Warsaw, December 21st, 2020

Opinion of the Polish Chamber of Information Technology and Telecommunications on draft Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("Recommendations 01/2020") adopted on 10 November 2020 by European Data Protection Board ("EDPB").

The Polish Chamber of Information Technology and Telecommunications ("**PIIT**"), established in 1993, is the largest national IT industry association and active NTA member in DigitalEurope. The members of the PIIT are entities from all market segments, including local and international companies, large corporations, and SMEs.

We hope that following remarks to the Recommendations 01/2020 will be valuable input for further development and digital transformation of the European economy with respect for the fundamental privacy rights. We also understand that it's not exceptional in the XXI century global economy, that data are transferred internationally within internal corporate structures, between vendors and clients or between controllers and processors all over the world. We believe that the Recommendations 01/2020 are dedicated to make these processes easier and to remove uncertainty in operations for controllers and processors of any size, with no impact on data subjects' rights. Notably, the GDPR was adopted not only to preserve fundamental rights and freedoms of individuals, but also to facilitate the free flow of personal data within the European Economic Area ("**EEA**") and the third countries. We are also bearing in mind that post-COVID recovery of the economy in Europe will heavily depend on digital transformation in the most work-effective and cost-effective way.

1. EDPB's omission of the risk-based approach and explicit recommendations without context

The GDPR has been adopted as a risk-based approach regulation, i.e., it is the responsibility of the controller or processor to implement protective measures corresponding to the level of risk of the data processing activities. The absence of specific solutions in the GDPR is an intended measure to cover many existing factual circumstances. The precise indication of explicitly authorized and prohibited data processing activities can be counterproductive due to the variety of factual circumstances. These circumstances may differ for different size of the companies or organizations, industries, countries, size of processed personal data sets and many more factors. Thus, the requirements under the GDPR are not homogeneous in application – the same provision may have different impact for organizations with different characteristics. However, the Use Cases presented in the Recommendations 01/2020 constitute a limitation in the interpretation of legal requirements – the Recommendations 01/2020 indicate one clear solution, ignoring, directly or indirectly, other options to ensure compliance and data protection. The Recommendations 01/2020 are moving from helpful, risk-based approach guidance towards long list

Polska Izba Informatyki i Telekomunikacji
Eurocentrum, IX piętro
Al. Jerozolimskie 136
02-305 Warszawa

tel. +48 22 628 22 60
+48 22 628 24 06
+48 785 500 949
biuro@piit.org.pl
www.piit.org.pl

Bank Pekao S.A Oddział w Warszawie
65 1240 6175 1111 0000 4573 4520
KRS: 0000130600, Sąd Rej. M.st. W-wy
XII Wydział Gospodarczy

of strict rules, including adoption of long list of costly safeguards. This caselike approach and application of the Recommendations 01/2020 in practice may stop or discourage to use any tool, application, platform where there is even theoretical possibility of data transfer outside the EEA.

Moreover, restrictive rules and narrow interpretations may in the future provide a basis for the invalidation of subsequent adequacy decisions and recurring events, as in the case of the invalidation of EU-US Privacy Shield due to Schrems II or the earlier invalidation of the International Safe Harbor Privacy Principles due to Schrems I judgment[1]. We believe that the way to ensure a high standard of data protection will not always be to make increasingly stringent and new demands, but to make it easier for organizations to adapt to the current ones.

In view of the above, it is recommended to:

a. indicate that the GDPR is a risk-based approach regulation, which covers also the data transfers to the third countries;
b. preserve the proportionality of data protection and ensure the free flow of data, including providing guidance to assessment of proportionality of risk and supplemental safeguards;
c. base the Recommendations 01/2020 towards Art. 46 GDPR by expressing their applicability in typical business scenarios, including binding corporate rules, standard data protection clauses, certification mechanisms and codes of conduct;
d. provide guidance on the minimum safeguards to be applied, e.g. requirements for ISO certification standards.

2. Negative consequences of the proposed safeguards for business and the level of data protection

The proposed safeguards are worryingly impractical and raise concerns among many organizations and businesses operating across Europe. For some companies, the proposed safeguards may make it practically impossible to continue operations. For example, in the cybersecurity, the application of the Recommendations 01/2020 may entail a real reduction in the level for information security and data protection.

