Netcomm's position to the EDPB consultation on its Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Netcomm, the Italian Consortium of Digital Commerce, is the reference point for e-commerce and digital retailing at national and international level; Netcomm includes among its members about 400 companies representing both international corporations and small- and medium-sized enterprises which are flagships of Italian excellence. The Consortium aims to promote the spreading of e-commerce and the digital evolution of companies, thus generating value across the entire value chain and consumers. Netcomm is co-founder of Ecommerce Europe -the European Association of E-commerce- and of the Italian Digital Federation, the organization for the digital development in Italy.

Netcomm appreciates the opportunity given by the EDPB to provide comments on the Recommendations.
Netcomm's feedback focuses on some concerns and suggestions for improvement of the recommendations considering the SME's point of view that are requested to deal with data transfer matters.

With a very realistic approach, it should consider some preliminary points:

i) most of the information society services (including cloud, e-mail services, etc.) are provided by non-EU companies in favor of small and medium-sized enterprises which, to be compliant, must be supported with rules that are easy to apply.

ii) in relation to some services of the information society which are crucial for the functioning of businesses (e.g., e-mail services) it should consider that it is very difficult for SMEs to dialogue and verify the application of the requirements from providers.

iii) If the Recommendations are adopted in their current form, any organization that uses an online service to process and transfer personal data—including email, hosted applications, or any other online service—could face fines up to 4% of its annual turnover, irrespective of whether public authorities in any third country ever access the data in question. They also will require EU organizations to undertake their own costly analyses of the laws and practices of dozens of non-EU countries (i.e., those not subject to an EU adequacy decision), which will be unrealistic for most small and medium-sized enterprises, research institutions, and others.

As a result, the Recommendations will make it highly risky for EU companies to engage in commerce with non-EU customers or partners, for researchers to share information with foreign colleagues, for companies with non-EU offices or personnel to communicate with them online, or to engage in countless other routine and necessary operational tasks. If adopted they could have potential negative effects on EU competitiveness, innovation, and society.
In such a complex context it is important and fundamental for companies - especially SMEs - to be supported with concrete and easy-to-apply tools.

Netcomm wishes to share the following points.

1. The Recommendations should allow data exporters to take account of the full context of a transfer and the kind of data

The GC, in Schrems II, indicated that data exporters should consider the full context of a transfer when evaluating its legality and, specifically, that transfers should be evaluated "in the light of all the circumstances of that transfer" and "on a case-by-case basis" (nr. 134). The Recommendations, instead of supporting this approach, eliminates the possibility to take the likelihood into account, which is a fundamental part of the GDPR (art 24, 25, 32, 34) and Recitals (75, 76, 77, 90) and any risk assessment in line with widely accepted international standards.

We believe that EDPB should support this approach and encourage organisations to consider the potential risks of a transfer (including the likelihood that law enforcement / agencies would request access to the data) distinguishing categories of data treated (i.e. metadata are different from medical status).
If these real-world risks are low or absent, or the data treated do not represents risk for the fundamental rights, the Recommendations should not require organisations to adopt any supplemental measures.

2. The Recommendations should propose technical measures that are workable in practice

The Recommendations propose a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. Unfortunately, some of these measures are unworkable and unrealistic in practice.
They also suggest that encryption almost never provides sufficient protection where data is accessible "in the clear" in the third country, including where an EU organisation uses an online service that may process the data in the third country (nr. 88-89), or where employees or others in the third country can access the data on a shared IT system.
Many online services that EU businesses rely on today require processing of the information in unencrypted form to work properly. Moreover, given the nature of the Internet and the global economy, such operations might entail some processing that occurs outside the EU, irrespective of where the data controller or data processor is based. The Recommendations would prohibit EU organisations from engaging in these commonplace and essential business activities.
It is necessary to consider that most EU organisations would not be able to cease these activities entirely and at the same time remain economically competitive. Likely, many would turn to other legal mechanisms, such as the derogations set out in Article 49 of the GDPR.
To avoid these consequences, the EDPB should revise the Recommendations to ensure that the proposed technical measures are workable in practice and should leave it to data exporters to determine case-by-case whether any measure adequately protects the transferred data.
It would be useful and appropriate and truly appreciated to support companies by providing tools and practical indications that can be applied to common concrete cases that guarantee the balance of interests, or that protect data and at the same time favour the circulation of information in line with the digital market.

3. The Recommendations should make clear that enforcement by supervisory authorities should be measured, proportional and appropriate

The effects of the Schrems II was a major and unexpected development, one that requires organisations across the EU to prepare new data transfer impact assessments and, in certain cases, to overhaul aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to the underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation.
Recommendations imply that supervisory authorities should move directly to "corrective measure[s] (e.g., a fine)" if they determine that a data transfer does not comply with the Recommendations (nr. 54). This focus on sanctions will lead EU organisations to rush through changes to their data transfer practices—making it far less likely that organisations address these issues carefully and precisely. To avoid this outcome, the Recommendations should expressly advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work and cooperate with data exporters to find acceptable safeguards and practical solutions and give them sufficient time to implement such solutions.

