AMERICAN CHAMBER OF COMMERCE IN ROMANIA
Member of the U.S. Chamber of Commerce and of
the European Council of the American Chambers of Commerce
11 Ion Campineanu St., Bucharest 1
Tel: + 40 21 315 86 94, 312 48 34
Fax: + 40 21 312 48 51
E-mail:amcham@amcham.ro

AmCham Romania Position Paper on the New EU Data Protection Regulation

Introductory Remarks

This document sets out the position of the American Chamber of Commerce in Romania ("**AmCham Romania**") with regards to the proposal for a new Data Protection Regulation launched on 25 January 2012 by the European Commission (the "**Regulation**").

AmCham Romania is a non-profit and non-political organization that promotes the commercial and economic interests of American, international and local business community in Romania. AmCham Romania is comprised of more than 300 companies operating in various business sectors, including information technology.

AmCham Romania acknowledges that, in the context of the unprecedented technological developments in recent years, the right balance between the privacy rights of individuals and the need for the economic environment and consumers to benefit from technological progress, must be found.

AmCham Romania supports the European Commission in its endeavours to build a strong data protection framework aiming to increase the protection of data subjects across the EU and EEA and to eliminate unnecessary burdens on controllers and processors. However, AmCham Romania believes the proposed Regulation, as currently drafted, poses some significant challenges and, if enacted in the proposed form, could harm businesses operating in Romania and create disincentives for future investment.

This position paper is issued in furtherance to and follows the position of AmCham EU on the Regulation, issued on 11 July 2012, (the "**AmCham EU Position**"), which AmCham Romania fully endorses. Given that AmCham EU Position already incorporates and builds on the fundamental issues raised by pan-European industry voices, this document aims to provide an overview of the main aspects that, in the opinion of Amcham Romania members, would significantly impact the Romanian business environment and the country's overall level of competitiveness.

Issues and Recommendations

AmCham Romania supports the harmonized legal framework provided by the Regulation. At the same time, AmCham Romania would like to draw attention to several aspects of the Regulation, which need further clarification or amendment in order to ensure a consistent approach throughout Member States. In the age of the ever-present connectivity, of e-commerce and of cloud computing, AmCham Romania's approach takes into account both the need to provide European and Romanian data subjects with strong privacy safeguards, as well as the compelling reality that organizations of all sizes need to constantly innovate and be able to function globally, in a manner that would ultimately generate progress and wealth for all countries.

Below is AmCham Romania's point of view on certain aspects of the Regulation which, in light of Romania's current position in the marketplace, as well as of its regulatory and enforcement stance on

data protection matters to date, need to receive careful consideration. If passed in its current form, the Regulation is likely to add supplementary compliance burdens on all companies operating in Romania and to hinder the functional data flows Romania needs in order to remain an attractive place to do business in the information age.

1. The requirement of express affirmative consent

The Regulation requires the explicit, affirmative consent of data subjects in all circumstances, without considering the variety of contexts involving data processing activities and the uneven privacy impact in each of such contexts.

This "one size fits all" approach raises particular problems for the online environment, which is by far the most affected sector, given that, by its nature, it makes consent difficult to obtain. **The practice of "ticking boxes" may lead to the overwhelming of users**. By requiring users to opt in to every use of their data, the Regulation will potentially require them to opt in dozens of times, if not more, during a single web surfing session or mobile internet use. However, AmCham Romania would like to stress that consumers demand internet services that are fast, easy-to-use and efficient. Onerous and static opt-in mechanisms instituted by controllers anxious to be in unambiguous compliance with an ambiguous requirement will frustrate many users – and ultimately may lead users to opt in as a matter of routine, without actually taking the time to read through the privacy notices they are confronted with.