Example: the use of cloud services provided from and within the EEA may be excluded from a cybersecurity service (e.g. authentication, anti-virus checking of attachments) due to much higher cost compared to such a global service, as well as a higher quality of service from a global operator due to greater market range. In view of the market practices, we estimate that the most likely the recipient of such service will use this type of service where there is

[1] Judgment of the CJEU of 16 July 2020, C-311/18 – Facebook Ireland (Schrems II) and Schrems and judgment of the CJEU of 6 October 2015, C-362/14 – Schrems (Schrems I).

Polska Izba Informatyki i Telekomunikacji
Eurocentrum, IX piętro
Al. Jerozolimskie 136
02-305 Warszawa

tel. +48 22 628 22 60
+48 22 628 24 06
+48 785 500 949
biuro@piit.org.pl
www.piit.org.pl

Bank Pekao S.A Oddział w Warszawie
65 1240 6175 1111 0000 4573 4520
KRS: 0000130600, Sąd Rej. M.st. W-wy
XII Wydział Gospodarczy

a service of the highest quality and lower costs (global entity) or will not use a cybersecurity service at all due to potential financial or regulatory barriers. This may lead to decreased level of data protection and potential cyberthreat.

Furthermore, it should be pointed out that the safeguards indicated in the Recommendations 01/2020 and their application can be described as 'one-size-fits-all' due to the requirement to apply safeguards to any conceivable access to data by public or government authorities. It should be noted that the Recommendations 01/2020 do not indicate circumstances or conditions which do not require the use of safeguards for individual transfers, or situations where only organizational safeguards are sufficient. It can be assumed that the Recommendations 01/2020 were wrongly intended to apply safeguards by default and in advance.

As a consequence of the default use of technical safeguards and the one-size-fits-all approach, the proposed safeguards are also disproportionate. In particular, use of contractual and organizational safeguards is excluded for data transfers to third countries, where there is even a hypothetical possibility that public authorities may gain access to these data. Notably, it is disproportionate to require that technical safeguards prevent government access to data, including encryption, which will be resistant to breach of such safeguards. In practice, these may be particularly costly or even impossible to meet these requirements in terms of resources held by government authorities[2].

Therefore, it would be most appropriate to indicate in the Recommendations 01/2020 the measures identified to ensure data protection in the transfer, from which they can be selected and adapted to specific circumstances on a risk-based approach. At the same time, these measures should correspond to reality, particularly taking into account that certain solutions, such as data encryption, may in many cases be impossible to apply.

3. Distinction between standard data protection and potential access to data by third country public authorities

[2] As indicated in the Use Case 1, using hosting service provider in a third country is allowed if "the encryption algorithm is flawlessly implemented". This requirement means that encryption protecting the data from brute force decryption performed by public authorities must be implemented. In view of current technological possibilities, such as the recent announcement made by China that that their new quantum computer has performed specific calculation in 3 minutes, while the fourth fastest supercomputer in the world requires 2.5 billion years to perform the same calculation. Consequently, that computer power which may be used by public authorities has increased 430 000 000 000 times and so the data transfer requires to implement encryption 430 billion times stronger than before. These conditions may change again any moment in the near future. This finally shows that on the grounds of the Recommendations 01/2020 most data transfers are not allowed in any circumstances for any, even for low risk transfers, because they cannot meet unrealistic criteria. Source of information from Dec 6th, 2020: New Quantum Computer in China Claims Quantum Advantage With Light (singularityhub.com).

