

July 2018

Extraterritoriality and personal data protection

How to acquire good
legal instincts



This document is the property of the law firm Mathias Avocats. Any reproduction and/or representation is subject to the prior consent of the firm Mathias Avocats and to provisions of the French Intellectual Property Code.

TABLE OF CONTENTS

INTRODUCTION	05
SHEET 1 : THE CLOUD ACT	07
SHEET 2 : THE GENERAL DATA PROTECTION REGULATION	11
SHEET 3 : THE PRIVACY SHIELD	13
SHEET 4 : THE FOREIGN INTELLIGENCE SURVEILLANCE ACT	16
SHEET 5 : THE USA FREEDOM ACT	19
SHEET 6 : THE DATA PROTECTION AND PRIVACY AGREEMENT (UMBRELLA AGREEMENT)	21
SHEET 7 : THE HAGUE CONVENTION OF 1970	23
SHEET 8 : BLOCKING STATUTE	25

SHEET 9 : THE TRADE SECRET DIRECTIVE	27
SHEET 10 : WHAT ISSUES MUST BE CONSIDERED DURING (e)DISCOVERY ?	30
SHEET 11 : WHAT TO CHECK BEFORE ENTERING INTO CLOUD COMPUTING AGREEMENT ?	32
SHEET 12 : WHAT ARE BCRs ? HOW CAN THEY BE USED FOR DATA TRANSFERS ?	34
SHEET 13 : HOW TO DRAFT CONTRACTUAL CLAUSES WITH A PARTY ESTABLISHED IN THE USA ?	37

INTRODUCTION


What does the term extraterritoriality cover? It refers to the application of a law outside the borders of the legislating country or to the extended competence of said country's jurisdiction. Originally, extraterritoriality emerged in international law to exempt certain diplomatic (moral or physical) persons operating in a foreign country from the jurisdiction of the host country. The persons instead stay accountable to the law of their native country.

The term has since evolved and covers a broader scope (ex: criminal law, civil law, surveillance, etc.). Its development has also led to the emergence of various issues such as overlapping and/or conflicting laws or uncertainty as to obligations and liabilities.

This White paper focuses on the issues extraterritoriality raises regarding the protection of personal data and transfers of such data. The international dimension of the protection of personal data raises certain questions in particular with regard to the sovereignty and compatibility of the various worldwide legislations. These questions are essential considering the trade flows and globalization movement of data and more particularly pertaining to the transfer of personal data. It must be underlined that the conception and approach to the protection of personal data greatly varies from one country to another.

A clear dichotomy can be drawn between the United States and the European Union. The former uses a sectoral approach that relies on a mix of legislations, regulations, and self-regulations whereas the European Union has set up a common framework through Directives and Regulations. There are very few federal laws regulating the protection of personal data in the United States which leads to a patchwork of legislations and a lack of visibility and transparency.

Furthermore, as will be further developed through this White paper, the United States has a very broad approach and holds an element of extraterritoriality which directly impacts the regulations on the protection of personal data. Indeed, the notion of territorial jurisdiction is broadly interpreted which in turn implies that American regulations may apply in other countries. Nonetheless, European Union law also holds an element of extraterritoriality in the sense that the GDPR seems to edge towards the American conception considering its broad territorial and material scope. It must be underlined that the GDPR may apply to entities established in the United States. What happens when laws overlap? Can they interact in an effective way or must one trump the other? This can lead to the issues discussed above.



Another point to keep in mind is the duality of cultures between the United States and the European Union. The coming into effect of the General Data Protection Regulation ([regulation n° 2016/679](#)), also called the GDPR, highlights the duality between the United States and the EU. For example, medical information or social security numbers are considered as personal data in the United States whereas, in the EU, such data would be considered as sensitive and benefit from a reinforced protection. In addition, the latter holds 28 Members States and implies an inherent transfer of sovereignty to the European Union. Although the same could be argued regarding the Federal and States' governments in the United States, the situation differs. Indeed, in the European Union, and in many other countries, this implied transfer of sovereignty means that their national laws may be constrained by international commitments and thus subject to international negotiations. Traditionally, the United States has been very reluctant to accept legally binding international commitments and has adopted a strong external legal policy. The country feels in some ways entitled to intervene abroad and impose its rules. For example, if we consider the GDPR, its aims at harmonising the laws and rules applicable to the protection of personal data. It seeks to

strengthen protection of data subjects within its borders. On the other hand, the United States has a patchwork of legislations which often holds an intent to collect the most data possible at the extent of the protection of data subjects. There have also been quite a few tensions between the European Union and the United States regarding the protection of personal data. They will be further developed in this White paper.

Mathias Avocats has analysed the momentous pieces of legislation on the protection of personal data on both sides of the Atlantic illustrating the extraterritoriality. The firm has also drafted practical sheets on the subject.

We hope you enjoy the reading and that this article will be useful for your projects.

Garance Mathias

Avocat à la Cour



Sheet 1 - The Cloud Act

What is it?

The Clarifying Lawful Overseas Use of Data Act, also called the [Cloud Act](#), was passed in 2018 in the United States as part of the [Consolidated Appropriation Act \(2018\)](#) which is the omnibus spending bill necessary to avoid government shut-down. The Act states that it namely aims at improving “law enforcement access to data stored across borders”. To achieve this goal, the Cloud Act modifies and brings up to date the [Stored Communication Act \(SCA\)](#).

In addition to modernizing the SCA, the Cloud Act was implemented in response to the [Microsoft v. United States case \(2013\)](#). The question raised in the latter was whether the United States Government could access data stored abroad. The Cloud Act settles the issue: the Government has the power to access data stored outside of the United States. The case was considered as moot by the United States Supreme Court and therefore [vacated](#). Indeed, the Government obtained a new warrant under Section 2703 of the Cloud and the parties agreed that the new warrant had replaced the original one.

What's its purpose?

Following the Microsoft case, the Cloud Act aims at setting up a comprehensive framework for data exchanges between the United States and other

foreign governments as well as expanding the United States Government's reach to data stored abroad. For these reasons, it has implemented two significant changes: executive agreements and a broader disclosure requirement for providers of electronic communication services or remote computing services.

It must be stressed that the Cloud Act can apply to providers of electronic communication services or remote computing services which are not based in the United States or do not operate in the United States. It furthermore applies to United States and non-United States persons. Indeed, when the Government requests disclosure of personal data by providers of electronic communication services or remote computing services, the Act does not specify that the request must concern a United States person. It is reasonable to assume that non-United States persons are also concerned. It thus has an immense extra-territorial scope.

What are the key points?

As previously stated the Cloud Act amends the SCA. Both Acts apply to [providers of electronic communication services](#) or [remote computing services](#). They thus apply to any company or individual providing electronic services including computer storage, transfer of signs, signals, writing and so forth transmitted in whole or in

part by electronic means (ex: Google, Snapchat, Facebook). This implies that all non-electronic services or computing activities are outside their scope (ex: oral communications).

The SCA imposes a general obligation of non-disclosure on service providers. Nonetheless, under [Section 2703 of Chapter 18 of the United States Code](#) (18 U.S. Code) providers of electronic communication services are required to disclose the contents of a wire or electronic communication to governmental entities upon their request. The Cloud Act expands this exception with the new [Section 2713](#) which states that providers of electronic communication services or remote computing services must comply with their obligations, namely to disclose the information pertaining to a customer, whether the information “is located within or outside the United States”. Therefore, the Government will be able to access data stored or collected outside of the United States.

