Joint GSMA and ETNO comments on draft recommendations issued by the European Data Protection Board on 10th November 2020 in relation to "measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" in light of the Schrems II decision

December 2020

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Thrive series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.
Follow the GSMA on Twitter: @GSMA.
Policy Contact: Boris Wojtan Director of Privacy bwojtan@gsma.com

ETNO represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For more information, please visit www.etno.eu
Follow ETNO on Twitter: @ETNOAssociation
Policy Contact: Paolo Grassia, Director of Public Policy grassia@etno.eu

Introduction
The GSMA and ETNO welcome the opportunity to comment on the draft recommendations issued by the European Data Protection Board (EDPB) on 10th November 2020 in relation to "measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" in light of the Schrems II decision ("the EDPB Draft Recommendations").

Cross-border data flows underpin the data-driven economy and society. Telecommunications network operators depend on data flows to be able to operate efficiently, to innovate, to contribute to society and to enable the wider digital ecosystem to do the same. A reduced ability to transfer and access personal data across borders makes the world less connected and undermines regional approaches to harnessing data such as the recently proposed EU Data Strategy. Telecom providers appreciate and support the protection of EU/EEA personal data at a level that is essentially equivalent to the GDPR and that respects the human rights, as enshrined in EU law, when data is moved or accessed from outside the EU/EEA. Unfortunately, the EDPB Draft Recommendations do not go far enough to address the legal uncertainty arising from the European Court of Justice (CJEU) decision. The GSMA and ETNO believe the EDPB Draft Recommendations could be improved by taking the following comments into account..

GSMA and ETNO joint comments

The EDPB Draft Recommendations are inconsistent with the GDPR, because they omit its risk-based approach.

A central feature of the EU data protection framework is the importance of assessing risk that processing personal data presents for the rights and freedoms of data subjects when determining which safeguards to apply. A risk-based approach provides data controllers with practical tools to determine how to allocate their resources while ensuring that individuals' privacy is protected effectively.

The GDPR provides that the implementation of appropriate and effective compliance measures "should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons" (GDPR recitals 74, 75-76). The adoption of technical and organizational measures to secure personal data should also depend on an assessment of risk (GDPR Article 32, recitals 78 and 83). Similar evaluations of risk should guide controllers in their selection of processors, in the performance of data protection impact assessments (GDPR Article 35, Recitals 89-91 and see also Article 29 Working Party guidelines on DPIAs), and in determining the extent of breach reporting that is required (Articles 33-34, Recitals 81-88). Similarly, the new draft Standard Contractual Clauses also include a risk assessment taking into consideration (i) the specifics of the transfer, e.g. the nature of the personal data transferred etc; (ii) the third country laws including access rights by law enforcement in the third country and (iii) any additional technical and organisational safeguards (see Clause 2(b)); and not just the third country laws.

The *Schrems II* decision is generally consistent with this risk-based approach, providing that an assessment of the circumstances is needed prior to applying additional safeguards (*Schrems II*, paras. 131-34). However, the EDPB Draft Recommendations are inconsistent with the Schrems II decision. The Draft Recommendations do not set out a risk-based approach as a guiding principle for data exporters when determining which safeguards are needed. Such an approach is a key element of the accountability principle emphasized by the recommendations (see paras. 3-5), and the EDPB alludes to the importance of risk

(para. 49), but more explicit recognition of the importance of risk assessments is needed to make the guidance consistent with EU data protection rules.

The EDPB Draft Recommendations suggest that the mere presence of personal data beyond the borders of the EU/EEA can subject it to any manner of intrusion, by lawful or illicit means, by a third country's public authorities (see para. 75). Such a theoretical danger could occur within or outside the EU/EEA, and it is difficult for a controller to calibrate any additional safeguards that might be needed to address it. Within the EU, measures adopted by EU Member States to protect their respective national security interests fall outside the acquis Communautaire (see Treaty of the European Union EU art 2(4)). The approach suggested by the EDPB could, therefore, be regarded by some as arbitrary practice on respecting national sovereignty.

The proposed recommendations would also appear to preclude scenarios where there is negligible, or very low risk to data subjects, such as in third-level IT support and bug fixing services where the nature of the data often has less potential for causing harm and where access to the data is infrequent and entirely incidental to the primary purpose of fixing a problem. The lack of a risk-based approach, particularly in light of Use Case 6, essentially make it more challenging to continue using low-risk, support-style services outside the EEA which does not seem consistent with the general approach supervisory authorities have hitherto adopted regarding to data protection and cross-border data flows.

Overly strict requirements, such as to promptly suspend data transfers for failure to meet the EU standard of essential equivalence (see para. 67), could disincentivize the dynamic and iterative implementation of supplementary measures and result in a major compliance challenge in particular for small and medium enterprises.

Therefore, we urge the EDPB to modify the Draft Recommendations to better acknowledge that the role of data exporters is to ensure the highest level of data protection for data subjects, by minimizing risk in the most efficient manner according to a risk assessment.

Organisations should be allowed to rely on derogations set out in Article 49 GDPR

Article 49 provides for derogations allowing transfers of personal data in the absence of an adequacy decision and any other transfer tools as per Article 46. The EDPB maintains that "Article 49 GDPR has an exceptional nature. The derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive" (see para. 25). This is an extensive interpretation of recital 111, which does not stipulate that all said cases of transfer must be occasional. Most notably, this requirement is not imposed for transfers based on the data subject's explicit consent or on a public interest. For other derogations, it is arguable that the effect of the Schrems II decision itself constitutes the exceptional circumstances that justify reliance on them until alternative robust transfer tools can be established.