As a result of the Schrems II judgment, the Recommendations 01/2020 place a strong emphasis on issues relating to the legal framework and legal practice in the third countries. The EDPB European Essential Guarantees recommendations ("**EEG**"), which are referred to in the Recommendations 01/2020, provide elements which have to be assessed to determine whether the legal framework governing access to personal data by public authorities in a third country can be regarded as a justifiable interference or not. However, despite the reference to the EEG recommendations, they do not indicate practical solutions for carrying out such assessments. What is more, the EEG recommendations have a more risk-based-approach to making assessments then the Recommendations 01/2020. They refer to the case of the ECtHR which stated in Kennedy that "assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by national law".[3]

Significantly, the Recommendations 01/2020 indicate that even the potential possibility that public authorities in a third country may have access to the data is a circumstance which obliges them to use additional technical safeguards. In practice, given the present national security environment and the strict requirements arising from the Schrems II judgment, organizations will need to apply additional safeguards for transfers they make to any country in the world that has not been deemed adequate by the European Commission. Further, the Recommendations 01/2020 indicate that these requirements apply even if the data is simply transiting through the third country.[4] In effect, any organization or company that uses the internet for operations involving personal data would likely need to adopt additional technical safeguards, even if the risk that third country authorities will access the data is marginal.

4. Assessment of the legal framework in the third countries

The purpose of the Recommendations 01/2020 is to provide clarification on the practical application of the provisions concerning the protection of personal data. One of its more important elements is the assessment of the legal framework of countries to which some part of the processing may potentially be transferred. In our opinion, there are hardly any helpful guidelines in the Recommendations 01/2020 which would facilitate such an assessment of the legal framework of a third country.

The Recommendations 01/2020 indicate sources of information on the legislation of another country for assessment purposes are general i.e. public legislation, elements demonstrating that a third country authority will seek to access the data with or without the data importer's knowledge or elements demonstrating that a third country authority will be able to access the data through the data importer or

[3] ECtHR, Kennedy §153.
[4] See, for example, Use Case 3, on p. 24 of the Recommendations 01/2020.

through direct interception of the communication channel in light of reported precedents, legal powers etc.[5]

Consequently Recommendations 01/2020 lack precise criteria. For example, the Recommendations 01/2020 indicate that "you should look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards. You should conduct this assessment with due diligence and document it thoroughly, as you will be held accountable to the decision you may take on that basis"[6]. Such guidelines may be too general to be applied in practice, in particular, in the context of the assessment not only of the legal regulations in the third country concerned, but also of the practice of that country.

Also the provided example from the Schrems II judgment regarding Section 702 of the U.S. FISA that "these provisions do not respect the minimum safeguards resulting from the principle of proportionality under EU law"[7], is insufficient in practice and will not, in fact, help to make decisions in connection with the transfer of data to a third country.

Therefore, the instructions contained in the Recommendations 01/2020 are not, in our view, sufficient to indicate at least the principles for legal assessment of the legal framework of a third country. It should be noted that this issue is now a fundamental one in the light of the Schrems II judgment. The lack of practical guidelines may not achieve the purpose for which the official Recommendations 01/2020 are to be adopted.

Currently, the obligation to assess the legal framework of a given third country lies with the data controllers. However, in our opinion, this type of assessment should be carried out by administrative bodies of the European Union. Nevertheless, there are many potential tools to consider, for example mutual legal assistance treaties (MLAT) for the purpose of gathering and exchanging information in an effort to enforce public laws, including laws relating to personal data protection and surveillance. Another potential solution, and an example of an organizational measure that could be included in the Recommendation 01/2020 (or at least should be considered), would be to introduce a procedure – contractually obliging both the data exporter and data importer – and indicating the rules of conduct towards third country public authorities in relation to the possible disclosure of data, aiming at data protection and respect for the fundamental rights and freedoms of data subjects.

[5] See point 42-42 on p. 14 of the Recommendations 01/2020.
[6] Point 42 on p. 14 of the Recommendations 01/2020.
[7] See example on p. 15 of the Recommendations 01/2020.

Polska Izba Informatyki i Telekomunikacji
Eurocentrum, IX piętro
Al. Jerozolimskie 136
02-305 Warszawa

tel. +48 22 628 22 60
+48 22 628 24 06
+48 785 500 949
biuro@piit.org.pl
www.piit.org.pl

Bank Pekao S.A Oddział w Warszawie
65 1240 6175 1111 0000 4573 4520
KRS: 0000130600, Sąd Rej. M.st. W-wy
XII Wydział Gospodarczy

5. **Excessive generalization of cloud services; no consideration of other component services; highly demanding assessments**

The Recommendations 01/2020 refer directly to cloud services[8]. According to us, they do not take account of the fact that today's cloud services do not consist only of one model of providing services, but as a product they consist of many different component services. For example, an office suite is not only an application but also a related authentication, encryption, versioning, dictation or reading services. Cloud services are also related to data classification, data retrieval, data protection, access monitoring, modification and transfer restrictions. The Recommendations 01/2020 consider cloud services to be a unit, whereby potentially all component services may involve a data transfer outside the EEA. In fact only some of them may potentially involve such a transfer. On the other hand, disconnection of individual services is a counter-productive and non-market activity due to the functional integration of all the components that make up a cloud service.

