AmCham EU Speaking Points on GDPR Implementation

***

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 2015, directly supports more than 4.3 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

***

BACKGROUND PAPER

American Chamber of Commerce to the European Union (AmCham EU)
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Register ID: 5265780509-97
Tel: +32 (0)2 513 68 92 | www.amchameu.eu

Secretariat Point of Contact: Maika Föhrenbach; [mfo@amchameu.eu] +32 (0)2 289 10 11

10 January 2017

AmCham EU Speaking points on GDPR Implementation Priorities[1]

On 25 May 25 2018, the General Data Protection Regulation ("GDPR") will become applicable, bringing significant changes to data protection rules across the European Economic Area (EEA).

The next months will be marked by significant activity at the EU and Member State level, including rulemaking (the GDPR requires implementation and allows Member States to legislate on specific issues), issuing of guidance, and adopting codes of conduct and certification schemes.

To help AmCham EU develop positions on GDPR next steps, this document provides background and sets out an initial high-level proposal for AmCham EU messaging on eight key issues:

[1] See AmCham EU's Position on GDPR Implementation Priorities here.

1. PROFILING

1.1 The issue

Consistent with AmCham EU's calls during the legislative process, the GDPR largely regulates profiling[2] the same way as other "processing of personal data" (see Recital 72). However:

- The GDPR specifically regulates profiling when it is used for fully automated decision-making that can produce "legal or similar significant effect[s]" for individuals ("ADM"). ADM is prohibited without the data subject's explicit consent, contractual necessity, or an authorizing law. The GDPR also penalizes failures to implement "appropriate mathematical or statistical procedures" for profiling used for ADM (Recital 71, Article 22); and ADM based on profiling needs a data protection impact assessment ("DPIA") (Article 35).
- In addition, online profiling is a basis for extraterritorial application of the GDPR to companies that don't have an establishment in the EU (Recital 24); individuals must be informed not only about the existence of profiling, but also its *consequences* (Recitals 60 and 63); and profiling related to direct marketing is subject to the data subject's absolute right to object (Recital 70).

1.2 Next steps

- The EU and Member States may consider whether to enact specific laws for ADM based on profiling for specific situations, *e.g.* for automated fraud prevention (Article 22).
- EU and Member State authorities may also issue guidance, including on what types of profiling constitute "high risk processing," which is subject to enhanced compliance obligations (Articles 35 and 57; Recital 72).

1.3 Proposed key messages and AmCham EU talking points

- Profiling plays a key role in many beneficial business activities that deliver economic growth, including analytical work to improve how services are run, delivered, and personalized, and fraud prevention. Without profiling, many services, ranging from insurance and financial services to online websites, as well as multiple routine business functions (such as recruitment), would be impaired. Some simply would not be able to function, or would cease to be economically viable.
- At the same time, we recognize the privacy concerns that profiling can raise when it may have negative or discriminatory effects on individuals. Therefore, we understand the application of specific requirements when profiling is used as the basis for automated decision-making that can have legal or similar significant impacts on individuals.
- When formulating any guidance on "legal or similar significant effects", DPAs should focus on identifying *actual negative* and *discriminatory impacts*. Any guidance should make clear that "legal or similar significant effects" are not typically generated by profiling used in beneficial activities as part of routine business operations, such as fraud prevention, product and service personalization (including targeted advertising) and service improvement. Indeed, it is recognized in Recital 71 that activities that produce such effects include "automatic refusal of an online credit application or e-recruiting practices without any human intervention," rather than routine personalized services we have described.

[2] Profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;"

- When formulating any guidance on what the phrase "appropriate mathematical or statistical procedures" means in the context of ADM based on profiling, DPAs should consult with industry in order to have regard to the state of the art and standard industry practices across various sectors.
- EU and Member State legislators should also ensure that these important rules are well integrated with the rest of European law. Guidance and implementing measures for the new Network and Information Security (NIS) Directive should clearly state that it provides a legal basis for covered entities to use ADM as part of cybersecurity measures.

2. ONE-STOP SHOP (MAIN EU ESTABLISHMENT)

2.1 The issue

The GDPR will introduce a "lead DPA" in multi-jurisdictional matters, but fails to deliver on its "one-stop shop" promise: multiple national regulators will continue to scrutinize and regulate cross-European businesses (Articles 55 and 56). More specifically, local DPAs retained sole authority over local infringements that do not have a multi-Member State dimension (Article 56), gained powers to intervene in investigations and dispute rulings by the lead DPA in multi-jurisdictional matters (the EDPB will act as neutral arbiter in those cases) (Articles 60 and 65), and can bypass the lead DPA on multi-jurisdictional matters in "urgent" situations (Article 66).