Furthermore, the requirement of express consent may lead to a **decrease in Internet use in Romania**. Statistics show that this country has registered one of the highest percentage of people that have never used the Internet. At 39% of the population in 2011, Romania's rate of regular internet use (at least once a week) is significantly below the EU average (69%).[1]

A major point of concern may be anticipated for Romania's **employment market** where employers currently rely on employees' consent to justify certain data processing operations like international data transfer. Under the Regulation, consent alone shall not provide a legal basis for such processing. This would arguably render the management of HR data more difficult and, in case of multinational employers operating in Romania, would prevent the integration of Romanian employee data into the global workforce organizational processes operating at group-level. Although we agree that generally employment relationships are based on a significant imbalance of power, this does not necessarily exclude the validity of employee consent. A relevant example would be where an employer decides to ask its employee details of a contact person in case of emergency. The employee is free to offer such information to the employer as its benefits are clearly more beneficial than any consequences triggered by the actual disclosure of such data. In conclusion, **there are situations in the employment context whereby consent is validly expressed despite the imbalance of power.**

Moreover, from AmCham Romania's experience with the Romanian Data Protection Authority (DPA), when examining data processing operations of controllers, the DPA values the existence of employees consent. Therefore, it may be construed that **the practice of the Romanian DPA may be significantly affected by the Regulation in the absence of clear new rules to regulate the matter**. In order to mitigate any potential negative implications, Amcham Romania recommends that the Regulation allows employers to process employee personal data based on consent in certain situations where the imbalance of power is not a determining factor in relation to personal data processing.

Furthermore, prescriptive consent requirements are not only impacting the flexibility in designing ways to seek informed and meaningful consent, but they are also **increasing the costs of data processing**, especially in the online environment, where service providers would incur significant costs in order to accommodate the consent requirement from a technical point of view. Ultimately, this may reduce

[1] For more information, http://ec.europa.eu/information_society/digital-agenda/scoreboard/countries/ro/internet_services/index_en.htm and http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/2012/scoreboard_life_online.pdf.

Romania's competitive advantage in the IT & Communications sector and its chances of becoming a regional technological hub.

Last but not least, the **new rules will discourage the positive trend towards anonymization and minimization of personal data processing**. Amcham Romania believes that rather than requiring express consent, the Regulation should provide more incentives for data controllers and processors to render anonymous the processed personal data. On the long term, such procedures may prove more beneficial to data subjects than express and affirmative consent.

2. Profiling

Profiling itself is merely a technical process that helps identify patterns across large quantities of data, and in doing so allows information to be collected and organised in meaningful ways. As such, there is nothing inherently wrong with profiling. Indeed, profiles are frequently used to satisfy consumer demands for technologies and services that remember their preferences, such as their native language or home country, or that are customised in any other ways. Of course, as with any business process, automated profiles can also be used to achieve less desirable outcomes, such as discriminating against individuals on the basis of their health. To ensure that user data is not used to achieve goals that are contrary to EU citizens' interests, it makes sense to regulate the use of profiles for harmful purposes. However, such rules should not restrict the building of profiles for all purposes – including beneficial purposes that are intended to respond to legitimate consumer demands.

AmCham Romania's recommendation is that the Regulation be amended to make clear that profiles can continue to be used for beneficial and legitimate purposes such as, monitoring and fraud and crime prevention, service improvements, providing customised internet experiences to users, marketing. Subjecting both beneficial and harmful profiling activities to the same rules would impede many consumer driven services which would have a negative impact both on consumers and on service providers. Consumers will no longer benefit from marketing products specifically designed to suit their preferences. On the other hand, **profiling lies at the core of the direct marketing business model and e-commerce. Therefore, companies that offer their services and products on-line, which have registered a continuous growth in sales in the past years in Romania, might be irreversibly affected and decide to withdraw from the Romanian market.**

Another relevant example of industry which will be affected by the current provisions of the Regulation on profiling is the healthcare industry. Health research, particularly in the areas of health services, population and public health, critically depends on the availability of existing data about people. However, most of this data can be anonymised and/or pseudonymised to serve the purpose.

We are concerned about Article 20 not providing a distinction between data processing that identifies an individual and data processing that does not. As currently drafted, Article 20 - which uses the term "natural person" rather than "data subject," seems to broaden the overall scope of the Regulation even further by not focusing on what would constitute a risk for the data subject. **We believe profiling techniques per se do not need special regulatory treatment given the many safeguards introduced in the draft Regulation especially when incentives are provided for companies to anonymize and/or pseudonymise data**. The current text of Article 20 might render legitimate use of data for health research impossible with great consequences for the social benefits in this area. While individual research institutions can work for years on a cure for Alzheimer's, results come much faster when analytics are applied and these institutions combine data sets.