The Recommendations 01/2020 indicate that where a data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country, if "the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society". In the light of the Recommendations 01/2020, such a condition includes the right to an effective remedy and to a fair trial[9]. This condition should also be reflected in Article 23(1) GDPR and indicated therein grounds for restricting the fundamental rights and freedoms by way of legislative measures, which should be necessary and proportionate in a democratic society. In view of the difficulty of making such a complex assessment against the background of broad legal regulations for a complex service consisting of many components, such as cloud services, the requirements indicated in the Recommendations 01/2020 do not constitute effective guidelines and solutions. It is difficult for entrepreneurs and organizations to assess such a general clause as "democratic society". Requiring such a comprehensive assessment, taking into account the resources of entrepreneurs and most of the organizations concerned, is disproportionate and highly demanding. This also makes it all the more important to emphasize the nature of the GDPR in terms of risk-based approach.

Since cloud services are of great importance for today's information technology landscape and economy, their continuous development, as well as the large number of entities that provide or use cloud services, it is necessary to develop and differentiate between its different components in order to put the Recommendations 01/2020 into practice and ensure data protection. At the same time, it will be advisable to synchronize the Recommendations 01/2020 with the processes related to the implementation of the Directive on security of network and information systems (NIS Directive) and the requirements for the

[8] See, for example, Use Case 6 of the Recommendations 01/2020.
[9] Article 47 of the Charter Of Fundamental Rights Of The European Union.

Polska Izba Informatyki i Telekomunikacji
Eurocentrum, IX piętro
Al. Jerozolimskie 136
02-305 Warszawa

tel. +48 22 628 22 60
+48 22 628 24 06
+48 785 500 949
biuro@piit.org.pl
www.piit.org.pl

Bank Pekao S.A Oddział w Warszawie
65 1240 6175 1111 0000 4573 4520
KRS: 0000130600, Sąd Rej. M.st. W-wy
XII Wydział Gospodarczy

Digital Services Providers. The lack of systematic inclusion of these issues in the Recommendations 01/2020 may lead to contradictions or shortcomings in their application.

6. The Recommendations 01/2020 set requirements for data transfer such as for adequacy decisions

According to Article 45(2) of the GDPR, the European Commission, when assessing the adequacy of a third country's level of data protection, should take into account its legislation and the rule of law, the existence of an adequate independent supervisory authority, as well as the third country's obligations in the field of personal data protection. The requirements for adequacy decision coincide in many ways with the requirements of the Recommendations 01/2020, according to which it is necessary to assess, on a case-by-case basis, whether the legislation of the country concerned or the practice of the authorities (rule of law) meets the requirements for data protection and the rights of data subjects. This is closely linked to the other requirements of the existence of an appropriate supervisory authority in the country concerned and the contractual obligations with regard to data protection of the country concerned.

The above leads to the conclusion that, in the light of the requirements of the most formalized legal instrument enabling data transfer (adequacy decision), the Recommendations 01/2020 follow a relatively very high standard. While a high standard of data protection should be the preferred option in each case, it is not always indispensable. This approach of setting highest possible standards will not necessarily be practical or feasible, as well as does not reflect the risk-based approach. Therefore, the minimum thresholds for data transfer should not be the same as those applicable to the European Commission's adequacy decision.