It must however be underlined that providers of electronic communication services or remote computing services may challenge the Government’s request for disclosure by filing a motion to modify or quash the legal process ([§2703, h\) of the Cloud Act](#)). This action is limited to customers or subscribers which are non-United States persons and do not reside in the United States. The providers have a restricted remedy.

Executive agreements ([2523 of the Cloud Act](#)) are the other crucial change brought by the Cloud Act. Under this section, the President of the United States may enter into an executive agreement with a qualifying foreign government. The agreement would allow providers of electronic communication services or remote computing services to disclose their customers’ data to the foreign government. Under the SCA, the providers were generally prohibited from complying with a request from foreign governments.

In sum, executive agreements enable foreign governments to directly request data of a non-United States person if they can comply with the [numerous requirements](#) under Sections [2703 of the Cloud Act](#) and [2523 of the Cloud Act](#). It must be underlined that the foreign government’s request must only be for “the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism” and not intentionally target a United States person. For requests concerning United States persons however, the foreign government will have to use the [Mutual Legal Assistance Treaty](#) (MLAT) process or obtain assistance in a criminal investigation or prosecution ([28 U.S. Code §1782](#) and [18 U.S. Code §3512](#)).

It would appear that the requirements for executive agreements and to be considered as a “qualifying foreign government” greatly impede on the

foreign government's power. Unless certain conditions are met, executive agreements are off the table. Furthermore, the Government of the United States is merely required to make a disclosure request for data stored abroad and the latter does not necessarily have to concern a United States person. These rigorous conditions create a clear unbalance of power between the United States and other countries.

What are the drawbacks?

The main issue arising from the implementation of the Cloud Act is its compatibility with the European Union's General Data Protection Regulation or GDPR ([regulation n°2016/679](#)).

A first point of contention seems to arise from the disclosure obligation of the providers of electronic communication services or remote computing services, on request of the United States Government, regarding any record or information pertaining to a customer or subscriber whether the record or information is located in the United States or abroad ([§2713 of the Cloud Act](#)). The Cloud Act offers no remedy for European data subjects and the latter won't be informed of the communication and access to their data. This is in complete opposition with the GDPR.

The other point of contention arises from data transfers, either through executive agreements or the disclosure request described above. It is unclear whether either one of the dispositions provides sufficient protection

and guarantees under [Articles 44 to 50 of the GDPR](#).

More specifically Article 48 of the GDPR states that "any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State". The Cloud Act does not seem to fit this definition. It is not an international agreement and there was no consultation with the European Union (EU) beforehand.

So, what does this imply for the interaction between the GDPR and the Cloud Act? Which law will providers comply with? Practitioners have not reached a consensus on whether both pieces of legislation are compatible. It is still unclear how they will interact in practice.

These questions are all the more important in practice considering the economic and political value of data. Governments want to keep an eye on what is happening in the digital world. Considering the GAFA (Google, Apple, Facebook and Amazon)'s power, it can be assumed that United States based companies hold most of the data worldwide. This creates a certain unbalance in powers between the United States and other governments such as the EU. How do the Cloud Act and GDPR influence this balance? Some Member States of the EU are already

worried such as France. A French deputy sent a [written question](#) to the French Prime Minister regarding the consequences the Cloud Act on the French people's privacy and the remedial measures which will be taken on a national and European level for personal data and privacy protection. The question has not yet been answered.



Sheet 2 - The General Data Protection Regulation

What is it?

[Regulation n°2016/679](#) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, called the GDPR, came into force on May 25th, 2018.

It repealed [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. The Directive was in need for modernization. It was adopted in 1995, when the Internet was just in its infancy. The GDPR incorporates the recent technological evolutions. Furthermore, the Directive led to a fragmentation in the implementation of data protection across the EU. The GDPR aims at homogenizing the level of protection.

The coming into force of the GDPR created its own international commotion similarly to the Cloud Act. It significantly changed the legal landscape of personal data protection in the EU as explained in this White paper.

What's its purpose?

As explained above, the GDPR aims at harmonizing the current legal framework and increasing legal certainty. [Recital 2 of the GDPR](#) states that the Regulation "is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and


the convergence of the economies within the internal market, and to the well-being of natural persons".

What are the key points?

The scope of the GDPR is a cornerstone of the Regulation's strength. Indeed, it broadly applies to all types of processing activities ([Article 2 of the GDPR](#)). More importantly however, under [Article 3 of the GDPR](#), it has a significant extraterritorial scope seeing as it applies to:

- Data controllers or processors established in the EU regardless of whether the processing takes place in the EU; and
- Data controllers or processors not established in the EU when their processing activities concern the personal data of data subjects who are in the EU and the processing activity is related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union or the monitoring of their behaviour as far as their behaviour takes place within the Union.

This broad scope can be compared to that of the Cloud Act or generally to the extraterritoriality of United States legislation seeing as the GDPR applies well beyond the borders of the EU.



Despite the numerous changes brought by the GDPR, the latter takes up the core principles set out in the Directive 95/46/EC. The principles are set out in [Article 5 of the GDPR](#) and are as follows: (i) lawfulness, fairness and transparency; (ii) purpose limitation; (iii) data minimization and accuracy; (iv) storage limitation and (v) integrity and confidentiality. These principles are minimum requirements for any personal data processing activities.

Another prominent issue are transfers. [Articles 44 to 50 of the GDPR](#) lay out the requirements for the latter. As a general rule, transfers of personal data will be allowed if the conditions defined in the GDPR are respected by the controller or processor. In other words, if a transfer does not fall within one of the categories of the GDPR, it will be considered as a violation of the applicable legislation.

What are the drawbacks?

The GDPR aims at harmonizing the framework for personal data protection in the EU as well as providing a unified level of protection. Companies and public bodies will henceforth be subject to the same obligations whereas individuals will benefit from an equivalent protection in all Member States. A harmonized legal framework allows for an easier flow of business and keeps international business partners in check. To some extent, it has

succeeded. It should nonetheless be kept in mind that Member States have some leeway and that cooperation amongst them will be necessary to achieve a unified framework.

Transfers are one of the main bones of contention between the Cloud Act and the GDPR. The former does not seem to fall in any of the categories stated above. It does not appear to provide appropriate safeguards seeing as European data subjects will not be informed of the communication and access to their data and have no remedy against the United States Government's decision. The Cloud Act has also not been recognized as providing an adequate level of protection for an adequacy decision. However, [Article 49 of the GDPR](#) may offer a possibility: could executive agreements be considered as "necessary for important reasons of public interest" and thus fall under the exceptions of Article 49 of the GDPR?

Furthermore, the Regulation's extra-territorial scope leads to similar questions concerning the extraterritorial scope of United States legislation. What law will apply in the event of a conflict? How will the GDPR and the Cloud Act interact? Which law must providers comply with?



Sheet 3 - The Privacy Shield

What is it?

The Privacy Shield is a self-certification mechanism for companies established in the United States. It has been recognised by the European Commission as providing an adequate level of protection for personal data transferred by a European entity to companies established in the United States. It is a framework for personal data transfers of European data subjects to organisations in the United States for commercial purposes.

What's its purpose?

