AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Guidelines 2/2019 on processing personal data under Article 6(1)(b) of the EU GDPR

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2018, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

The American Chamber of Commerce to the EU (AmCham EU) welcomes the opportunity to provide feedback on the Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) of the EU GDPR (hereafter 'the Guidelines') in the context of the provision of online services to data subjects. This paper outlines our comments aiming at a consistent and balanced application of the GDPR.

Scope of the guidelines

The limitation of the scope of the Guidelines to 'processing of personal data in the context of online service' only (as per stated in point 7 of the Guidelines) seems too restrictive. The issues at stake are not specific to online services but are linked to the very essence of how a contract shall be validly entered into, performed, monitored, enforced and terminated. Companies in all industries and sectors, including online and offline services, need to rely on contractual necessity as a legal basis for processing. In addition, all companies as part of their digital transformation are increasingly relying on data processing and digital services to sell and market their products and services. As a result of this, companies that used to have pure 'brick-and-mortar' business models are now also providing online services in addition to their traditional services of products. Often, all of this is part of the same contractual arrangement. All companies would benefit from a better delineation and understanding of the contractual necessity lawful basis. Therefore, **the scope of the guidance should be expanded to cover any performance of a contract beyond online services.**

Necessity test

The Guidelines follow a too narrow approach of the necessity test on the basis that the contractual necessity would operate as a limitation on the right to personal data. This approach is not justified as a legal basis is not *per se* a derogation or a limitation of data protection rights. Per definition legal bases are all equal, as they identify the circumstances under which personal data can be *legally* processed.

A restrictive construction is required in other scenarios where the right to data protection is either (i) being limited by legislation such as under Article 23 of the GDPR (which allows data protection rights to be 'restricted' in certain cases where it is 'necessary and proportionate' to do so), or (ii) not subject to substantially equivalent safeguards in international transfers, such as when the derogations under Article 49 of the GDPR apply. Similarly, in circumstances where fundamental rights are abridged (since they are not absolute rights), case law confirms that the 'necessity' test should be applied in a strict manner. However, **in cases where the right to data protection is not being abridged, the 'necessity' should be given the interpretation that is due based on contract law and consistent case law, which is wider.**

Contract law aspects

It is essential to take into account the notion of performance in contract law. **The concept of 'performance' should be interpreted consistently across Member States according to the applicable contract law that the GDPR is unable to modify**.

For example, under Irish contract law, 'performance' refers to the fulfilment by a party to the contract of his or her contractual obligations under the terms of the contract. Under UK contract law, performance under contractual necessity includes processing 'to fulfil your contractual obligations'. In these two examples, the concept of performance displays considerable flexibility in the sense that, depending on the circumstances and the terms of the contract, effective performance may take the form of entire performance or something less than that (ie, substantial performance).

The view that performance is a flexible concept is also shared by civil law countries where the contract obliges the contracting party to comply with its provisions and the nature of the contract according to law and ordinary usage and with reference to good faith. It emerges from this analysis that 'performance' is not the narrow concept that the Guidelines seem to suggest.

Accordingly, Recital 44 of the GDPR states that '[p]rocessing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract'. Recital 44 does not mention the term 'performance' but rather refers to 'the context' of a contract. A literal reading of Recital 44 suggests that 'the context' of a contract refers to the circumstances in which a contract is entered into, performed, monitored and enforced, according to law, ordinary usage and good faith.

There may be multiple purposes for which processing is necessary for the performance of the contract. This might include activities such as: an international transfer of personal data in the context of a derogation; party compliance with contractual warranties, fraud prevention; security of processing; enforcement of contractual rights clauses, etc. Like many other areas of the GDPR, this proves that the context is essential, **contractual necessity cannot be determined with blanket assessments of hypothetical provisions**: the specific processing activities in light of the purposes of the specific contract and the way in which such processing might increase the effectiveness of the contract must also be considered. For example, Article 22(2)(a) GDPR expressly recognises that automated processing including profiling may be necessary for entering into or performing a contract.