That is the promise of today's business analytics: extracting insights from proliferating data to help individuals, organizations and entire societies get smarter. Indeed, analytics are no longer a luxury but a requirement for organizations that seek to make sense of the ever-increasing sum of what they know.

3. Definition of personal data

The Regulation defines personal data as any information relating to a data subject. AmCham Romania believes that such a general wording triggers the risk of qualifying all information about data subjects as personal data, which would not be an accurate approach. **The definition blurs the distinction between information that identifies directly or indirectly a data subject and the information which does not lead to such identification and which should therefore not be qualified as personal data.** Consequently, in practice data controllers and data processors would experience serious difficulties in determining whether the information collected from individuals falls within the definition of personal data. Given that the concept of "personal data" is fundamental in establishing the applicability of the Regulation, AmCham Romania believes that there can be no uncertainty surrounding its definition and the exact data it refers to. In practice, this would create confusion amongst **organisations** which **may not be able to assess whether their activities are subject or not to the Regulation.**

Moreover, please note that **a too general and unclear definition of personal data would complicate to a large extent the data protection issues in Romania, where in AmCham's opinion, the level of awareness in respect of this field is relatively low.** Moreover, apart from the national law implementing the current Directive 95/46, there are not too many guidelines issued by the Romanian DPA.

Last but not least, the definition of **"genetic data"** is equally broad. Genetic data is deemed as highly sensitive data whose processing requires additional safeguards. Therefore, **in order to avoid an extensive interpretation whereby ordinary personal data such as hair colour is included within the scope of the definition, a very clear and precise wording is advisable.**

4. The right to be forgotten

According to Article 17 of the Regulation, data subjects shall have the right to obtain from the controller the erasure of their personal data. However, the nature of the right to be forgotten does not reflect the structure of the internet.

Digital data today is often quickly replicated across the web on systems and servers across the globe with or without any formal technical or contractual relationships between different parts of the online ecosystem. For example, many search engines and content aggregators use publicly available internet information to catalogue and build large caches of data without any explicit contractual agreement with the primary publisher of the information. These caches are what make it possible for individuals to find data quickly on the internet when they do an Internet search. However, as a result, **it can be difficult if not impossible to "remove all tracks"**, such as information created by a third party. Given the high diversity of online channels, personal data may be stored by platforms which are not under the authority of the data controller. **By requiring that controllers notify any and all third parties, the right to be forgotten provision seems to be based on the assumption that companies can oversee the entirety of the World Wide Web and control the information on it** – an obligation that is directly at odds with the open architecture of the internet. Indeed, European law (in the E-Commerce Directive) already recognises that it would be unreasonable to ask companies to monitor the internet and makes clear that companies should not be required to do so.

To be workable, any interpretation of the right to be forgotten must not obligate companies to do that which is technically impossible. Accordingly, **the Regulation should limit the right to be forgotten to that data retained by and under the control of the controller and reasonably accessible in the ordinary course of business.** At the same time**, the right to be forgotten should extend only to a user's own data** (i.e., data that a user inputs directly) **and not to data generated in the operation of the service (for example, error messages or uptime statistics).** For user convenience, service providers should also be permitted to retain data for a limited period of time in order to re-enable users accounts where users expressly requested this. **Furthermore, AmCham Romania believes that the**

Regulation should pave the way for on alternative mechanisms protecting the right to be forgotten, such as the obligation for online providers to inform users about privacy settings.

5. Data Portability

AmCham Romania acknowledges the need for consumers to be able to take their data in a commonly-used format subject to further use. However, **the Regulation should recognize the** technical **reality that the ability to export data does not necessarily mean that such data can be used "as is" in other services**. Companies use a wide range of mechanisms to enable the export of data – among them industry standard formats, import/export functions and application program interfaces permitting others to connect to the data directly – depending on the technology, service and functionalities involved. Moreover new mechanisms are invented every day. As a result, **the successful transfer of data from one service to another is not a simple proposition** – and **mandating a single format for data transfer will require technology providers to change other aspects of their products and services which may result in less functionality, less diversity and a worse overall user experience.**

Furthermore, **the principle of data portability does not reflect cloud computing services** which are based on a variety of data formats and integrated models in continuous innovative technology.