The first adequacy decision between the EU and the United States, adopted the 26th of July 2000, for transfers from the former to the latter was the [Safe-Harbor Framework](#). Entities based in the United States could voluntarily comply with the Safe-Harbor Framework's requirement to become eligible for transfers from the EU. It was however invalidated a few years later by the Court of Justice of the EU in the case Maximillian Schrems v. Data Protection Commissioner ([C-362/14, 6th of October 2015](#)). Following this decision, data transfers to the United States were no longer considered as transfers to a country offering "adequate personal data protection".

The situation was quickly resolved with the adoption of the [Privacy Shield](#) by the EU and the United States on


July 12th, 2016. It became operational as of August 1st, 2016.

What are the key points?

For organisations to comply with the Privacy Shield, they must comply with the Principles (ex: the notice principle which requires organisations to provide certain information to data subjects, the security principle under which organisations must take reasonable and appropriate security measures considering the risks involved with the processing, data minimisation, etc.). These requirements ensure a similar level of protection for the personal data of European data subjects on both sides of the Atlantic.

It must be underlined that the Principles are similar to those of the Safe Harbor. Nonetheless, the Privacy Shield expands the compliance obligations and liability. For example, companies must provide "clear and conspicuous" privacy policies that contain at least 13 enumerated items of information about the company, its data processing, and the consumer's rights under the Privacy Shield. Data subjects' rights are also enhanced. They now have several remedies and can lodge an Alternative Dispute Resolution body, a National Data Protection Authority, the Department of Commerce, the Federal Trade Commission or a Privacy Shield Arbitral Panel.

In the United States, the Principles were issued by the Department of



Commerce under its statutory authority to “foster, promote, and develop international commerce” ([15 U.S.Code § 1512](#)). The Federal Trade Commission and the Department of Transportation have also made representations.

An entity based in the United States must self-certify on the [Department of Commerce’s website](#) and publicly commit to comply with the Privacy Shield’s requirements. While joining the latter is voluntary, once an eligible organisation makes the public commitment to comply with the Privacy Shield’s requirements, the commitment will become enforceable under United States law.

In order to help professionals, the European Commission published a [Guide to the EU-U.S. Privacy Shield](#). It outlines the Principles or requirements which companies based in the United States must comply with to be considered as “Privacy Shield companies”. They must renew their “membership” to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework. It must be underlined that companies which no longer comply with the Framework must return or delete the data they have.

What are the drawbacks?


The main drawback recently appeared when the European Parliament pub-

lished a [press release](#) calling into question the Privacy Shield. It resulted from the [Civil Liberties Committee’s](#) call on the Commission to suspend the Privacy Shield on the grounds that it fails to provide enough data protection for European Union citizens. It namely invoked the [Cloud Act](#) and the [Facebook-Cambridge Analytica scandal](#).

The Privacy Shield may be suspended unless companies based in the United States comply with it by September 1st, 2018. The full House is expected to vote on the resolution in July. If the Privacy Shield were to fall, companies would once again have to turn to Binding Corporate Rules or standard data protection clauses. This would be a significant issue considering the important flow of commerce between the European Union and the United States.

In the event that the Privacy Shield is maintained, another question arises regarding its compatibility with the Cloud Act. The mechanism provided for in the Privacy Shield only covers personal data transfers to companies based in the United States which have self-certified as fully adhering to the principles contained in this agreement, not government entities.

Furthermore, it may be argued that the Privacy Shield does not address the mass surveillance system of United States security agencies. How can European data subjects enforce their rights? Could amendments be made?



‘The Privacy Shield may be suspended unless companies based in the United States comply with it by September 1st, 2018.’

Sheet 4 - The Foreign Intelligence Surveillance Act

What is it?

The [Foreign Intelligence Surveillance Act](#) (FISA Act) was adopted in 1978. It was a direct consequence of the 1972 case [United States v. United States District Court \(407 U.S. 297\)](#). The Government had placed wiretaps on the defendants - who were planning to bomb a Central Intelligence Agency office - without obtaining a warrant and argued that they were nonetheless lawful as a reasonable exercise of presidential power to protect national security.

The United States Supreme Court did not agree on the grounds of the 4th Amendment prohibiting unlawful searched and seizures. It however recognized that a different standard than a warrant may be required for domestic intelligence surveillance: "Given these potential distinctions between [Wiretap statute] criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes [under the Wiretap statute]. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens".

What's its purpose?


The FISA Act creates a separate legal regime for foreign intelligence surveillance by United States agencies. Both electronic surveillance and physical searches of foreign powers and agents are covered. It must be underlined that the Act was recently amended in January 2018 and namely extended [Section 702](#) for the following six years.

The Act also sets up a Foreign Intelligence Surveillance Court (FISC) which entertains applications made by the United States Government for approval of electronic surveillance, physical searches, and certain other forms of investigative actions for foreign intelligence purposes.

What are the key points?

Section 702, which is codified under [50 U.S. Code § 1881a](#) relating to the procedures for targeting certain persons outside the United States other than United States persons, is at the heart of the FISA Act.

Under [50 U.S. Code § 1881a \(a\)](#) the "Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information". The following paragraph ([50 U.S. Code § 1881a \(b\)](#)) restricts the above-mentioned rule



to non-United States persons. For example, it holds that “an acquisition authorized under subsection (a) may not intentionally target a United States person reasonably believed to be located outside the United States”.

This provision is often used for cloud computing and gives United States law enforcement agencies a broad scope of action. They may collect and access information and data of non-United States persons without having to make a request to the foreign government. The FISA Act is a clear affirmation of the extraterritoriality of the United States legislation.

It must also be underlined that for United States persons’ communications to be targeted, there needs to be some level of suspected involvement in criminal activity whereas this is not the case for non-United States persons.

Furthermore, the Act has codified the “abouts” practices under [50 U.S. Code § 1881a \(m\) \(4\)](#). “Abouts communications” are communications that contain a reference to, but are not to or from, a target. Entities thus legally have access to information and data concerning United States persons. As Snowden [revealed](#), these practices are not new. This section expands and reinforces the United States’ access to data abroad and within its borders.

What are the drawbacks?

The FISA Act has sparked much controversy. Several civil liberties organizations, and namely the [American Civil Liberties Union](#), have argued that the use of Section 702 is unconstitutional. They namely invoke the important number of Americans whose communications have been collected without 4th Amendment guarantees.

