framework of the purchase of security tools can be a very big step toward compliance with this requirement. Assistance in analyzing which data is being sent to a cloud provider and how use of cloud-stored data is monitored, as CipherCloud offers, would in a documented form, likely be a good basis for compliance with risk analysis and privacy impact requirements.

3.3 Encryption and tokenization vis-à-vis future data protection laws

Context: Technical developments as well as the diverging national implementations of EU data protection laws have resulted in the European legislator reconsidering the current data protection framework. A first step towards a new legal framework was taken when the European Commission presented its draft proposal for a new Data Protection Regulation on the 25 January 2012, directly applicable in all EU Member States. The proposed Regulation, after the European Parliament had adopted its position at first reading, is now proposed to the Council in order for the latter to adopt its position on the amended text. The newly installed European Commission has made it a priority to quickly finalize discussions on this legal instrument.

Many companies are aware that the proposed regulation strongly **increases sanctioning capabilities** in case of infringement of data protection laws, which makes compliance issues ever more important.

How do encryption and tokenization products impact the newly proposed legal provisions?
In addition to the various aspects discussed above, security tools based on encryption and tokenization, as CipherCloud offers, can help companies to make "future-proof" decisions. In the table below some of the cornerstones of the proposed regulation are summarized along with the impact of security tools, such as those offered by CipherCloud.

CORNERSTONE	SHORT EXPLANATION	CIPHERCLOUD IMPACT
1. Data Minimization	This principle indicates that the processing of personal data must be limited to the minimum necessary for the purposes indicated.	Using security products minimizes the amount of personal data sent to the cloud provider, or at least secures the data, minimizing third-party exposure to the data.
2. Data Portability	This is the right to transfer personal data from one electronic processing system into another, while having all data permanently removed from the first system.	The CipherCloud solution provides an effective way to "digitally shred" sensitive information that has been removed from a cloud provider. By destroying old keys, unwanted remnants of encrypted data can never be decrypted.
3. Privacy by Design	Technical and procedural measures should be taken by the controller in order to make sure that the processing, throughout the whole processing lifecycle, complies with the proposed Regulation.	Securing the data certainly helps to establish a privacy-by-design approach as sensitive data is protected by policy and rendered unintelligible for third parties.
4. Privacy by Default	This is the requirement to implement mechanisms in order to ensure that personal data is only processed when necessary for each specific purpose.	The CipherCloud solution can automatically encrypt or tokenize data in specified fields. When new data is added to protected fields, it is protected by default.
5. Privacy Impact Analysis (PIA)	The proposed Regulation provides for the need of a PIA in case the processing presents specific risks.	As stated above, any prior assistance in analyzing data flows, and how cloud services are used, is likely to be a good basis for compliance with a PIA.

4.

BENEFITS OF ENCRYPTION AND TOKENIZATION TECHNIQUES FOR SECURING DATA

Context: As stated, for numerous reasons, the security of data placed in the cloud is a concern for many companies. A key goal is to sufficiently secure data when placing it in the cloud to avoid the risks of data security breaches, business interruptions, commercial loss and reputational damage, as well as breaches of applicable laws, such as data protection laws or sector-specific laws, or contractual obligations

Using encryption and tokenization techniques: There are no generic security laws that apply specifically to cloud services, although it should be stated that local requirements may likely apply. Therefore, it is often up to the customer to verify which security measures are offered in practice by a particular cloud provider and whether these measures are sufficient.

We have indicated though that several standards are available and that the certification of compliance with such standards will likely signify that a company is at least using state-of-the-art techniques, which brings it a step closer to compliance. We see a number of advantages in using security tools within the organization before placing data in the cloud:

- In essence, such solutions provide for an additional layer of security. Where the legal provisions go beyond merely selecting a cloud provider offering sufficient security measures (such as when processing personal data or complying with industry-specific laws, e.g., in the financial sector), the **cloud customer in this case runs the extra mile** itself by first proactively securing the data before sending it into the cloud. This is a very strong argument from the viewpoint of data security.

- Further, tools which allow the customer to **locally and safely store** the encryption keys or token mapping table, such as CipherCloud's, offer additional security that decreases the number of entities that can restore the secured data to its original state. This offers protection against any kind of unauthorized access or leak of the data as it will be extremely difficult for any third entity to make the data intelligible.

- All these arguments self-evidently depend on the **quality of encryption or tokenization**, including types of algorithms used, the length of the encryption key, and the methods for securing keys. As such, we note that the CipherCloud security solution uses standards-based AES 256-bit encryption and has been certified by independent and reputable institutions, including NIST FIPS 140-2 validation (certificate #2261, October 2014), and the solution meets several industry standards including NIST SP 800-57 standard and Requirement 3 of the PCI Data Security Standard.

5.

