American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

Comments to the European Data Protection Board's (EDPB) draft recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB Guidance)

Summary

General: a guidance impossible or extremely onerous to comply in practice, disproportionate and damaging EU citizens and businesses

- The EDPB Guidance places extremely onerous obligations on organizations to comply in practice since it imposes a specialist multi-jurisdictional legal advice and an expensive and time-consuming implementation.
- The EDPB Guidance undermines and will damage EU citizens and organizations of all sizes and sectors, based on a disproportionate approach against the Charter and the EU objectives.
- The collective impact of this EDPB guidance will be a dramatic reduction in personal data transfers from the EU depriving EU organizations and its citizens of fundamental rights to trade and communicate with those outside the EEA.

Essential equivalence: a guidance that neglects taking into account CJEU recent surveillance case law and post-2016 US surveillance changes

- The EDPB Guidance does not take into account that US surveillance laws and practices have evolved since 2016 (which is the framework analyzed in the Schrems decision).
- The EDPB Guidance obviates that the US and the EU share common values and interests, in terms of respect human rights, the rule of law and the cybercrime collaboration.
- The EDPB does not take into account the recent CJEU case law that confirms that national security can justify serious interferences with individuals' rights, in certain cases and subject to proper safeguards.

Supplemental safeguards: a guidance that puts organizations in an impossible situation, inappropriately focuses on technical safeguards and contradicts EU Member States surveillance requests

- The EDPB Guidance puts forward safeguards that are unworkable. Day-to-day processing would be prohibited at enormous cost to EU organizations and ultimately citizens.
- The EDPB Guidance inappropriately focuses on specific technical measures.
- The EDPB requires strong encryption while EU Council proposed a regulation regarding the imposition of backdoors to encrypted communications for surveillance purposes.
- In contradiction with the CJEU, the EDPB Guidance seeks to prohibit reliance on SCCs for transfers to key US service providers.

Derogations: an unjustified overly restrictive interpretation contrary to CJEU and GDPR goals (i.e., to enable transfers rather than avoiding them)

- A balanced interpretation is not necessarily a restrictive interpretation.
- Some of these derogations are not and cannot actually be "exceptional", as wrongly construed by the EDPB, such as the performance of international communications or international money transfers. In any event, the EDPB Guidance fails to distinguish between the business transfers and the transfers due to governmental access requests, which are exceptional by nature.
- The EDPB should take this opportunity to holistically revisit the overly narrow interpretation of the derogations in light of the *Schrems II* ruling and that the goal of GDPR provisions on international transfers was to enable them rather than prohibit them.

1. **General: a guidance impossible or extremely onerous to comply in practice, disproportionate and damaging EU citizens and businesses**