This approach will provide incentives for EU organisations to address these issues thoughtfully, while also encouraging good-faith and collaborative solutions to these quite difficult legal and technical issues. Moreover, it will encourage data exporters to seek adequate solutions in full cooperation with supervisory authorities instead of not contacting them to avoid serious repercussions.
Netcomm concerns that the EDPB is shifting a responsibility from the European Commission (usually responsible to take 'adequacy decisions' and with the knowledge and experience to do so) to companies. Netcomm stresses that the scale of the effort required to comply with the requirement to review all data sharing contracts on a case-by-case basis might take months if not years and at considerable costs. As a result, we believe that data exporters should be granted a transition period of at least 1 year.
Netcomm considers that the EDPB Guidance on Schrems II adds several far-reaching requirements to the existing GDPR requirements, and thereby goes beyond the actual GDPR text. Although we realise that the EDPB guidance is factually only a non-binding guidance issued by the assembly of EU data protection authorities, it will have a far-reaching effect, especially for the interpretation and enforcement by EU data protection authorities.
Considering that the Recommendation's additional privacy requirements will in effect result in a change in the politically agreed system of the GDPR Netcomm therefore urges for a proper legal basis, issued by the right legislative institution, which in our view would be a GDPR amendment or revision of the GDPR and not a guidance by the EDPB.
In the same logic, it is important to note that companies that rely on Binding Corporate Rules (BCRs) have invested a significant amount of time, effort and money in their approval. The EDPB guidance now adds additional assessment requirements to BCRs even though these additional requirements are not covered by the GDPR.

4. The Recommendations should maintain a risk-based and proportionate approach to transfer assessment

Netcomm notes the absence of a risk-based approach which represents one of the fundamental principles of the GDPR capable of guaranteeing the balance of interests.
The absence of a risk-based approach in the Recommendations will, in our view, lead to significant legal uncertainty.

As we see the guidelines the European Data Protection Board (EDPB) does not consider 'likelihood' to be an objective factor in transfer impact assessments. This decision, in our perspective, is not in line with the GDPR, which evidently refers to the concept of 'likelihood' in the context of other obligations (e.g., under Articles 32 and 35 GDPR) while supervisory authorities historically have recognised this concept that requires data exporters to assess and identify the most high-risk data transfers subject to eventual public authority's requests.

Furthermore, identification of supplementary measures should account for the nature of the data being transferred and not only for the data protection legislation in the third-country recipients. Not all information is relevant or would be subject to law enforcement requests (e.g., processing of employee credentials or limited profiles to provide access to a technical solution that does not process personal data as its primary function). Proportionality always needs to be considered when performing an assessment on eventual risks and additional measures. A potential infringement and need for additional safeguards always need to be put in relation to the importance of the personal data concerned and the parties involved.

In that perspective, there is a need for clarity in the guidelines on the division of responsibilities between data exporter and importer that should consider which of the involved parties is in a better position to conduct assessments both from competence and scalability standpoints.

The introduction of requirements only for the data exporter could make it impossible for exporting companies to assess the legislation of the destination country and the legal remedies fully and consciously to be adopted for the protection of privacy.

As data importers mostly are in a better position to know which laws apply to them in both import and export markets, and as they often typically serve multiple exporters, standardised assessments performed by the data importer could benefit all their exporter customers and consequently should be supported in the EDPB guidelines. The same clarity is needed to allocate responsibilities among joint controllers and processors, especially in cases where only one of them is basically determining the purpose and the functioning of the data transfer service which is offered to the joint controller on a ready tailored and non-negotiable basis. Examples of such scenarios would be more than welcome and should preferably focus on most common cases.

Furthermore, any suggestion that controllers are liable for sub-processors' supplemental measures appears to be inconsistent with the requirements in the GDPR. In relation to this, the contractual relationship between the exporter and the importer must consequently be considered as a relevant factor. When it comes to the many vendors on which retailers rely, the bargaining power of each individual business, no matter how large, vis-à-vis the vendor is limited. This contractual imbalance is being addressed in certain sectors, such as financial services (where specific contractual clauses are being drafted to reduce risk of vendor lock-in) but is not currently available in the retail content. It is therefore likely, based on the recommendations as drafted, that such vendors will also insist on an agreement from retailers that these measures are sufficient on a take-it-or-leave-it basis. In line with the practical realities and contractual imbalances noted above, we would like the recommendations to direct greater responsibility towards these vendors.

Further, we note that the Recommendations do not distinguish categories of data. this type of approach is limiting and does not consider the real circumstances that can occur on a case-by-case basis.
For example, IP addresses, or simple service metadata would get the same treatment as special categories of data (racial, sexual orientation, political affiliation). Clearly the risk inherent to those to the rights and freedoms of natural persons are very different. Also, they eliminate the possibility to take the likelihood into account, which is an essential part of any risk assessment.