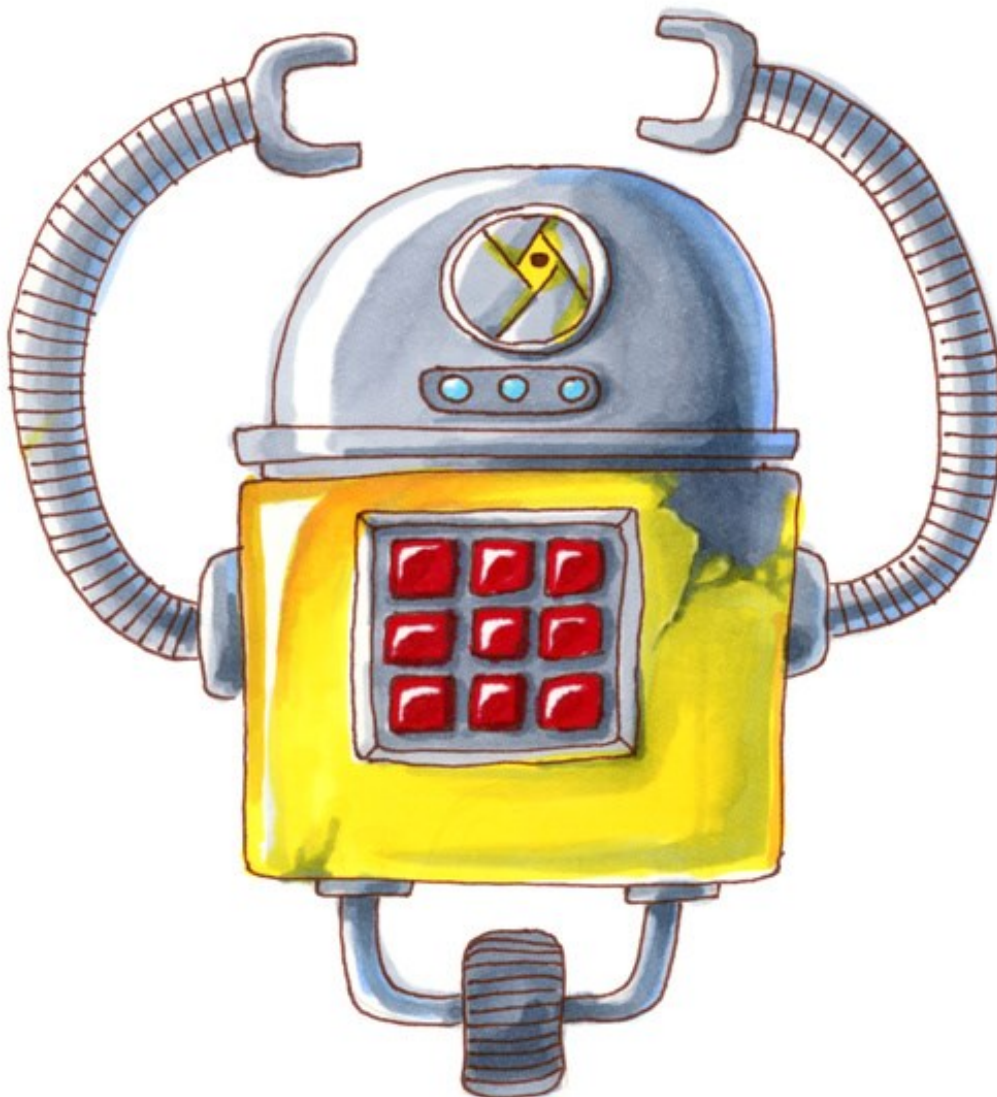
Under the 4th Amendment, a warrant must be specific. This implies that it must be based on probable cause – supported by Oath or affirmation - or particularly describe the place to be searched or the persons or thing to be seized. This is not the case under Section 702 and it seems to directly violate United States persons’ rights.

Regarding non-United States persons, questions may be raised regarding their expectation of privacy and the protection of their personal data. Indeed, systematic surveillance under the FISA Act would go against the principles of the GDPR.

Furthermore, FISA orders imply data transfers. The later are only be allowed in specific instances under the GDPR ([Articles 44 to 50 of the GDPR](#)). The FISA orders don’t seem to fall under any category.

More specifically under [Article 48](#) states that “any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may

only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State". No international agreement was negotiated before the extension of Section 702 of the FISA Act and the European Union wasn't consulted beforehand. It remains to be seen if actions will be taken in practice.



Sheet 5 - The USA Freedom Act

What is it?

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ([USA PATRIOT Act](#)) was implemented in 2001 shortly after the September 11, 2001 terrorist attacks. As shown in the title, its aim was to prevent and fight against terrorism. For this purpose, it amended the [FISA Act](#) namely to expand surveillance to individuals not directly linked to terrorist groups. The Act also covered a broad range of subjects other than surveillance such as border security, detention of immigrants or funding for counter-terrorism. The USA PATRIOT Act sparked controversy and was set to expire in 2015.

The Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act ([USA FREEDOM Act](#)) was enacted in 2015 to extent the USA PATRIOT Act's provision, in whole or in part, until 2019. It however introduces several changes such as strengthened scrutiny on the Government or United States law enforcement agencies (ex: Federal Bureau of Investigation, National Security Agency, etc.) and transparency. The modifications are, in part, a result from [Snowden's revelations](#) regarding the National Security Agency (NSA)'s collection of information and data in 2013.


What's its purpose?

The USA FREEDOM Act aims at establishing a more stringent framework for surveillance of United States and non-United States persons as well as the collection of information and data namely under the FISA Act. It further seeks to establish adequate and reliable safeguards.

What are the key points?

Under the USA PATRIOT Act, law enforcement agencies could collect business records and other data on the condition that the data was "relevant" to national security. The USA FREEDOM Act changes this standard. Law enforcement agencies' applications for said data must now include a "specific term" which is defined as "a term that specifically identifies an individual, account, or personal device" ([50 U.S. Code § 1861\(k\)\(4\)\(B\)](#)). The agency must also show that the entity or person – whose data is sought – is associated with a foreign power or terrorist group. The new standard seeks to limit the agencies' power and the extraterritoriality of legislations. It must be underlined that the agencies can request the information and data of United States persons and non-United States persons.

The replacement of "relevant" with "specific term" also puts an end to bulk collection. The latter can be defined as a large-scale collection (ex: State, zip



code, Internet domain, etc.). The prohibition of bulk collection is clearly stated in [Sections 103, 201 and 501 of the USA FREEDOM ACT](#). It is prohibited for tangible things, such as business records, pen registers and trap and trace devices and National Security Letters (NSLs). To the extent that European citizens may participate in calls or electronic communications with United States persons, they benefit from this new rule. Unless the law enforcement agency specifically identifies the non-United States person or another specific selection term referring to the latter is determined, the non-United States person's data cannot be collected.

Another important change concerns NSLs. They are administrative orders that are sent to compel the recipients to provide information to federal investigators. The USA FREEDOM Act still holds the principle of non-disclosure for recipients of the letters. As such, they are prohibited from saying that they were compelled to provide information to federal investigators. The USA FREEDOM Act nonetheless introduces certain exceptions under [18 U.S. Code § 2709 \(c\) \(2\)](#) (ex: the disclosure is made to an attorney to obtain legal advice or assistance regarding the law enforcement agency's request). NSLs can also be challenged immediately whereas, under the USA PATRIOT Act, a person had to wait a year.

What are the drawbacks?

Despite the protective steps taken by the USA FREEDOM Act, it does not reform the surveillance authority of [Section 702 of the FISA Act](#). United States law enforcement agencies thus still have a broad scope of action and may collect and access information and data of non-United States persons without having to make a request to the foreign government.

Furthermore, it does not take into consideration the principles or requirements of the GDPR if a non-United States person is a European citizen. The latter has reinforced rights namely regarding information. If a provider cannot disclose the request of a United States law enforcement agency regarding the information of a European data subject, there is a potential violation of the European data subject's rights. How is the provider to manage? Which law should it apply? And what remedy does the non-United States data subject have?

Sheet 6 - The Data Protection and Privacy Agreement (Umbrella Agreement)

What is it?

Negotiations regarding the Agreement between the United States and the EU on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses ([Umbrella Agreement](#)) began in [March 2011](#).