Confusingly, the test for determining "main establishment" (and thus the location of the lead DPA) differs depending on whether an entity is acting as controller or processor (Article 4(16)). For controllers, the main establishment is the place of "central administration," unless management decisions concerning processing are taken elsewhere. For processors, the main establishment is either the place of central administration, or, if the company does not have one, then wherever the data processing actually takes place in the EU.

2.2 Next steps

The WP29 has made "one-stop shop" issues a priority for 2016, and will produce guidance on determining where the main establishment is located. The WP29 will also establish procedures for information sharing and consensus-building between national DPAs.

2.3 Why guidance or rulemaking is needed

- The drafting and application of the "main establishment" test is confusing and vague, particularly for data processors.
- It also is not clear how this principle will apply to companies that are both controllers *and* processors; or to companies that are not established in the EU, especially when they are based in a country with recognized adequate protection such as Switzerland; or to multi-national investigations in which one DPA alleges that there has also been a breach of a national implementing provision.

2.4 Proposed key messages and AmCham EU talking points

- The one-stop shop mechanism was intended as a key benefit for businesses under the GDPR, in order to increase the attractiveness of the European single market for investment and cross-border service provision. However, the compromises reached for the adoption of the GDPR undermines the value of the one-stop shop concept.
- There is still a significant lack of certainty as to how the "main establishment" is determined, especially in complex cases. One way to help restore value to the one-stop shop concept, and at the same time to encourage business to invest by boosting business certainty, would be to endorse in guidance the idea that if a company designates a location as its main establishment, for current companies to be done prior to the effective date of the GDPR (May 25, 2018), that designation presumptively decides the issue, unless clearly contrary to facts on the ground or the GDPR. Likewise, joint controllers (whether belonging to the same group of entities or not) should be encouraged to designate a single competent authority to monitor their joint data processing activities.
- The urgency procedure, in particular, which enables local DPAs to intervene in lead DPA scrutiny, needs to be carefully delineated in guidance, in order to prevent conflicts between DPAs and to preserve the purpose and benefit of the one-stop shop concept.

- In particular, the "exceptional circumstances" considered to trigger the urgency should truly be "exceptional", meaning that there is a significant and possibly irreparable infringement of data subjects' rights and freedoms pursuant to the GDPR.

3. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS) AND HIGH-RISK PROCESSING

3.1 The issue

The GDPR sets out a number of requirements designed to encourage data controllers to effectively manage data protection risks. This includes requiring Data Protection Officers ("DPOs") to pay particular attention to high risk processing (Article 39(2)). In addition, controllers companies must undertake data protection impact assessments (DPIAs) prior to engaging in potentially "high risk" processing (Article 35). The GDPR also mandates DPIAs in a number of other situations, including (i) ADM based on profiling; (ii) large-scale processing of sensitive personal data; and (iii) CCTV or other "systematic monitoring of a publicly accessible area on a large scale" (it is not clear if this only means in the physical environment, or potentially also tracking on large, publicly-accessible websites) (Article 35, Recital 91). DPAs can also draw up lists of other specific types of processing that do or do not require DPIAs (Article 35); drafts of those lists must be approved by the EDPB (Article 64(1)).

Where DPIAs are required, they must contain at least a systematic description of the envisaged processing and its purposes, including, where applicable, the legitimate interest pursued by the controller; an assessment of the necessity and proportionality of the processing; and an assessment of the risk and the measures envisaged to address the risks (Article 35(7)).

If after conducting DPIAs, organizations find that risk remains high in the absence of mitigation, they must consult with DPAs, in a procedure that could take several months. DPAs are also empowered to require changes – or even a halt – to the planned processing (Article 36). In some cases, it may be necessary to consult the public in the context of a DPIA (Article 35(9)).

Once processing has commenced, the controller must review the processing to make sure it complies with the DPIA, particularly when there is a change in the risk presented by the profiling (Article 35(11)).