We propose a solution that permits users to port the data they had originally created, but allows industry to decide on formats and technical details of returning user data back to users, based on a variety of technical and commercial factors – including an emphasis on ease of use and the prevalence of a particular format and method.

In addition to this, the Regulation should expressly provide that the **rules on data portability are without prejudice to the proprietary rights of data controllers such as intellectual property rights and trade secrets.**

6. Administrative burdens

Although AmCham Romania supports the **removal of the requirement to notify the DPA** in respect of data processing operations, AmCham believes that the Regulation **has replaced it with new obligations** which do not in fact reduce the administrative burdens for data controllers and data processors.

6.1 Privacy impact assessment

According to Articles 33 and 34 of the Regulation, data controllers and data processors are required to perform a privacy impact assessment and require prior authorisation for a range of processing operations from the DPA. Requiring such prior authorization undermines the declared objective of the Regulation. Furthermore as data privacy awareness is **limited in Romania**, so are the **resources for professionals to undertake such impact assessments.** AmCham Romania recommends the removal of such authorization requirements.

6.2 Data Privacy Officer

As per the Regulation, data controllers and data processors having more than 250 employees or whose core activities consist of processing operations which require regular and systematic monitoring of data subjects must designate an independent data protection officer. AmCham Romania believes that **the number of employees within an organisation is not an appropriate threshold for determining the mandatory appointment of a data protection officer.** There are many organisations with a very large number of employees which are involved in limited data processing operations. At the same time, there are organisations with very few employees which are engaged in massive data protection operations.

7. Distinction between data controllers and data processors

The legislative framework imposed by the Directive 95/46/EC, currently in force foresees a clear separation between the role of a data controller and a data processor. Usually the primary entity with a direct relationship with the data subject is the data controller (e.g. a bank or insurance company) on whose behalf a service provider processes data. The data processor usually acts upon the instruction of the data controller and his responsibilities and liabilities are laid down in a contract negotiated by the parties. The data controller is liable towards the data subject. Many business arrangements and processes existing today are based on the understanding of the difference of these roles and the freedom to negotiate accordingly.

The draft Regulation is fundamentally changing this concept by establishing new responsibilities and liabilities by law.

Of greatest concern is Article 77 paragraph 2 in the proposed regulation which is establishing a joint liability between all data controllers and data processors for which justification is lacking. Freedom to negotiate between contractual parties is a firmly established principle and practice throughout the European economies. It is up to the data controller, to choose his 'suppliers' and define responsibilities. **Extending a joint liability to all contractually parties within large projects will result in endless negotiations and finger pointing with no added value for the consumer/data subject**, especially in situations of great complexity where different IT providers are involved. To the contrary, if a data controller will point a data subject to a data processor with whom he never had any contact this will hardly re-assure the individual.

Where obligations are directly imposed on the processor by law, they will have a duty to better understand the information they process as opposed to simply relying on the controller's representations related to the nature of the data. This defeats the concept of data minimization as more entities will need to know more details about data subjects. Furthermore, the processor may be less willing to accept the controller's suggested processing requirements as sufficient, based on their interpretation of their obligations to secure the data. This decreases the legal certainty in the instructions of the data controller. As for the consumer, It may well be that the **Romanian individual would rather have the Romanian company act as his personal data controller than having first to identify who is the responsible party and then having to liaise with the data processor as well.**

In order to avoid unnecessary additional burden and render current business practices impossible, the new legal framework needs to clearly delineate the responsibilities of the different parties involved in processing information and ensure that the parties bear burdens that are appropriate to their role in the business environment.

However, in its proposed form, the Regulation increases the obligations on processors, which blur the dividing line between the concepts of "data controllers" and "data processors" especially in the context of cloud computing. If an enterprise is not clear on the role it is playing, it cannot determine which tests apply or identify its supervising DPA. Therefore, AmCham Romania considers that the Regulation should further clarify the distinction between controllers and processors. Otherwise these provisions would seriously risk confusing the already established consumer relationships and market dynamics and become a huge impediment to jobs and growth.