- **The EDPB Guidance places extremely onerous obligations on organizations to comply in practice: a specialist multi-jurisdictional legal advice and an expensive and time-consuming implementation**
    - **A specialist multi-jurisdictional legal advice and continuous assessment of compliance.** The six-step roadmap set out in the EDPB Guidance places a heavy burden on organizations exporting data and will require significant resources to comply (and to maintain compliance on an ongoing basis). For example, the roadmap requires a detailed analysis of the characteristics of every transfer, an assessment of all applicable local laws (including complex surveillance laws) and how they impact on the requirements under EU law (which in and of itself requires a detailed assessment). This is a highly complex assessment requiring specialist multi-jurisdictional legal advice which many businesses will not have otherwise have available to them. The cost of obtaining that advice will be prohibitively expensive for many. Moreover, despite the legal advice required for this assessment, a detailed analysis on transparency, how the data protection authorities implement data protection provisions in the respective state and particularities on each transfer is also required and involves extensive human, time and financial resources.
    - **Prohibitively expensive and time-consuming implementation.** Similarly, the EDPB Guidance call for the implementation of technical measures and fundamental changes to processes to rely on the SCCs which would be prohibitively expensive and time-consuming even if they were capable of being implemented (for many they are not).
    - **Impossible or unrealistic effort.** As many of those affected will be small businesses and organizations, it will be incredibly difficult (if not impossible) in practice to comply with the EDPB Guidance. Even for larger organizations with time, resources and expertise, achieving compliance with these obligations is totally unrealistic given the scale at which they need to be carried out to comply with the EDPB Guidance (i.e., the conducting of a detailed assessment for each and every transfer, requiring specialist legal advice in respect of the laws each third country and how it impacts of the protection of data).
    - **Conflict of law and business opportunities lost.** Organizations will be confronted with the difficult decision to continue to trade and use services supplied by non-EEA businesses risking GDPR fines or cease availing of these services and trading relationships thus foreclosing global markets and opportunities resulting in lost revenues, opportunities and ultimately jobs. The collective impact of this EDPB guidance will be a dramatic reduction in personal data transfers from the EU depriving EU organizations and its citizens of fundamental rights to trade and communicate with those outside the EEA.
- **The EDPB Guidance undermines and will damage EU citizens and businesses, based on a disproportionate approach against the Charter and EU objectives**
    - **A disproportionate approach.** The EDPB Guidance undermines and will damage EU businesses by failing to adopt a proportionate approach (as required by EU law) and by not acknowledging the importance of other fundamental rights and freedoms, including the right to freedom of expression and information (Articles 11 and 7 of the Charter) and freedom to conduct a business (Article 16 of the Charter). This is in conflict with GDPR itself with Recital 4 GDPR stating "*[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*". The right to the protection of personal data must co-exist and be balanced against these other fundamental rights and governments' interest in protection people from terrorism and crime. The EDPB Guidance fails to have due regard to the impact on businesses, their customers and EU citizens.
    - **Impact on all sizes, all sectors.** Today, practically no organization, irrespective of sector, would be able to do business, let alone take part in international trade, without the ability to transfer data cross-borders. The EU's global trade is inextricably linked with the cross-border flow of data with partners outside the EEA, including in particular the US. The SCCs are the principal legal instrument relied on by EU-based businesses for transferring personal data to third countries. These businesses and

organizations are looking to the EDPB Guidance for guidance as to how to continue to carry out transfers. Yet, the EDPB Guidance effectively seeks to prohibit reliance on SCCs by many EU businesses – especially those using key US service providers such as those which provide email and communications services, cloud services and others.

- **Disruption of transfers damages EU citizens and businesses.** The extensive use of SCCs means that, in the event they cannot be relied upon (as indicated by the EDPB Guidance), severe disruption will be caused to both EU consumers and EU-based businesses across all industrial sectors. The exact level of the resulting economic damage is difficult to assess. However, as the EU is the world's largest exporter of digitally delivered services, accounting for 24% of the world's total trade in services (https://ec.europa.eu/eurostat/statistics-explained/index.php/World_trade_in_services), the economic consequences of not being able to rely on SCCs for an international free flow of data would be profound. The alternative might be a scenario where wholesale non-compliance with EDPB guidance will occur which will serve to erode undermine the GDPR and its effectiveness.
- **Against the EU objectives.** The roadmap set out in the EDPB Guidance, in combination with a focus on technical measures (discussed below) means that it will only be in a limited number of cases that businesses and organizations will be able to rely on SCCs for transfers to third countries. This is fundamentally at odds with the purpose of the SCCs and the objective of the EU Commission.

2. On essential equivalence: a guidance that neglects to taking into account CJEU recent surveillance case law and post-2016 US surveillance changes