3.2 Next steps

- The WP29 has been prioritizing issuance of guidance on high risk processing and DPIAs for 2016.
- The GDPR invites the EDPB and DPAs to publish lists of processing that present a high risk (or "whitelists" of operations deemed low risk), and appropriate risk-mitigation measures (Article 35). "High risk processing" lists must be submitted to the DPA/EDPB to ensure that each DPA's list is consistent with those of other DPAs (Article 64).
- Guidance on identifying and assessing risks and "best practice" mitigating measures may also be covered in approved codes of conduct, certifications, EDPB guidelines or internal company guidance from DPOs (Recital 77).

3.3 Why guidance or rulemaking is needed

- There is a need for clarity on what constitutes "high risk" processing to identify when DPIAs, prior consultations, and/or special risk-mitigation measures are required. If the "high risk processing" threshold is set too low, routine business activities will become subject to burdensome administrative measures. There is also a danger that recommended mitigation measures will be too demanding and/or too inflexible.
- There is a risk that DPAs will prescribe their own, local DPIA requirements in addition to those in the GDPR: a single DPIA might then not be able to satisfy all DPAs, multiplying the administrative burden and impairing the harmonization which is one of the key goals of a Regulation.

3.4 Proposed key messages and AmCham EU talking points

- The special protections set out in the GDPR for "high risk processing" activities have the potential to benefit data subjects and businesses by improving product and service design. But these processes can also add substantial administrative burdens without delivering significant improvements to data subject privacy. It is important that regulators approach DPIAs pragmatically, in order not to unduly hinder innovation.
- A key concern is that the rules in this area are not clear, and could result in divergent interpretations across the EU, in particular if different national DPAs develop diverging whitelists / blacklists. As a first step, there should be additional context provided regarding what constitutes "high risk processing", for example through factors or criteria that data controllers can take into account when conducting their internal assessments. These criteria should be based on careful study and evidence that the relevant processing carries a risk of serious and irreparable harm.
- In addition, when considering risk, DPAs should bear in mind that *all* processing, whether high risk or not, is subject under the GDPR to significant redress and supervision, heavy sanctions, and duties to put in place appropriate data protection measures and follow privacy by design and default principles. These protections limit the number of scenarios where there will be a genuine and proportionate need for the additional protections reserved for "high risk" situations, including the adoption of DPIAs.
- The same pragmatic approach should be taken to determining what operations are whitelisted as *not* being high risk. Routine business operations, such as Human Resources administration, should generally be whitelisted. In order to ensure that whitelists (and blacklists) reflect modern practices, industry should be consulted before lists are drafted.
- In terms of how DPIAs are done, organizations should be permitted to carry out DPIAs with flexibility, consistent with the context in which they are processing data. This reflects the "accountability" principle that is an underlying principle of the GDPR as a whole (see article 5).
- DPAs should avoid the temptation to dictate DPIA content, format, frequency, *etc.* (beyond what is already in the GDPR); instead, businesses need to remain free to exercise their judgment to match the context. To the extent DPAs *do* publish such guidance, it is critical that the GDPR "consistency mechanism" apply in order to ensure that the guidance is consistent across Member States. (Or, alternatively, guidance should clarify that when businesses carry out DPIAs, they should do so in accordance only with the guidance and DPIA specifications of the lead DPA.) These measures will help ensure that businesses understand DPIA requirements and that differences in execution between Member States are minimized.
- The "prior consultation" process should also be approached pragmatically, and required only where strictly relevant. The Regulation is clear that prior consultation is only triggered when the data controller determines a particular type of processing qualifies as high risk, but is unable to mitigate these risks to data subjects.
- Businesses will look to DPAs and the EDPB to provide guidance on a number of key issues on this topic, in particular including: (i) when is prior consultation triggered? (ii) When and how will DPAs advise that the procedure is over? (iii) Will only the lead DPA need to be consulted when processing has a multi-national scope? And (iv) will there be an urgent consultation process (*e.g.* for small, one-off but potentially high-risk and time-critical processing operations)? DPAs should work with industry to resolve these questions before the GDPR comes into force.

4. PERSONAL DATA BREACHES AND NOTIFICATION

4.1 The issue

GDPR requires notice to DPAs of a data breach "without undue delay," unless the breach is unlikely to result in a "risk to the rights and freedoms of individuals", as well as notice to data subjects where a breach is likely to result in a "high risk" to their rights and freedoms. Notification is not required if the data is secure (e.g., encrypted) or if the risk has been mitigated.

4.2 Next steps

The Article 29 WP work programme 2016-2018 indicates that the technology subgroup will be working on data breach impact assessments, next to data protection impact assessments. As part of its work the subgroup will consider whether previous opinions need to be updated in light of the GDPR.