8. Administrative fines

Data protection obligations are only effective to the extent they are enforced. Therefore, AmCham Romania welcomes an enforcement regime whereby DPAs are empowered to impose meaningful sanctions for flagrant or repeated violations that threaten real harm of the individuals affected. Consequently, AmCham Romania believes that the "one size fits all" approach imposing the same level of sanctions irrespective of the harm caused by a certain conduct, which may be either deliberate, flagrant or merely accidental, should be amended. A company that inadvertently fails to use a specific

electronic format when giving a customer access to his information could face the same penalty as a company that repeatedly and intentionally collects and processes data about individuals without informing those individuals about its activities. To be balanced and effective, the Regulation should ensure that the most punitive sanctions are reserved for truly bad actors.

In order to assist DPAs in applying sanctions, **it would be useful if the Regulation provided clear criteria determining aggravating circumstances, in which case the penalty should be at the high end, as well as extenuating circumstances limiting the sanctions to the lower end.** Although the Regulation includes a list of factors to be used by DPAs as guidance, the list is not comprehensive. **Additional factors could include, for example the sort of measures the company involved took to avoid the breach**, whether the company was genuinely unaware about the activity amounting to a breach of obligations and if the organisation took steps to remedy the breach immediately upon becoming aware of it.

In terms of the **level of fines**, AmCham Romania believes that it is rather **excessive**. For global companies, fines can result in hundreds of millions of Euros. Therefore, AmCham Romania fully supports AmCham EU's proposal to **subject the fines to a cap**, more specifically 0,5% of the annual global turnover up to EUR 500,000, 1% up to EUR 1 million and 2% up to EUR 2 million.

As further detailed at section 10 below, **in order to avoid the double sanctioning of the same conduct by several DPAs, the Regulation should clearly specify that the competent authority to apply administrative sanctions is the DPA determined as per the "one stop shop" principle**.

9. Delegated acts

The Regulation includes 26 provisions conferring power on the Commission to adopt delegated acts, empowering the Commission to subsequently provide more detail on some of the drafted measures. In Amcham Romania's opinion, these provisions should be significantly reduced, especially since many of these provisions deal with fundamental elements of the law, such as (i) the material scope of the Regulation and the lawfulness of processing (Article 6(1)(f)); (ii) data breach notification (Articles 31 and 32); (iii) administrative sanctions (Article 79). These essential elements should be addressed in the Regulation itself, not left to secondary law-making by the Commission. This would also go against the harmonising objective of the Regulation.

Other delegated act provisions give the Commission power to prescribe technical formats, standards and solutions threatening to replace industry innovation with regulatory intervention. This threatens to complicate, rather than simplify data protection rules. **If new rules are regularly adopted, it means that benchmarks for data protection are always changing and it becomes virtually impossible for organisations to ever achieve compliance.** Moreover, prescriptive measures would potentially hinder innovation in privacy protection. Therefore, AmCham Romania believes that at a minimum, the Regulation should make clear that any secondary rules do not take the form of design mandates or preferences for particular technology solutions.

Finally, as the Article 29 Working Party and the EU Data Protection Supervisor have noted, the delegated acts provisions in the Regulation do not include a clear timetable for implementation. Therefore, should the mechanism of delegated acts be maintained in the final version of the Regulation, AmCham Romania would like to reiterate the importance of establishing a **clear deadline for the adoption of delegated acts in order to avoid businesses facing a lengthy period of legal uncertainty about their rights and obligations.** In this sense, please note that, **given the heavy workload the Romanian DPA has to deal with on a daily basis, procedures in front of the DPA, as well as the creation of the much-needed regulatory guidelines are affected by considerable delays. Therefore, from a Romanian perspective, Amcham Romania believes that the institution of delegated acts will cause severe disruptions in the operation and functioning of the Romanian DPA, especially in terms of timing of adopting the measures adopted by the European Commission as well as of processing requests from data controllers and/or data processors.**

10. Territorial scope and applicable law

According to Article 3, the Regulation is deemed to apply in respect of non-EU controllers in case their envisaged processing activities relate to the offer goods and services to EU residents or to the monitoring of their behaviour. However, **the Regulation fails to clearly define what kind of activities fall under the scope of the term "monitoring".** This is likely to cause many uncertainties in respect of the scope of the Regulation, especially in the context of the widespread use of the internet.