Multinational corporations must have a legal basis for transferring employee data to corporate headquarters.

While the recommendations do not address all scenarios in which personal data is transferred, this is one of the most common use cases, and one that presents low risk of harm to data subjects. Employers' efforts to ensure that workers are properly compensated, trained, promoted, and provided with benefits also impacts the labor rights of these

employees. Similarly, employers need access to the proper data to investigate complaints of misconduct.

The EDPB Draft Recommendations would disincentivize companies located outside the EEA (particularly small and medium enterprises) from employing EU/EEA data subjects, as the cost of compliance could become prohibitive.

The EDPB should clarify that, pursuant to reasonable safeguards, employers may transfer or access the data of EU/EEA employees to their headquarters.

It is not clear whether the data importer and data exporter are always jointly liable or whether this can be determined contractually

Paragraph 60 of the EDPB Draft Recommendations provides that it is *the responsibility of the data exporter and the data importer to assess* whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the BCRs can be complied with in practice. However, other parts of the EDPB Draft Recommendations state that it is the data exporter that is responsible for the assessment of the need of supplementary measures.

The EDPB should clarify that liability for assessing whether appropriate safeguards are in place is something that can be freely determined between the data exporter and data importer by contract.

The EDPB Draft Recommendations are counterproductive to ongoing adequacy negotiations and the benefits they produce for data subjects globally.

Rather than creating prohibitive barriers to the cross-border transfer of data, the EDPB should leave room for the Commission to drive higher global standards through the negotiation of adequacy decisions.

Through the adequacy negotiations leading to Safe Harbor, the Privacy Shield, and a possible third agreement, the European Union and the United States have come together to create more robust privacy protections for millions of data subjects around the globe. With the Privacy Shield came reforms to the U.S. surveillance regime, and it has informed U.S. efforts to pass a national data protection law. The possibility of extending adequacy to other countries in Asia, Africa, and Latin America will also raise the bar for data protection internationally.

The EDPB Draft Recommendations place a greater onus on data exporters than is warranted by the CJEU judgment.

The *Schrems II* decision addresses the importance of both supervisory authorities and data exporters in protecting personal data that is transferred outside of the EU/EEA. A full evaluation of the essential guarantees provided by a third country's law is a complex endeavor, and it is more suited to a public authority than to a private actor. The EDPB Draft Recommendations suggest that this duty falls almost exclusively on the data exporter, with little support from the supervisory authority. This is a disproportionate burden for a private company to bear, and the cost for small and medium enterprises will be prohibitive.

Tasking companies with country assessments will also lead to inconsistent and incorrect results, increasing confusion for data subjects, employees, and B2B clients.

More clarification from supervisory authorities regarding cases where a EU/EEA processor exports the data on behalf of a controller by using a cloud service provider situated outside the EU/EEA (i.e., remote access from a third country) would help to handle respective responsibilities and liability.

It would be helpful if the EDPB provided more detailed guidance on how companies can mitigate the risks highlighted in the in the draft recommendation in particularly complex environments, such as those described in the use cases 6 and 7.

The EDPB Draft Recommendations create an uneven playing field by only targeting Chapter 5 transfers and not direct transfers by data subjects.

The draft recommendations do not address the scenario of direct transfers from EEA data subjects to a data controller in a third country. It is unclear how the EDPB envisages enforcing the GDPR including the Charter with regard to such data controllers. Examples may be providers of operating systems for various devices such as mobiles, tablets, tv's etc. We believe this lack of clarity in reality gives rise to an uneven playing field between data controllers in the EU/EEA using data processors outside the EU/EEA and data controllers established outside the EU/EEA.

The EDPB Draft Recommendations should emphasize the need for consistent decisions on data transfer recognized by the CJEU.

The *Schrems II* judgment recognized that any decision by a supervisory authority to prohibit transfers to a country should be referred to the EDPB for an opinion, "in order to avoid divergent decisions" (*Schrems II*, para. 147). Divergent decisions would create tremendous disruption and uncertainty for data exporters. The draft recommendations suggest that such inconsistent results may occur.

The EDPB should commit to uniform guidance being provided in order to avoid any such divergent decisions regarding data transfers to third countries.

Consistent guidance could also take a more proactive form. Even though the adequacy of safeguards is to be determined on a case-by-case basis when using SCCs or other mechanisms under Article 46 GDPR, a legal overview by the EDPB or the European Commission regarding the essential guarantees and relevant legal framework in particular destination countries would, nevertheless, be a very useful starting point for companies to assist them when they are to make their own assessments. Such guidance could include a form of benchmarking of countries.

Given that some third countries are more heavily relied upon than others for IT support and customer care related services provided to companies that process EU/EEA personal data, it would be highly beneficial if the EDPB were to prioritise guidance for these countries.

Data exporters must have sufficient time to implement the new recommendations before enforcement actions commence.

Many contracts that incorporate SCCs are valid for much longer than the one year envisaged by the EDPB Draft Recommendations. The supplementary measures recommended by the EDPB will take time to implement and may require data exporters to redraft numerous contracts.

Just as the GDPR provided a two-year implementation period, the EDPB should provide at least two years for controllers to perform the necessary assessments, determine which measures should be adopted, and implement them, before they may be held liable for actions related to these recommendations. An alternative could be for SCCs in existing contracts to be deemed to be valid until the contracts expire or are renewed. It would also be inconsistent of the EDPB to enforce an immediate cessation of certain transfers when EU/EEA data protection authorities have themselves not seriously challenged the use of SCC in similar situations before.

Thank you for the opportunity to provide these comments. We look forward to engaging with the EDPB to support the development of sustainable cross-border data flow solutions that companies and data subjects can rely on in future.