The Agreement was finally signed in June 2016, according to the European Commission's [press release](#) and it was [published](#) in the Official Journal of the EU on December 10th, 2016. It entered into force on 1 February 2017.

In a few words, the Umbrella Agreement was adopted to facilitate the sharing of personal data between the EU or one of its Member States and the United States in relation to the prevention, investigation, detection or prosecution of criminal offenses, including terrorism.

What's its purpose?

The Umbrella Agreement aims at establishing a lasting legal framework to facilitate the exchange of information, which is critical to prevent, investigate, detect and prosecute criminal offenses, including terrorism. It furthermore sets an elevated level for the protection of personal data of European citizens.

What are the key points?


It is important to note that the Umbrella Agreement covers all personal data (ex: names, addresses, criminal records, social security numbers, etc.) and exclusively personal data transfers between the Competent Authorities of the United States and the EU for judicial cooperation.

Indeed, the purpose of the transfer, use and re-use of such data is limited solely to the prevention, investigation, detection and prosecution of criminal offences, including terrorism ([Articles 1 and 6 of the Agreement](#)).

The Competent Authorities are defined in [Article 2 \(5\) of the Umbrella Agreement](#) as "national law enforcement authorities responsible for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism". The scope of the Agreement is thus quite broad while remaining limited to a specific purpose or use of said data: the prevention of crime.

For further transfers, the Competent Authority originally sending the information must consent to the transfer to a third party ([Article 7 of the Umbrella Agreement](#)). This ensures better security and visibility. It should also be noted that quality requirements for the data transferred are set out in the Agreement.

Regarding security, [Article 9 of the Umbrella Agreement](#) states that the



United States and the EU “shall ensure that they have in place appropriate technical, security and organizational arrangements for the protection of personal information”. The risks against which the personal data must be ensured are destruction, loss, unauthorized disclosure, alteration, access or other processing. The notification of security incidents must moreover be organised between the parties.

For European citizens, the Umbrella Agreement holds two significant rights: the right of access to their data and a right to rectify data that are inaccurate or processed in an improper manner. Furthermore, European citizens will benefit from equal treatment. Indeed, under the [Judicial Redress Act of 2015](#), European data subjects may exercise administrative or judicial remedies in the United States when the United States authorities have denied them access or rectification, or have unlawfully disclosed their personal data.

The Umbrella Agreement clearly states that it “supplements” but does not replace provisions regarding the protection of personal data in international Agreements between the United States and the EU ([Article 5 of the Umbrella Agreement](#)).

What are the drawbacks?

Despite the advancements of the Umbrella Agreement, the rights to remedy

of European citizens are quite limited. It only sets up two rights for violations of the [United States Privacy Act of 1974](#). What about all the other rights provided for in the GDPR such as the right to erasure or to restriction? What about misuses of the personal data by Federal agencies in the United States?

Moreover, the security requirements remain vague. What measures should be implemented? Will they be regularly reviewed or audited? How can one be sure that the security measures are equivalent to those required by the GDPR?



Sheet 7 - The Hague Convention of 1970

What is it?

The [Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters](#) or Evidence Convention was concluded on March 18th, 1970. It now has [61 Contracting Parties](#) which include most Member States of the EU. In a few words, the Convention seeks to harmonize the competing interests of the Contracting Parties in the context of evidence cross-border legal proceedings.

What's its purpose?

The Evidence Convention aims at establishing methods of co-operation for the taking of evidence abroad in civil or commercial matters. It has set up two methods which we will discuss below: Letters of request and diplomatic or consular agents and commissioners. The purpose of these methods is to simplify the obtention of evidence on an international level and namely adapt evidence procedures to both civil and common law systems.

The Convention further provides for a specific pre-trial discovery rule. [Discovery](#) is a process specific to common law countries. Although discovery procedures also exist in civil law systems, it does not play such a crucial role. In common law countries, it is up to the parties to engage in discovery and the judge will weigh the evidence presented whereas in civil law countries, the judge will investigate the facts of the

case and make her own discovery. In civil law countries, discovery is within the judge's tasks. The pre-trial discovery rule provides for effective means of overcoming the differences between civil law and common law systems regarding the taking of evidence.

What are the key points?

As the term implies, Letters of requests are requests from one Contracting Party to another to obtain evidence or to perform some other judicial act. However, the request must be for evidence which is "intended for use in judicial proceedings, commenced or contemplated" ([Article 1 of the Evidence Convention](#)). Evidence can only be asked if it is related to a case to be brought in front of a court or the appropriate authority.

The Letter must specify certain elements such as the names and addresses of the parties to the proceedings and their representatives (if any), the evidence to be obtained or other judicial act to be performed and documents or other property (real or personal) to be inspected ([Article 3 of the Evidence Convention](#)). A model Letter of request is [available](#) for Contracting Parties.

Regarding diplomatic officers or consular agents, they may take evidence (ex: testimony, documents, etc.) in another Contracting Party than the one they are from. However, the taking of said evidence may be subject to the

prior permission of the appropriate authority of the State in which the evidence is to be taken ([Article 15 of the Evidence Convention](#)). States are free to exclude this option or whole or in part ([Article 33 of the Evidence Convention](#)). In practice, it is crucial to check whether a State has made a declaration on this option.

Finally, [Article 23 of the Evidence Convention](#) governs the obtention of pre-trial discovery documents. The pre-trial discovery covers requests for evidence submitted after the filing of a claim but before the final hearing on the merits.

The Article states that “a Contracting State may at the time of signature, ratification or accession, declare that it will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries”. The United States has clearly opted for this reservation. In turn, this leads to the United States Supreme Court forsaking the Evidence Convention. Indeed, as early as 1978, it [held](#) that the Hague Convention was merely an option. The non-application of this Convention therefore leads to a pre-eminence of the discovery procedure. However, failure to provide evidence, whether tangible or intangible, can have a very negative impact on the party that refuses to provide it (ex: unfavorable judgment, loss of market due to a ban on any activity in the territory concerned, financial penalties, etc.).

The United States therefore easily imposes its rules, procedures and laws and it is not surprising that the EU and its Member States have taken protective measures namely regarding personal data protection and trade secrets.

What are the drawbacks?

In addition to the Contracting States taking advantage of certain rules or exceptions to impose their national legislation, the Evidence Convention leaves quite a degree of latitude to the Contracting States. Although this respects State sovereignty it also leads to a “patchwork” of rules regarding the Evidence Convention. States must pay particular attention to what other signatories do and which rules they implement.

Furthermore, in 2013, several Contracting States [underlined](#) that the evidence procedures were sluggish, that they did not always get responses to their Letters and that certain Letters did not hold enough information for the judge to assess the request. Therefore, the procedures seem to backfire against their intention to simplify and facilitate international evidence obtention.

Sheet 8 - Blocking Statute

What is it?

Certain Member States of the European Union, such as France, have adopted “blocking statutes” to protect themselves against the abusive application of foreign legislations allowing the communication of documents within the framework of Discovery. Implicitly, blocking statutes are protections against the extraterritorial laws. This is namely the case of the Hague Convention regarding evidence.

In France, [Act n° 80-538 of 16 July 1980](#) on the communication of documents and information of an economic, commercial or technical nature to foreign natural or legal persons, and amending [Act n°68-678 of 26 July 1968](#), establishes a blocking framework.