- **The EDPB Guidance does not take into account that US surveillance laws and practices have evolved since 2016 (which is the framework analyzed in the Schrems decision)**. US law and practice has changed since *Schrems II*. For example, important changes and clarifications regarding the scope and operation of FISA Section 702 requests in practice have occurred. These include (i) the termination of "about" collection and (ii) the requirement under the FISA Amendments Reauthorization Act of 2017 that the government develop and submit for FISC (FISA Court) approval, as part of a 702 certification package, procedures regarding the conditions and limitations on querying information collected pursuant to Section 702. In addition, further information has become available (such as now declassified information) demonstrating how the relevant safeguards and protections apply in practice, including those in relation to targeting determinations (and in particular, the requirement that the government memorialize a reasoned, written targeting determination for each individual target that is then subject to audit in a process supervised by the FISA Court) and querying procedures such as the information contained in the USG White Paper and explained in the Intelligence Community's 2018 Transparency Report.
- **The EDPB Guidance obviates that the US and the EU share common values and interests, in terms of respect human rights, the rule of law and the cybercrime collaboration.**
    - Regard must be had to appropriate standards and benchmarks when considering data transfers and anti-terrorism activities. For example, in respect of data transfers, regard has not been had to the fact that the US is also a member country of the OECD has been a driving force in the global harmonization of data protection and privacy laws and development of guidelines, and has signed the OECD Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which remain a principal benchmark for data protection laws. By way of further example, in respect of anti-terrorism activities, regard has not been had to the fact that the US played a central role in the negotiation, drafting and adoption of the Convention on Cybercrime in 2001, which begins by protecting private online communications by criminalizing unauthorized access to them. The US was one of the original signatories of the Cybercrime Convention, which was drawn up by the Council of Europe, and has as one of its main objectives "*to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation*".
    - More generally, regard has not been had to the fact that the US respects the rule of law and is consistently recognized for doing so by international organizations alongside Member States of the EU. The US is a key partner of the EU and its Member States in trade and combatting terrorism and yet the position adopted by the EDPB is entirely contradictory to this reality. Where the EU Commission in preparing new draft SCCs has looked to find solutions to enable transfers to continue globally, the EDPB

has endeavored to effectively terminate transfers of personal data to the many organizations in the US who are subject to the FISA 702 regime (and relying on out of date information in taking this preliminary position). The EDPB fails to take this into account and advocate for a proportionate and risk-based approach to compliance as envisaged by the GDPR.

- **The EDPB does not take into account the recent CJEU case law that confirms that national security can justify serious interferences with individuals' rights in certain cases and subject to proper safeguards.** The EU standard is not static and does not create hard and unchangeable rules regarding surveillance. The EDPB paper on European Essential Guarantees (EEG) relies significantly on the CJEU ruling in *La Quadrature du Net* which was published following the ruling in *Schrems II*. This is an important CJEU ruling which recognizes the importance of the objective of national security and acknowledging that such an objective can justify surveillance practices that result in serious interferences with individuals' rights. For example, the CJEU recognized that the following surveillance practices are capable of being justified: (i) real-time collection of traffic and location data where there is a valid reason to suspect the person involved; (ii) non-real time collection of traffic and location data where the data might make an "effective contribution to combating terrorism", (iii) the general and indiscriminate processing of communications data for a limited period where there are "sufficiently solid grounds"; and (iv) the general and indiscriminate processing of IP addresses and identification information, such as contact details. The CJEU also made clear that regard must be had to the various European Convention of Human Rights (which has traditionally afforded more flexibility for Member States to engage in surveillance than the CJEU), including the obligations on Member States to protection their citizens such as from terrorist attacks. Ultimately, every assessment of protection must take into account the relevant circumstances, context and up-to-date facts. The EDPB fails to do so by prohibiting reliance on SCCs for transfers to the US.

3. On supplemental safeguards: a guidance that puts organizations in an impossible situation, inappropriately focuses on technical safeguards and contradicts EU Member States surveillance requests