In order **to avoid an excessive application** of the Regulation **to non-EU based controllers** operating worldwide accessible websites, the Regulation should clearly provide that certain cases such as a **third country e-commerce website, which can be accessed and viewed by individuals in the EU should not in itself be considered as "offering of goods and services to EU residents".** In exchange, AmCham Romania recommends that **concrete criteria such as offering shipping to EU Member States should be considered.**

11. The one-stop-shop principle

Today, companies that operate across Europe are subject to multiple and divergent national data protection regimes. To address this problem, the Regulation introduces a "one-stop-shop principle" based on the location of an organisation's "main establishment". In other words, the Regulation provides for single competent data protection authority (DPA) to oversee all data processing activities of data controllers throughout the EU.

Although this approach offers a significant improvement over the existing, fragmented regime, the Regulation applies different tests for controllers and processors in determining their country of main establishment. To determine a **processor's main establishment,** the Regulation looks to the place of **"central administration**" – a term that is undefined and in practice may have no relation to the market where data is in fact processed. The Regulation uses a somewhat more sensible test for **controllers,** based on **where "main decisions" about processing** are taken in the EU – but then introduces **an unclear and circular test relating to "main processing activities"** in the context of an establishment. The result may be that multiple data protection authorities claim jurisdiction over organisations, especially organisations that act as both processors and controllers in multiple Member States. For example, a cloud provider that plays the role of data processor in relation to its cloud customers, may be at the same time a data controller as regards the data of its own employees. Therefore, AmCham Romania considers that the Regulation should subject controllers to the same test as processors when they are playing both roles. **As most of the IT companies representing the Information Technology & Communications Committee within AmCham Romania are global companies and, in most cases, cloud computing operators, and in order to ensure that the competent "one stop shop" DPA is the one which is naturally best situated to exercise adequate oversight and enforcement powers, it would be more relevant to link the main establishment to the location where the data processing decisions are taken.**

Moreover, in order to ensure consistency of the new legal framework, the "one stop shop" principle should be fully integrated throughout the Regulation. In this sense, key provisions such as the right of data subjects to lodge complaints with the DPA (Article 73), the right of data subjects to bring proceedings before the courts of their place of residence (Article 75) and rights of DPAs to take provisional measures against controllers established in other member states (Articles 55 and 56) do not recognise the primacy of the competent supervisory authority determined as per the "one stop shop" principle. Therefore, it is unclear whether enforcement of the Regulation will rest with that authority, or alternatively, the enforcement will be ensured by the DPA in the country where the data controller/ processor is located. Similarly, it is unclear to which authority data subjects may lodge their complaints.

Furthermore, **the Regulation does not provide any guidelines in respect of the competences and relationship between the DPA, determined as per the one stop shop principle, and the DPAs in**

each Member State. This could cause major procedural difficulties for data controllers and processors as well as possible conflicts of competence, and different interpretations and enforcement measures within several DPAs which would ultimately lead to delay in procedures. Unless DPAs would be required to follow the same procedural rules and operate based on the same standardised documents, each DPA will develop its own practice and working documents (e.g. data breach notification forms, contractual clauses, and other templates), depending on its experience and level of sophistication. In this respect **AmCham Romania is concerned that the Romanian DPA might not be able to face the challenges imposed by the Regulation, due to its limited resources, both in terms of headcount, financials and training**.

In order to mitigate the above potential negative consequences, AmCham Romania recommends that the Regulation clearly determines how several relevant DPAs are to cooperate so that the interests of data controllers, data processors as well as individuals are not affected. In addition to this, Chapter VII (co-operation and consistency) should explicitly require DPAs to refer complaints and investigations relating to a controller to that controller's competent DPA according to the "one stop shop" principle.

12. Certifications

The Regulation helpfully promises to promote certifications and other mechanisms to encourage organisations to demonstrate their security and privacy commitments. AmCham Romania welcomes such efforts. Moreover, it would like to **encourage the Regulation to support international certifications, including EU-adopted international certifications, instead of sector-specific or regional certification programs, which can lead to fragmentation of standards in privacy and data security.**

Given that, in general, the industry is better equipped to keep up the pace with technological developments than state institutions, AmCham Romania recommends that certification mechanisms be industry-driven, with oversight and help from the Commission if required.