What's its purpose?

As previously stated, blocking statutes aim at protecting national interests and namely strategic information held by companies. In France, Act n°68-678 protects the communication of documents and information of an economic, commercial, industrial, financial or technical nature to foreign natural or legal persons.

What are the key points?

The French Act states in [Article 1](#) that no natural or legal French person “may communicate in writing, orally or in any other form, anywhere, to foreign

public authorities, documents or information of an economic, commercial, industrial, financial or technical nature, the communication of which is likely to prejudice the sovereignty, security, essential economic interests of France or public order, specified by the administrative authority where necessary”. It continues to limit what information may be provided in [Article 1 bis](#): “no person shall request, seek or communicate, in writing, orally or in any other form, any document or information of an economic, commercial, industrial, financial or technical nature for the purpose of obtaining evidence in or in connection with foreign judicial or administrative proceedings”.

The Act therefore seem to preclude any Discovery process. However, this is not the case. Both Articles hold an important exception regarding international treaties or agreements. Documents or information, regardless of their nature, can be communicated if the process is provided for in an international treaty or instrument (ex: the [Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters](#), the [Privacy Shield](#), etc.). This exception thus enables France to control and regulate Discovery processes.

Finally, [Article 2](#) imposes the obligation to inform the competent Minister without delay when a person receives any request concerning the communications described above. The negotiation becomes political.

What are the drawbacks?

The Act has seldom been used and seems outdated. Although companies may still be using it, one the most recent decisions dates back to December 2007 ([Cass. Criminal division, 12th of December 2007, n°07-83.228](#)). In this case, a French lawyer had been asked by an American lawyer to obtain information on the manner in which decisions were taken within the board of directors of a French company. He wished to transmit them to his American colleague in order to be able to include them within the framework of a pending procedure in the United States. He was then found guilty of wanting to transmit economic information and sentenced to a €10,000 fine.

In addition to modernization, the Act also seems to call for clarification (ex: specify the competent administrative authority and the procedures for referral to it, better define the objective sought by the law, i.e. the protection of the fundamental interests of the Nation, etc.).



Sheet 9 - The Trade Secret Directive

What is it?

[Directive n°2016/943](#) of the European Parliament and of the Council of June 8th, 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure came into force on June 9th, 2018 in the EU.

It must be underlined that the Trade Secret Directive is currently being implemented by several Member States. For example, a [bill on the protection of trade secrets](#) was recently adopted in France. It is now being [examined by the Constitutional Council](#) on request of the Senate.

What's its purpose?

The Directive sets a common and unified definition of trade secrets in accordance with existing internationally binding standards. Thus, companies will benefit from a common legal framework throughout the Internal Market which will secure and help develop their businesses.

Furthermore, the Directive defines the relevant forms of misappropriation and harmonises the civil means through which victims of trade secret misappropriation can seek protection. Companies, researches, inventors and so forth will know how to best protect their trade secrets, the legally prohibited actions and the remedies they can seek. The Trade Secrets Directive ben-


efits all actors throughout the Internal Market.

What are the key points?

One of the crucial elements of the Trade Secret Directive is the definition of "trade secrets" under [Article 2](#). The latter sets out the requirements the information must meet to be considered as a trade secret:

- It is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- It has commercial value because it is secret;
- It has been subjects to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

This definition is similar to that of [Section 1, 4° of the Uniform Trade Secret Act](#) (UTSA) in the United States which applies at a State level and to the [Federal Cohen Act \(1996\)](#). An international harmonisation is thus sought by the EU. It remains to be seen how Member States will implement the Directive into their national laws.



The Trade Secret Directive aims at protecting trade secrets by defining both lawful and unlawful acquisition, use and disclosure of trade secrets. For example, will be considered lawful a trade secret obtained by independent discovery or creation ([Article 3 of the Trade Secrets Directive](#)) whereas the disclosure of a trade secret in breach of a confidentiality agreement or of any other duty not to disclose the trade secret will be considered unlawful ([Article 4 of the Trade Secrets Directive](#)). These measures are once again very similar to those across the Atlantic.

It must be underlined that the civil remedies and/or protective measures offered by the Trade Secret Directive have a broad scope. They namely include the prohibition of the production, offering, placing on the market or use of infringing goods or the importation, export or storage of infringing goods for those purposes ([Article 10 of the Trade Secrets Directive](#)), damages and recurring penalty payments ([Articles 14 and 16 of the Trade Secrets Directive](#)). There appears to be a clear deterrent effect.

In light of our comparison with the United States, the [Defend Trade Secrets Act \(2016\)](#), amending the Cohen Act, created a federal civil cause of action for trade secret misappropriation. This implies that both criminal and civil action can be brought on a federal level. However, the Trade Secret Di-

rective does not cover criminal actions in the EU. It will up to the Member States to determine conditions for such actions.

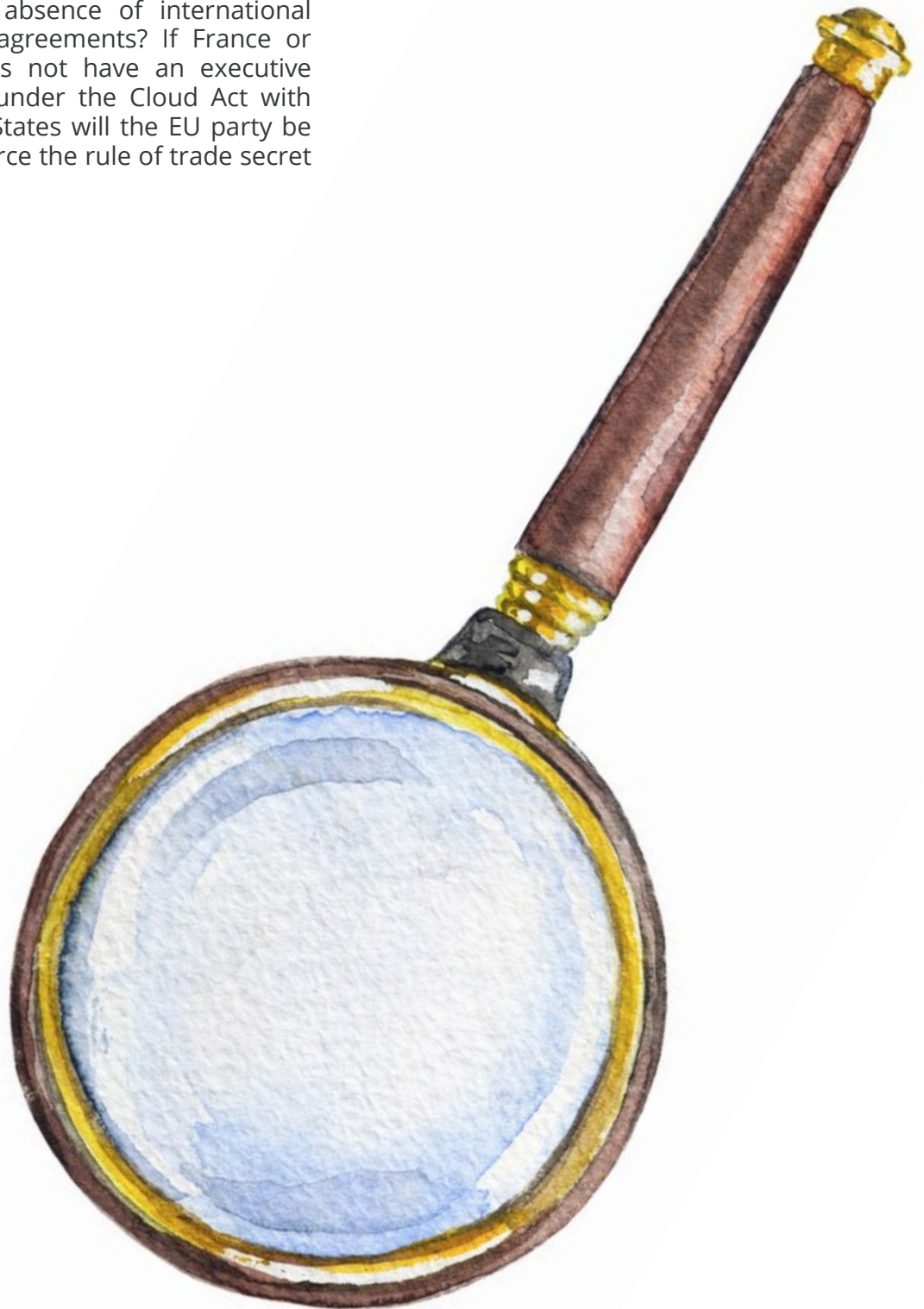
What are the drawbacks?