4.3 Why guidance is needed

- Without more objective standards, data subjects could receive notices so frequently that they become unable to distinguish between breaches that reflect significant risk and those that reflect minimal or no risk, rendering notices ineffective while imposing huge costs on data controllers.
- The upcoming e-privacy regulation is likely to remove existing breach notification provisions and refers back to the GDPR.

4.4 Proposed key messages and AmCham EU talking points

- Guidance is needed regarding the types of breaches that create a "risk" requiring notice to DPAs, and what additional factors create a "high risk" requiring notice to data subjects. Without more objective standards, data subjects could receive notices so frequently that they become unable to distinguish between those that reflect significant risk and those that reflect minimal or no risk, rendering notices ineffective.
- We suggest that guidance should include at least the following factors: (1) nature and extent of the Personal Information (PI) involved, including the types of identifiers and the likelihood of re-identification, (2) the unauthorized person who used the PI or to whom the disclosure was made, (3) whether the PI was viewed or acquired, (4) the extent to which the risk to the PI has been mitigated.
- In addition, guidance is needed on which DPA needs to be notified of the breach in cases where a breach involves several Member States.
- Finally, guidance is needed for recordkeeping requirements particularly where little or no risk is likely to arise from the breach.

5. APPROVED CODE OF CONDUCTS AND CERTIFICATION

5.1 The issue

The GDPR empowers DPAs and the Commission to approve codes of conduct and certification schemes that "flesh out" GDPR rules for particular situations or industries (for example, the GDPR sets out the opportunity for codes of conduct on "pseudonymization") (Articles 40-43).

Codes of Conduct

The GDPR allows industry to draft codes of conduct, provided that they include compliance monitoring and governance mechanisms. Such codes can then be submitted to a national DPA, which must review the code and pass it onwards to the EDPB in cases where the code would impact cross-border processing. If the EDPB approves the code, the draft passes to the Commission, which can approve the code with a Decision to give the code EU-wide effect (Article 40). With regard to Codes of Conduct, the submission to the national DPAs is voluntary, whereas Certification Schemes have to be submitted.

Certification Schemes

The GDPR sets out a similar process for the creation of certification schemes. These schemes can be issued only by DPAs or accredited certification bodies. A scheme approved by the EDPB can become a European Data Protection Seal, which companies are permitted to display if they comply (Article 42).

The GDPR suggests that codes of conduct and certifications are good measures of assurance that adherents comply with the GDPR in a given an area (Article 42). For example, controllers might be able to choose certified processors, and could then cite that choice in DPIAs, etc., as a compliance/risk mitigation measure. The GDPR also indicates that seals etc. should be considered by DPAs when assessing fines (Article 83(2)).

Approved codes and certifications can also enable data transfers from the EU to organizations in third countries. Where a controller or processor that is not subject to the GDPR makes a binding commitment to adhere to a code or certification, this can be the "adequate safeguard" necessary for transfers (Articles 40(3) and 42(2)).

5.2 Next steps

- Industry can take the lead in setting up codes of conduct and working with accredited certification bodies to design certification schemes (Article 40(2)). Once drafts are ready, they can be submitted to DPAs and/or the EDPB for approval (Article 40(5-8). The Commission can give EU-wide effect to an approved code of conduct (Article 40(9)).
- The Commission can adopt delegated acts to specify further requirements for certification mechanisms (Article 43(8, 9)). DPAs or the EDPB can also decide the criteria which certification schemes need to meet before they get approved (Articles 42(5), 58(3) and 63).

5.3 Why guidance or rulemaking is needed

- As noted above, codes / certifications could have real benefits for industry. They have the potential to both protect businesses from regulatory enforcement, and to act as sales hooks in certain industries. They also help to establish standard processes, which can increase business certainty.
- At the same time, codes / certifications might also pose the risk of adding rigidity. In the past, this has been the case for the code on conduct on direct marketing. The publication of a strict code or certification scheme could set high bars for the rest of a sector, increasing the expectations placed on non-certified companies too.