- **The EDPB Guidance puts forward safeguards that are unworkable.**
  - The inappropriateness of the position put forward by the EDPB Guidance is all the more acute given the fact that the technical measures are simply unworkable for any organization that needs to provide access to personal data to a US service provider (i.e., not personal data that has been encrypted or pseudonymised). In particular, the EDPB Guidance fails to acknowledge that for many legitimate reasons, such as providing services and technical support, almost all service providers will need access to personal data on a day-to-day basis at some stage. The EDPB Guidance precludes EU business from relying on SCCs to engage such service providers that need such access at any point.
  - For example, the following day-to-day processing would be prohibited at enormous cost to EU organizations and ultimately consumers:
    - SMEs using US cloud providers to operate online stores: smaller companies have greatly increased their participation in international trade transactions using online services based in the US to connect with customers and suppliers, provide information, take and place orders, and facilitate the delivery of products and services. The restrictive use cases provided for in the EDPB Guidance mean that smaller companies that have benefited from greater connectivity with customers and suppliers through online platforms will be seriously impacted if they cannot rely on SCCs to use these services.
    - NGOs and charities using US-based email providers: international NGOs and charities would be precluded from communicating and working on cross-border initiatives using email providers in the US. NGOs and charities need to collaborate internationally (including with those in the US) on day to day issues such as to prepare the channels that enable international response, conduct research in their areas and understand global trends.
    - Healthcare research initiatives communicating with US-based cloud solutions: global healthcare research is necessary in order to advance medicine and collaborate in the field. For example, international collaborations account for almost one-quarter of all publications and international partnerships have been growing between the US and the EU.

- University research using online collaboration software: EU based universities engage in collaborative research with institutions and organizations around the world. This research will inevitably involve the transfer of personal data to third countries such as the US and these organizations need to use online software to communicate and collaborate globally.
- US cloud provider as an employer in the EU: the EDPB Guidance would prohibit common practices such as using shared systems and providing remote access to data where a parent or group company is based in the US.

  - The EDPB Guidance should explicitly state that GDPR and the ruling in *Schrems II* permit reliance on a combination of measures – and make clear that there is no hierarchy of measures. The flexibility afforded to exporters, in particular, by the GDPR and *Schrems II* must be respected by the EDPB. The EDPB Guidance should provide a clear path to allow business to take steps to comply with GDPR in a manner that is appropriate and, consistent with the EU Commission's approach, recognize the importance of contractual and organizational measures.
  - The EDPB Guidance should also provide practical and workable guidance that will allow for businesses and organizations to take steps ensure that they can continue to transfer data in a manner which respects the essence of EU data subjects' GDPR rights without ignoring other Charter rights of EU organizations. In particular, the EDPB Guidance should acknowledge that it is not workable that EU business insist that service providers based in the US cannot access personal data as part of providing their services.

- **The EDPB Guidance inappropriately focuses on specific technical measures**

  - The EDPB Guidance essentially requires organizations to implement specific technical measures in order to rely on the SCCs in many cases and preclude reliance on organizational, contractual and other measures. In doing so, the EDPB Guidance departs significantly from the wording of the GDPR and the *Schrems II* ruling – neither of which prioritized technical measures over and above other types of measures, such as organizational, contractual or legal.
  - GDPR is a deliberately technology-neutral piece of legislation. It requires the implementation of "appropriate" measures and makes clear that what is appropriate will depend on the circumstances. Similarly, the CJEU in *Schrems II* referred to the implementation of "additional" and "supplemental" without specifying the form those measures must take. It is clear there is no hierarchy of measures. In addition, the EDPB Guidance also effectively departs from the EDPB's FAQ published following *Schrems II* which noted it was considering a range of measures "*whether legal, technical or organizational measures"* by now creating a core set of mandatory technical measures. Observing such measures in practice, in particular the technical and organizational measures may prove to be very difficult and challenging. For instance, performing IT audits overseas is a complex process and may not be suitable for all companies, considering that no differentiation is made between SMEs or larger companies.