The impacts of the Trade Secret Directive are unclear. Member States are still in the process of implementing it and will most likely make several adjustments. Furthermore, let us recall that Directives under EU law must be implemented whereas Regulations are directly applicable. This implies a potential patchwork of legislations in the EU regarding the protection of trade secrets regarding the remedies available (ex: different conditions, different judges, etc.).

This uncertainty also leads to ponder on the way in which the Cloud Act and the Trade Secret Directive will interlay. If the United States Government requests the disclosure of information considered as a trade secret, will the provider be compelled to comply? Can the provider argue that disclosure would violate the EU legislation on trade secret protection?

What about the Member States' legislation? For example, the French bill on the protection of trade secrets inserts a new article in the Code of Commerce regarding the disclosure of trade secrets on an international level. In a few words, if the disclosure, use or obtention of trade secrets is required or authorised by EU law, international treaties or agreements in force or national law, trade secrets will not be enforcea-

ble. This implies that the information will be disclosed. How will this work out in the absence of international treaties or agreements? If France or the EU does not have an executive agreement under the Cloud Act with the United States will the EU party be able to enforce the rule of trade secret protection?



Sheet 10 - What issues must be considered during (e)Discovery ?


As previously said in this White paper, Discovery is an important process in common law countries. It is a crucial stage of any legal action or proceedings during which the parties gather pertinent facts or documents. In our digital word, a new form of discovery emerged: electronic discovery, called eDiscovery. It is the discovery of electronic information in litigation.

The term "electronic information" has a broad scope including any information stored on electronic media (ex: computers, email and other servers, memory sticks / flash drives, CDs, DVDs, backup tapes, cell phones, etc.).

Mathias Avocats has drawn an overview of the issues which must be considered when subject to a Discovery, namely eDiscovery, request.

requested by the other party? Are there any recourses available to avoid the disclosure and/or transfer of the data or information requested?

- ❖ Is there a specific protocol or policy within your entity regarding (e) Discovery requests?
- ❖ Is a register or document kept for the information or data received and/or requested? Does it hold the crucial information regarding the information or data (ex: name of the requesting party and of the person whose information or data is requested, form of the document sent, etc.)?
- ❖ Do you have the obligation to produce the data or information requested by the other party? Are there any recourses available to avoid the disclosure and/or transfer of the data or information requested?
- ❖ What type of information or data is requested? Is it sensitive? Does it concern clients, third-parties, your personnel or company?
- ❖ Under what format must the data or information requested be transferred (ex: paper, PDF, MSG, rendered HTML, etc.)?
- ❖ Have security measures been implemented upon receipt or sending of the information or data?
- ❖ Does the (e)Discovery request go against the rules of confidentiality? If this is the case, how will your entity deal with the request?
- ❖ In what geographic location and on which computers or devices is the information or data stored?
- ❖ Who will review the information or data? The other party or a third-party? Where is either established?

- 
- ❖ Are there any international agreements or laws applicable to the (e)Discovery request? If not, which national law will apply?
 - ❖ What are the specific rules for data transfers in your country?



Sheet 11 - What to check before entering into cloud computing agreements ?

Cloud computing can be [defined](#) as a method for delivering Information Technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server. For example, instead of saving your files on a USB key, the files can be kept in a remote database (i.e. the cloud). Several types of cloud computing exist. However, the idea remains the same: the creation or transfer of data in a remote database.

Cloud computing has become a customary practice in companies considering the flexibility it offers. Entities can centralize their data, services and applications while being able to access them from everywhere and at any time.

Mathias Avocats has outlined several key points to consider before entering into or drafting a cloud computing agreement.

- ❖ What type of cloud have you chosen? Is it private, public or hybrid?
- ❖ Are the cloud computing services offered by one or several companies? Does the cloud provider use its own infrastructure, or does it use cloud-based services provided by third-parties?
- ❖ If there is a third-party, where is it established? Can data transfers be

lawfully made to the third-party's country? What are the obligations of said third-party?

- ❖ How will the cloud provider handle, control and process the data? Who will be in charge of these tasks?
- ❖ Does the cloud provider have access to your or the client's personal data? Can the cloud provider use said data?
- ❖ What kind of personal data is concerned by the cloud computing agreement? It is important to keep in mind that sensitive data requires specific measures. They may also be subject to sector specific legislation.
- ❖ What security measures have been taken (ex: encryption, pseudonymisation, firewalls, passwords, notification of security incidents, backups, etc.)?
- ❖ Have measures been taken to ensure the privacy and confidentiality of the data? Which party must implement these measures?
- ❖ What are the conditions for support? When will the cloud provider be available? Can the cloud provid-

er provide quick and efficient solutions?

- ❖ Does the cloud provider have a Privacy and Confidentiality agreement or policy? Does it comply with the applicable legislation in your country?
- ❖ Where will the data be stored? What is the applicable legislation or regulation? Which judge is competent?
- ❖ Are audits of the cloud computing agreement provided for? Will they happen regularly?
- ❖ Are the parties' liabilities clearly defined? Is there a cap?
- ❖ Under which conditions can the parties terminate the agreement?
- ❖ Upon termination of the cloud computing agreement, what happens to the personal data? Will you be responsible for retrieving your data or will it fall on the cloud provider? What happens if data has been lost or destroyed?



Sheet 12 - What are BCRs ? How can they be used for data transfers ?

Binding Corporate Rules (BCRs) are defined under [Article 4 \(20\) of the GDPR](#) as “personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity”. They are part of the types of transfers authorized under the Regulation.

It is important to note that BCRs must be binding and respected by all entities of the group, regardless of their country of establishment, as well as by all their employees. They offer an alternative to standard contractual clauses and to transfers under the [Privacy Shield](#). However, BCRs do not cover personal data transfers outside a corporate group. They have a limited scope.

Mathias Avocats has analysed the requirements for BCRs and gives guidance regarding their drafting.

What are their minimum requirements?