5.4 Proposed key messages and AmCham EU talking points

- Industry welcomes the GDPR's provisions for the formalization of codes of conduct and certification seals. Well-designed codes and certifications have the potential to set high standards of practice across industries, at the same time as ensuring business certainty. Data subjects and customers will also benefit from increased transparency and accountability delivered by codes / certifications.
- At the same time, codes / certification schemes must be pragmatic and should never be less flexible than the basic rules of the GDPR. They should set out examples of approved ways of complying with requirements, but should avoid highly granular criteria and should not favor certain business models over others.
- While codes have the potential to increase transparency and accountability, if ill-designed, they also threaten to create barriers to entry for start-ups, as well as increasing administrative burdens for existing businesses. For this reason, codes must be developed carefully, and with unilateral assent from industry. The industry-led Data Protection Code of Conduct for Cloud Service Providers (European Commission C-SiG subgroup on Data Protection Code set-up in 2013) which is being finalized is a good example of how this process works, following these guidelines.
- The negotiation procedure mechanism should allow for fluid interaction between the representatives of the code and the EDPB rapporteur as opposed to a static written procedure. In the case of the Data Protection Code of Conduct for Cloud Service Providers, it would have helped for a more timely adoption.
- Codes / certifications should also interoperate, wherever possible, with international practice. It is important that European standards and practices do not diverge substantially from data protection regimes in third countries, in order to avoid market fragmentation and divergence of privacy and security practices.
- Once a code or certification is approved, DPAs, the EDPB and the Commission should work together to incentivize adoption of the code, including through setting out forward-guidance on enforcement priorities in relation to businesses in connection with that specific industry. However, codes and certifications should remain voluntary, as the GDPR makes clear.

6. DATA PORTABILITY

6.1 The issue

The GDPR introduces a new right to "data portability" for data subjects (Article 20). The right, which applies where processing is based on the data subject's consent or where processing is necessary to fulfill a contract between the controller and data subject, enables data subjects to demand that data they have "provided" to a controller be returned to them "in a structured, commonly used and machine-readable format." It also requires controllers to allow data subjects to transfer this data to another controller "without hindrance," and empowers data subjects to require controllers to transfer data "directly" from one controller to another, "where technically feasible." GDPR recitals encourage data controllers to develop "interoperable" formats to facilitate compliance with these requirements (Recital 68).

6.2 Next steps

The Working Party Article 29 action plan for 2016 includes an item to develop guidance on the data portability right.

6.3 Why guidance or rulemaking is needed

The data portability concept is novel, and a number of concepts need to be clarified in order for it to work in practice. This includes a common understanding of the term "structured, commonly used and machine-readable." Guidance to clarify how the phrase "technically feasible" will be interpreted may also be helpful, so that firms can understand when and how they need to develop and maintain interoperability.

6.4 Proposed key messages and AmCham EU talking points

- Industry welcomes the right of data portability, which should help to enable the free movement of information in the Single Market.
- At the same time, because the right of data portability is new, guidance will be required. That guidance should clarify that this right covers only information actively provided by data subjects – for example, information filled in by the data subject in data entry fields like their name or address – but not data generated by a data subject's actions on or use of a service, such as metadata about the user's use of a service or telemetry data collected about the operation of the service in general, data inferred about a data subject by the company, or transformed data (e.g. using Big Data technologies) and therefore including proprietary rights belonging to the data controller (or the data processor).
- Guidance should also clarify that "technical feasibility" excludes scenarios where new systems or capabilities would need to be built in order to enable direct exchange. Furthermore guidance on how this principle is to be applied for employee data (in particular when employees leaving an organization invoke this right) would be welcome.
- Likewise, we would welcome clarifications as to how regulators will interpret the phrase "structured, commonly used and machine-readable," in order to enable industry to develop appropriate compliance procedures and capabilities in existing systems. Our view is that such formats should be limited to only the most popular and common standards for structured documents and web data, potentially with other formats used only where data cannot be expressed through these common formats.

7. SANCTIONS

7.1 The issue

The GDPR substantially expands the ability of DPAs to impose fines (in addition to providing for other non-fining enforcement powers -- see Articles 58 and 84). While the amount of a fine will depend on various factors, fines can reach the greater of EUR 20,000,000 or 4% of total worldwide annual turnover (Article 83).

7.2 Next steps

It is not clear whether or when DPAs plan to release any new guidance or further rules about the use of these new fining and other enforcement powers.

7.3 Why guidance or rulemaking is needed

- The GDPR allows fines *and/or* other enforcement measures to be taken. Any guidance should recommend a graduated, warning-first approach, with significant fines imposed only for the most serious violations, especially in the beginning when stakeholders are still in the learning curve and as long as guidance is in progress.
- It is unclear to what extent opening clauses elsewhere in the GDPR (*e.g.* allowing additional rules/safeguards in research) allow different (and perhaps higher or lower) fines than the caps set out in Article 83. In addition, Article 84 requires Member States to establish penalties "for infringements which are not subject to administrative fines pursuant to Article 83". Guidance should clarify what these areas are (if any), and what Member States are allowed (or not allowed) to do in this respect.