ACCESS TO DATA BY FOREIGN LAW ENFORCEMENT AGENCIES

Context: The issue of foreign governments potentially accessing sensitive data in the cloud, either openly through court orders or administrative request or in secret, is a major issue for many companies that deal with large amounts of sensitive data.

It should be noted that this issue has a broader scope than personal data as the concern exists for any kind of business-critical information.

These considerations first come into play where data is stored outside of the EU and local law enforcement agencies may undertake certain actions. However, even when data is kept on servers within the EEA territory, without "transferring" the data in any way to a third party located in territories not offering an adequate level of protection (cfr. above), protection from requests of foreign enforcement authorities may still not be adequate. This was demonstrated very recently by the Microsoft Ireland judgment, mentioned previously. In this case it was ruled that even though data was stored on servers located outside of the United States (in this case Ireland), Microsoft was still obliged to comply with a US law enforcement agency's request to hand over data stored on that server. It indicates that the risks in this respect are not theoretical.

Securing data before placing it into the cloud: Securing data through encryption or tokenization before placing it into the cloud largely offers an answer to this legal barrier for companies that are considering adopting cloud solutions.

By ensuring that the cloud provider who would be requested to hand over data, (or might even be unaware that the data is being processed), does not have the keys to convert the data in its original state, the cloud customer can make sure that the data is to some extent protected against government intervention. As only the cloud customer holds the keys, it would require cooperation from the cloud customer to have access to intelligible data.

Securing data through encryption or tokenization before placing it into the cloud largely offers an answer to this legal barrier for companies that are considering adopting cloud solutions.

6. KEY TAKE-AWAY POINTS

Secured data may not constitute personal data
In some jurisdictions, sending sufficiently secured personal data (that cannot link to, or single out an individual) to a cloud service provider does not constitute processing of personal data, if the cloud provider does not have access to the key to decrypt the data. This results in data protection rules not being applicable in those jurisdictions.

High-level of overall security compliance
Even in cases where the use of cloud-based services is considered to fall under the scope of data protection laws, encryption and tokenization solutions as offered by CipherCloud can help achieve compliance on a number of legal requirements. These solutions can offer a high level of compliance for the security of personal data through local storage of encryption keys (or token mapping tables) and a granular and layered approach to securing sensitive data. In addition, these solutions can complement local storage offered by cloud providers in addressing cross-border transferring of data outside of the EEA, and can help organizations in carrying out privacy impact analyses of cloud providers.

Future-proof technology for proposed DPR
Moreover, CipherCloud solutions seem to offer a future-proof answer in relation to several new cornerstones of the proposed Data Protection Regulation, including data minimization, data portability, privacy by design and default, and privacy impact analysis.

Compliance with general security requirements
Encryption and tokenization as offered by CipherCloud helps companies in complying with general data security requirements, be it personal data or not. Compliance with several standards and the third-party certification indicates that the solutions offered are likely to be considered compliant with the current state of the art.

Protection against forced disclosure
Encryption and tokenization solutions, based on the local storage of the key and mapping table, help protect data from being seized or otherwise accessed by foreign law enforcement agencies. Such a demand, in principle, would require the cooperation of the cloud customer to allow access for such agencies to the data under investigation. This further protects companies against foreign authorities who may have no judicial competence over the cloud customer.

ABOUT DLA PIPER

DLA Piper is a global law firm with 4,200 lawyers located in more than 30 countries throughout the Americas, Asia Pacific, Europe and the Middle East.

DLA Piper's technology practice has deep industry sector experience, that allow us to provide valuable practical advice and innovative solutions over and above our first rate base of technical know-how. Our practice counts many of the world's largest high profile IT as clients.

More information is available at **www.dlapiper.com**.

ABOUT THE AUTHOR

Professor dr. Patrick Van Eecke is Partner at DLA Piper's Brussels office and head of the Internet law group. He is a specialist in data protection, new technologies, cyber security laws as well as e-commerce and e-government. He is extensively involved in diverse research and consulting projects for the European Commission, international bodies and several national governments, including the European Commission and the United Nations.

Patrick has been named Belgium's leading lawyer and is ranked in the world's top 20 IT lawyers in the "Guide to the World's Leading Technology, Media & Telecommunications Lawyers." Patrick is also recommended by the Legal 500 and Chambers as one of the top legal advisors in Brussels.

Patrick teaches IT law at the University of Antwerp, at King's College and Queen Mary University in London, United Kingdom. He is the author of diverse legal articles and books on (among others) new technologies, privacy, computer crime and cyber security and he is a regular speaker on national and international conferences.

ABOUT CIPHERCLOUD

CipherCloud provides industry-leading cloud visibility and data protection solutions, enabling enterprises to adopt the cloud while ensuring security, privacy, compliance and control. Based in San Jose, California, with offices globally, CipherCloud supports major enterprises in 25 countries in a wide range of regulated industries including financial services, healthcare, telecommunications, technology and government.

More information is available at **www.ciphercloud.com**.

CipherCloud™
Trust in the Cloud