13. International data transfers

In line with AmCham EU's position, **AmCham Romania welcomes many of the proposed amendments regarding international data transfer, in particular the fact that Binding Corporate Rules ("BCR") may be adopted by both data controllers and data processors** and require approval only from one DPA. **This will significantly reduce the costs and administrative burdens for Romanian data controllers given that, to AmCham Romania's members' knowledge, the Romanian DPA has never recognized BCRs as legitimate grounds justifying international intra-group data transfer, even in cases where such BCRs were approved by an homologous DPA in another Member State.**

However, AmCham Romania believes that there are several aspects of the Regulation which may be further improved. In this sense, the Regulation should clarify that **no authorization or other administrative requirements are further required in case a country, territory or a processing sector within that country has been considered as adequate by the European Commission.** Moreover, the Regulation should make clear that derogations enabling transfers to a country, territory or sector affected by a negative adequacy decision are also applicable. Therefore, Article 41(6) should make clear that "*without prejudice to Article 42 and Article 44*" means that in case of a negative adequacy decision of the European Commission, data transfers to the concerned third country are nevertheless possible based on these articles.

In addition to this, given the vast technological developments in the area of cloud computing, AmCham Romania believes that **the Regulation should provide that international data transfers through cloud computing services offer adequate safeguards in case cloud computing service providers have acquired a recognised certification in this field.**

Moreover, AmCham Romania asserts that the prohibition of data transfers that are frequent or massive, listed in Article 44 paragraph 1 letter h), does not benefit cloud service providers, given the lack of clarity of what the term "massive" means. Moreover, AmCham Romania recommends that rather than prohibiting such transfers, the Regulation should allow organisations to define appropriate safeguards for "massive or frequent" data transfers.

Also, given the numerous data transfers to the US that take place in connection with Romanian businesses, **AmCham Romania advocates for the Regulation to explicitly mention the fact that the EU-US Safe Harbor program remains in place in order to avoid any possible non-clarities.**

14. Data breach notification

The Regulation requires data controllers to notify a personal data breach to the DPA "*without undue delay and where feasible, not later than 24 hours after having become aware of it*".

Although AmCham Romania acknowledges the need to notify data breaches promptly, **the complexity of each particular data breach makes it difficult to subject all data breaches to a fixed notification term.** Moreover, the 24 hours target set forth by the Regulation is not realistic and counterproductive. Due to technical and administrative constraints, filing a complete data breach notification within 24 hours is virtually impossible. **Data controllers need more time to investigate exactly what data has been breached, the potential impact on data subjects, as well as any remedies to mitigate any adverse effects.** It would be premature to notify a breach before all such information is collected and carefully considered. **Data controllers should be allowed to focus more on gathering information about the affected data and related data subjects and to assess the impact of the breach, rather than focus on administrative burdens.** Therefore, in line with the breach rules in the 2009 additions to the e-Privacy Directive (2009/136), companies should be required to notify DPAs "without undue delay" rather than within a 24-hour window. Severe penalties for non-compliance should be reserved for those controllers who wilfully and repeatedly fail to notify.

Moreover, the Regulation seems to require that all data breaches, both serious and non-serious, must be notified to the DPA, irrespective of the actual impact they have on data subjects. In AmCham Romania's opinion, this data breach notice regime is not workable in practice as it threatens to **overwhelm DPAs and data subjects with notices about breaches that may ultimately prove immaterial or trivial.** In turn, this may lead **data subjects ultimately to ignore all notices** and to impair the ability of DPAs to effectively tackle the truly serious breaches. In this sense, **Amcham Romania would like to express its concerns about the ability of the Romanian DPA to handle data breach notifications thoroughly, effectively and in a timely manner, considering its limited resources of qualified personnel.**

Excessive notices may also lead to an unreasonable **level of fear among Romanian** and **European internet users**, which may negatively affect the use of internet-based technologies.

To ensure the regime is effective, controllers should be required to notify data subjects and/or regulators of a breach only when there is significant risk of serious harm to the data subject. Criteria to be considered in making this assessment could include the type of data involved and its sensitivity, the nature of the breach, and the type of harm threatened by the breach.

Finally, AmCham Romania recommends that the **exemption from the data subjects notification requirement in case data has been rendered unintelligible by encryption or equivalent means (Article 32) be extended in respect of DPA notifications as well.**