- **The EDPB requires strong encryption while EU Council proposed a regulation on the imposition of backdoors to encrypted communications for surveillance purposes.**

  - The EDPB has elevated strong encryption and other technical measures, mistakenly, as the only true technical means of protecting data outside of non-adequate countries. At the same time EU Council is calling for the creation of "backdoors" to encrypted data EU intelligence and law enforcement can access EU data.
    - November 6, 2020 the German Presidency of the Council introduced a non-binding resolution on access to encrypted communications.
  - This guidance would mean companies in Europe could be unable to share their HR and employee data, customer files, or to operate any other intra-group transfers (if it includes personal data) with any branch outside the EU. This would be a huge disruption at an operational level for international organizations. This even applies to EU and US companies working together. For example, recent partnerships like Google and Orange would not meet the requirements of this guidance.

- **In contradiction with the CJEU, the EDPB Guidance seeks to prohibit reliance on SCCs for transfers to key US service providers**
    - The EDPB Guidance seeks to specifically rule out reliance on the SCCs (and any other Article 46 transfer tool) when transferring data to US companies that are subject to Section 702 FISA unless they can identify additional supplemental measures that make access impossible or ineffective. To provide some context, the EDPB Guidance would prohibit any EU business from relying on US service providers that provide email services or any cloud service providers that can access communications or related personal data in any way. There is no basis for adopting such a position.
    - **The EDPB Guidance seeks to rely on the ruling in Schrems II to take this position but this is entirely** misplaced for various important reasons. For example, the CJEU did not rule out reliance on the SCCs as a basis to transfer to the US (despite having the opportunity to do so) as implied by the EDPB Guidance. Further the CJEU endorsed Recital 109 of the GDPR which states that controllers and processors should be *encouraged* to provide additional safeguards via *contractual* commitments that supplement standard protection clauses. The EDPB has ignored this by effectively prescribing *technical* safeguards to operate in many cases.
    - In addition, there have been a number of developments in US law and practice and EU law that were not taken into account by the CJEU in *Schrems II*, including in particular those described in the United States Government White Paper and the new CJEU case law heavily cited by the EDPB in its European Essential Guarantees EDPB Guidance.
    - The EU Commission, which was aware of these developments, did not prohibit reliance the SCCs to transfer data to the US. To the contrary, the EU Commission has published the draft SCCs with the intention that they will provide for appropriate safeguards – even for transfers to the US. The EDPB Guidance is completely at odds with this position and prior to being finalized need to revisit their reliance on *Schrems II* given other developments and interpret *Schrems II* in a manner faithful to the GDPR including Recitals 4 and 109, discussed above.

4. On derogations: an unjustified overly restrictive interpretation contrary to CJEU decision and GDPR goals (i.e., to enable transfers rather than avoiding them)

- The EDPB Guidance continues to push for an overly restrictive interpretation of the derogations under Article 49 GDPR. The GDPR does not impose such a narrow view as has been taken by the EDPB in the EDPB Guidance or the Guidelines 2/2018 on derogations of Article 49 GPDR.
- The narrow approach which the EDPB applies to derogations in Article 49 GDPR means that there will be no alternative legal transfer bases for these organizations to avail of when it comes to routine transfers absent SCCs. In other words, many services which have come to be regarded as almost essential by EU businesses and other organizations will cease to be available to them.
- A balanced interpretation is not necessarily a restrictive interpretation. The proportionality test has already been done by the GDPR when identifying which situations may justify international transfers. The EDPB should take this opportunity to revisit the overly narrow interpretation of the derogations under Article 49 GDPR in light of the *Schrems II* ruling and the importance the CJEU attached to those derogations. In line with that ruling, it is essential that the derogations are interpreted appropriately to ensure that EU business and organizations can continue to transfer data when necessary to do so.
- Some of these derogations are not and cannot actually be "exceptional", as wrongly construed by the EDPB, such as the performance of international communications or international money transfers. In any event, the EDPB Guidance fails to distinguish between the business transfers and the transfers due to governmental access requests. Companies do not organize their business and technical infrastructure to serve national surveillance needs but their business. The governmental access requests are exceptional by nature and linked to the assessment of the public interest and defense of legal claims' derogations.
- The EDPB needs to holistically consider the combined impact of its guidance on derogations while taking account of how few countries have Article 45 adequacy decisions.