In addition, assessing the validity of a contract as a foundational matter ensures that the purposes of the processing activities under contractual necessity support a lawful business model. For instance, the proposed purpose of a valid contract cannot be for illegal processing, eg. a valid contract could not be made to sell illegal drugs or engage in unfair discrimination. When based on a valid contact, contractual necessity acts a lawful basis for processing activities that are necessary for a legal business model. Therefore, **as long as the contract is legal, processing activities which are necessary for the objective purpose of that contract should fall within the scope of contractual necessity.**

Finally, as the EDPB notes in point 33 of the Guidance, 'the mutual perspectives and expectations of the parties to the contract' must be considered. One cannot solely assess the contract via the prism of the expectations and benefits to the data subject. All contracts are, by definition, bilateral exchanges. **The benefits to and requirements of both the service provider and the individual need to be considered in determining what is necessary in the context of a contract.**

Applicability of article 6 (1)(b) in specific situation

Processing for 'service improvement'

The EDPB's view on 'service improvement' seems too narrow. Any party to a contract has a legitimate expectation that the organisation offering a product or service will work to improve them over time. This is true in particular when technology advances, or to ensure better connectivity or a higher level of security. Attackers are continually seeking vulnerabilities in systems; therefore, those systems might need to be updated from time to time to ensure that users get the service they contracted for in a reasonably safe and secure fashion. In addition, many businesses will process personal data through customer satisfaction surveys and business analytics to ensure that customers are getting the service for which they contracted and expect. Finally, including improvements in contractual terms can be objectively necessary, for instance when beta version or minimum viable products are offered in specific situations.

Processing for fraud prevention

The EDPB considers that processing for fraud prevention purposes which involves monitoring and profiling customers is likely to go beyond what is objectively necessary for the performance of a contract with a data subject (paragraph 47). This approach seems very restrictive. In some cases, such processing might fall under the legal basis of legitimate interest. However, this is not necessarily the case: the provisions of contract any

(offline and online) might also require a reliable service for the two contractual counterparties (both the user and the services provider) to be reasonably protected against fraud and other security risks. Depending on the context, delivering reasonably safe online services could form part of an integral part of the contractual rights and obligations of many service providers.

The very strict interpretation of contractual necessity puts a strain on legitimate, low-risk types of processing, including fraud prevention and product/service improvement. Even if it is likely that fraud prevention will be a compelling legitimate interest and be permissible, if data subjects can opt out of product improvement – a low-risk use of personal data that presumably benefits all – this is problematic and seems anti-business.

Processing for online behavioural advertising

Online and offline advertising is an important business in the EU. In particular, online advertising supports a variety of online services, including press and news media. From the user's perspective, the objective purpose of the contract would be to receive certain content. However, from the service provider's perspective, the objective purpose of the contract may consist or include to show ads next to that content so as to obtain the revenue which is inextricably linked to the economic viability of the services. **Claiming that advertising is separate from the objective purpose of the contract between the user and the service provider is equivalent to only look at one side of such contracts and does not respect the fundamental freedom of conducting a legitimate**. As it happens for TV broadcasters, the ability to run ads is not a tangential consideration – it is the very core of certain offline and online businesses.

Impact on WHOIS

Given that ICANN's purpose is to provide for third-party processing, it is unclear how the 6(1)(b) basis would apply without conflating this purpose. The contracts between ICANN and its Contracted Parties cannot be separated from the Agreements with the registrants due to the nature of the domain name registration framework.

Regarding processing for 'fraud prevention' (paragraph 47 of the Guidelines), it needs to be clarified whether processing for the purposes of fraud prevention is necessarily precluded under 6(1)(b), specifically in the ICANN context where fraud prevention is necessary for the performance of the 'secure, stable, resilient Domain Name System (DNS)' contractual obligation.

It would be useful to develop guidelines which consider and address the need to have access to registrant data for security purposes. Such guidance would also benefit law enforcement, domain registrars, as well as Generic top-level domains (gTLD) and country code top-level domain (ccTLD) registry operators.