7.4 Proposed key messages and AmCham EU talking points

- Industry welcomes the development of more robust enforcement and stronger sanctions in European data protection law. Sanctions should be given if there is a clear breach, and can deter bad practices within companies.
- That said, they are only effective if they are meaningful. Some of the most effective regulators in Europe make extensive use of warning letters and other "soft" enforcement measures prior to, when necessary, proceeding to formal sanctions, cease and desist notices, *etc*. The balanced use of a full spectrum of powers, and dialogue with industry, should be endorsed by the EDPB in order to create a harmonized, well-functioning and proportionate enforcement environment. This is particularly true and necessary considering that when the GDPR will start to apply, guidance will not be available to cover all aspects. Accordingly, we believe some leniency will be required until the DPAs and EDPB have issued guidance that is comprehensive and adequate to back up the GDPR sufficiently and clarify its intended application.
- An important aspect of such guidance should also concern cross-border enforcement issues. The EDPB should clarify that fines should account for whether an individual or entity has been subject to sanctions in another proceeding for the same conduct, so that a party is not penalized twice for the same conduct.
- It is also important to prevent divergent remedies and legal outcomes in different Member States. For example, guidance should be issued to clarify currently unspecified additional powers to impose penalties set out under Article 84, to pre-empt fragmentation caused by different Member State interpretations of this clause.

8. DATA PROTECTION OFFICERS (DPOS)

8.1 The issue

The GDPR requires controllers and processors to appoint DPOs if, among other circumstances, the "core activity" of a controller/processor is to process data which, "by virtue of [the data processing's] scope, purpose or nature," requires the systematic monitoring of data subjects on a large scale, and/or where large-scale volumes of sensitive categories of data would be processed (Article 37).

DPOs are charged with monitoring compliance of the relevant organization with the GDPR, and with various other tasks, including cooperating in the production of DPIAs where relevant. They must be independent, involved in all "issues which relate to the protection of personal data", and must be supported by the controller/processor with resources accordingly (Articles 37 - 39).

8.2 Next steps

The WP29 is planning to issue guidance on DPOs towards the end of 2016.

8.3 Why guidance or rulemaking is needed

- Many issues relating to DPOs still lack clarity. In particular, the meaning of the terms "core activity," and "large scale" processing remain vague, which is important because these terms will determine the threshold that requires businesses to appoint DPOs.
- It is also unclear whether DPOs can be legal persons, or whether they must be individuals and whether they can be external or only internal persons. The meaning of DPO independence – in particular if a DPO is an employee of a large business – is also unclear, as is the precise role of a DPO in terms of ensuring an organization's compliance with the GDPR (e.g. can a DPO be an HR or a Marketing Manager within a company?). The GDPR is also unclear as to whether DPOs must be – in order to be deemed capable of carrying out their duties mandated by the GDPR – physically located in Europe.

8.4 Proposed key messages and AmCham EU talking points

- DPOs represent an improvement on the data controller registration regime maintained by the Data Protection Directive, and will play an important role in enhancing business accountability and compliance with the GDPR.
- Further guidance on this topic would be helpful. In particular, key terms in the GDPR are unclear, making it difficult to know when DPOs must be appointed under the law. Guidance should clarify, in particular, the meaning of the terms "core activities" and "large-scale processing," for instance by giving clear examples of activities that *do not* require DPO appointment, *e.g.* normal recruitment and HR practices, a company's use of cookies to monitor its own websites, or routine use of everyday business contact information (*e.g.* for customer relationship management (CRM), marketing or contract performance purposes).
- Guidance could also be issued to clarify the role of DPOs and how they should maintain their independence (with clarification that they can be held accountable to management and boards); how SMEs should approach the issue of appointing DPOs, and whether DPOs can be legal entities (*e.g.* SMEs would prefer to use part-time DPOs) or external bodies (like law firms on an "as-needed" basis). Regulators should consult with industry to help produce best practices and working examples in order to provide further clarity in this area.
- In order to promote innovative business models and operational flexibility, in particular for large businesses that operate across many jurisdictions globally, guidance should clarify that data protection officers can be located everywhere within the EEA.