The drafting of BCRs is regulated. Indeed, the entity must seek approval of the competent supervisory authority for its BCRs in accordance with the consistency mechanism set out in Article 63 without requiring any specific

authorisation from a supervisory authority ([Article 46 \(2\) \(b\) of the GDPR](#)). In practice, the competent supervisory authority will most likely be the lead supervisory authority.

It must respect the minimum requirements set out in [Article 47 of the GDPR](#). Under the latter, BCRs must specify:

- The structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- The data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- Their legally binding nature, both internally and externally;
- The application of the general data protection principles (ex: purpose limitation, data minimisation, limited storage periods, etc.);
- The rights of data subjects in regard to processing and the means to exercise those rights;
- The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by

any member concerned not established in the Union;

- How the information on the BCRs are provided to the data subjects;
- The tasks of any DPO or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group;
- The complaint procedures;
- The mechanisms within the group for ensuring the verification of compliance with the binding corporate rules (ex: data protection audits, correction procedures, etc.);
- The mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
- The cooperation mechanism with the supervisory authority to ensure compliance by any member of the group
- The mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- The appropriate data protection training to personnel hav-

ing permanent or regular access to personal data.

In a few words, BCRs must hold all relevant information to the transfers. Although the list may seem lengthy to entities, BCRs offer several advantages such as enabling a group to establish a common data protection policy and not having to enter into a different contract for each transfer. They seem more efficient for large companies' part of a group.

It must be noted that two forms of BCRs are currently approved: BCRs between data controllers and BCRs between data controllers and processors.

Although BCRs were available under the [Directive 95/46/EC](#), the GDPR introduces several changes which must be taken into account by data controllers or processors. One of the innovations are the data subject's right to lodge a complaint and right to information. The data subject must be informed of his or her rights in a clear, concise and transparent manner. In practice, the language used must not to overly technical or legal. Furthermore, under the principle of accountability, data controllers shall be responsible for and able to demonstrate compliance with the BCRs.

What issues to consider?

Mathias Avocats has drafted a checklist of the issues which must be considered when drafting BCRs:

- ❖ What is your entity's status under the GDPR? What about third-parties the entity deals with?
- ❖ Where are your headquarters located? Where is each entity of your group established?
- ❖ Are BCRs the right fit for your group? Can another international agreement be used? Are there any conflicting rules to the use of BCRs?
- ❖ Do your BCRs have a legally binding effect internally between the members of the group and externally for data subjects who wish to exercise their rights?
- ❖ Does your entity use BCRs drafted before the coming into force of the GDPR? Have they been amended to meet the new requirements?
- ❖ Do your BCRs hold the minimum requirements set out in [Article 47 of the GDPR](#)?
- ❖ Has liability clearly been defined between your entity and the other entities of the group? With data processors?
- ❖ Which entity will be responsible for answering any request or questions from data subjects or a supervisory authority?
- ❖ Are the BCRs easily accessible to data subjects?
- ❖ Have the personnel been appropriately trained regarding BCRs?
- ❖ Who will perform the required audits? The entities of the group or an external company? Has a procedure been set up to transmit the audits to the appropriate entity within the group and person(s) supervising its conformity?
- ❖ How and when will the BCRs be updated? How will each member be notified?

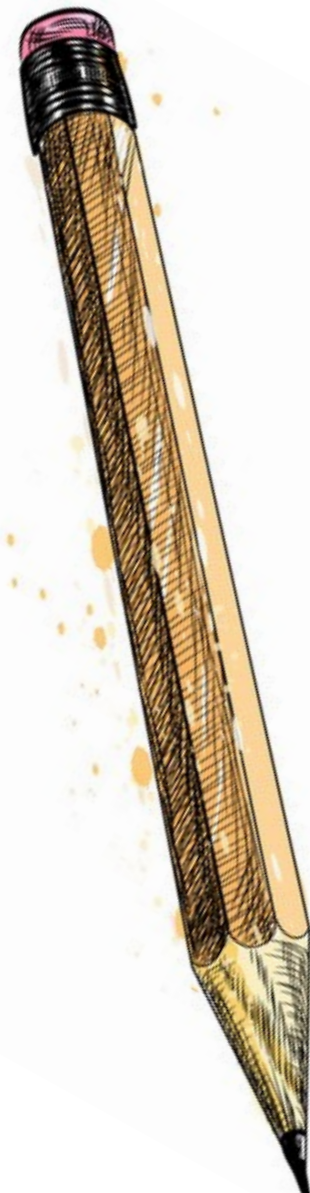
Sheet 13 - How to draft contractual clauses with a party established in the USA ?

This White paper has underlined the significant issues which arise when dealing with a party established in the United States and, more generally, with the extraterritorial scope of the United States legislations. These issues must be kept in mind when drafting legal documents such as contracts. Furthermore, where personal data is concerned, parties must examine whether or not the GDPR is applicable, and, if it is, they must ensure that every requirement is met.

Mathias Avocats has drawn up a list of crucial elements to consider when drafting contractual clauses with partners or parties established in the United States involving a transfer of personal data.

- ❖ Does a written contract, or other legally binding written document, set out the subject matter and duration of the agreement between the parties?
- ❖ Are the obligations and liabilities of each party clearly defined? This issue is all the more important considering that data processors are now held liable for their violations.
- ❖ Do specific EU or United States legislations apply to the subject matter of the contract? Is there a conflict? Which law must be applied?
- ❖ Where will the data be transferred? Is the country considered as providing adequate protection? If not, what guarantees are provided?
- ❖ Does the contract specify all the relevant information regarding the processing of the personal data transferred (ex: the type of data, the purpose of the processing, the period for which the data will be stored, the data subjects concerned, etc.)?
- ❖ Does the party established in the United States present sufficient guarantees that the requirements of the GDPR will be met and the rights of data subjects protected?
- ❖ Are there third parties involved (ex: sub-processors, external security company, etc.)? Where are they established? What obligations are they under?
- ❖ Are the personnel processing the personal data under a duty of confidentiality or secrecy?
- ❖ What security measures have been taken? How is the confidentiality of the data ensured?

- ❖ How are data subjects informed of their rights? Is the information easily accessible? Is the information complete?
- ❖ Are audits and inspections provided for? By whom will they be carried out? At what frequency will they be carried out?
- ❖ In the event of a security breach, which party must notify the competent supervisory authority? Has a procedure been implemented? Does it comply with the GDPR? Must the security breach also be notified to an authority within the United States?
- ❖ Has every step, procedure and action under the contract been adequately documented? Is this requirement of accountability provided for in the contract?
- ❖ What terms have been drafted for the termination of the contract? Will the data be restored or deleted? Has another option been provided for?
- ❖ In the event of a legal action, which judge is competent? Which law shall apply?



**You can subscribe to our Newsletter on the
firm's website:**

www.avocats-mathias.com



About Mathias Avocats

We are a law firm with a focus on organisations being changed by technology and the digital world.

Our clients include some of the largest financial institutions, and leading technology companies. We also represent investment funds and startup companies, and over the years have supported many in their growth and development as leading industry players and household brands.



Do you have a question ?

A team dedicated to achieve your ambitions will reply :

01 43 80 02 01

contact@avocats-mathias.com

19, rue Vernier – 75017 – Paris

Find our lawyers' practical advice on Twitter :

[@GaranceMathias](https://twitter.com/GaranceMathias)