7. The risk of non-application of the Recommendations 01/2020 by obliged entities and lowering the overall level of data protection

Considering that the Recommendations 01/2020 place high requirements on the transfers of data to third countries, even under the GDPR, we identify the risk that the Recommendations 01/2020 will not be applied or data transfers will be based on the derogations indicated in Article 49 of the GDPR. The requirements may be particularly impractical or even impossible to meet by data controllers and processors. In the event of a widespread use of the derogations under Article 49 of the GDPR, these transfers will take place without the appropriate safeguards foreseen for the other possibilities of data transfer to a third country. We therefore point out that the current Recommendations 01/2020 run the

risk of achieving the opposite of the intended and thereby reduction of data protection[10].**The Recommendations 01/2020 exceed their competence**

Although the Recommendations 01/2020 are not a source of law (hard law), but a guideline for interpretation and the setting out of best practices (soft law), they go beyond their competence and in effect they appear to create new obligations.

The purpose of the Recommendations 01/2020 is to explain and recommend solutions to existing regulations. On the basis of the GDPR, purpose of the recommendations issued by the EDPB is to identify best practices based on the applicable law in order to achieve consistent application of the GDPR. However, in the light of the restrictive expression of certain statements, as well as the definite indication of the admissibility or absence of individual safeguards, we get the impression that they go beyond their role and competence. For example, the Recommendations 01/2020 indicate that „you must monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third country to which you have transferred personal data that could affect your initial assessment of the level of protection and the decisions you may have taken accordingly on your transfers. Accountability is a continuing obligation (Article 5(2)GDPR)". Such guidance, although linked to the principle of accountability, is an additional requirement which does not derive from the law. It is therefore necessary to review the Recommendations 01/2020 and amend them to the extent that they are not based on legal provisions and go beyond their competence.

8. Summary

As a chamber bringing together different companies of different sizes whose core is data processing, including existing transfers to third countries, we address the EDPB on the following issues:

1) It is necessary to indicate that the GDPR is a risk-based approach regulation and to implement this approach to the Recommendations 01/2020.

2) We recognize the need to emphasize the proportionality of the safeguards applied, with an indication of the use of organizational and contractual measures.

3) The Recommendations 01/2020 shall provide realistic guidance on the minimum safeguards to be applied, not only those concerning highest desired level.

[10] According to the "Schrems II Impact Survey Report" published in November 2020 by DigitalEurope, 92% of companies that have reassessed their use of SCCs to comply with the Schrems II judgment consider that the cost of doing so is moderate or high. Only half of estimated SCC users have reassessed their use of SCCs.

Polska Izba Informatyki i Telekomunikacji
Eurocentrum, IX piętro
Al. Jerozolimskie 136
02-305 Warszawa

tel. +48 22 628 22 60
+48 22 628 24 06
+48 785 500 949
biuro@piit.org.pl
www.piit.org.pl

Bank Pekao S.A Oddział w Warszawie
65 1240 6175 1111 0000 4573 4520
KRS: 0000130600, Sąd Rej. M.st. W-wy
XII Wydział Gospodarczy

4) The Recommendations 01/2020 should provide precise guidance on Art. 46 GDPR by expressing its applicability in typical business scenarios, including binding corporate rules, standard data protection clauses, certification mechanisms and codes of conduct.

5) Reconciling consistency with a lack of categoricality, particularly when it comes to creating and developing new obligations.

6) Introducing in Recommendation 01/2020 a set of possible safeguards on specific cases that could be applied by the data exporters and data importers. Discontinuation of the casuistic case identification and one-size-fits-all approach.

7) A realistic approach to potential access to data by public authorities in third countries. Indication of a certain tolerance for cases where the risk of such access cannot be excluded, although it is very low or marginal.

8) Taking into account the complexity of cloud services and their many components in the Recommendations 01/2020.

9) We believe that Recommendations 01/2020 should not constitute new legal requirements, as it is beyond its competence. Therefore, the guidelines provided should be based on existing law and the obligations arising from it.

27 PIIT lat

Polska Izba Informatyki i Telekomunikacji
Eurocentrum, IX piętro
Al. Jerozolimskie 136
02-305 Warszawa

tel. +48 22 628 22 60
+48 22 628 24 06
+48 785 500 949
biuro@piit.org.pl
www.piit.org.pl

Bank Pekao S.A Oddział w Warszawie
65 1240 6175 1111 0000 4573 4520
KRS: 0000130600, Sąd Rej. M.st. W-wy
XII Wydział Gospodarczy