



EDPS OPINION ON A PRIOR CONSULTATION REQUESTED BY THE EUROPEAN CENTRAL BANK ON THEIR NEW CUSTOMER RELATIONSHIP MANAGEMENT SYSTEM

7 July 2021

(Case 2021-0528)

This Opinion addresses the question of whether mitigating measures identified by the European Central Bank (the ‘ECB’) can be considered sufficient to appropriately address the high risks identified by the ECB in relation to its use of Microsoft Dynamics 365. The European Data Protection Supervisor (the ‘EDPS’) has issued this Opinion in accordance with Article 40(2) of Regulation (EU) 2018/1725 (the ‘Regulation’)¹. The EDPS is of the opinion that the mitigating measures envisaged by the ECB are insufficient to mitigate the high risks it has identified. As a consequence, the EDPS finds that there are not sufficient guarantees and appropriate safeguards that the processing by Microsoft and its sub-processors resulting from the ECB's use of Microsoft Dynamics 365 and the associated transfers of personal data to them will meet the requirements of the Regulation and ensure an essentially equivalent level of protection to that guaranteed in the European Economic Area (the ‘EEA’). The EDPS therefore issues a warning pursuant to Article 58(2)(a) of the Regulation that the envisaged processing operation is likely to infringe Articles 4(2), 27, 29, 46, and 48 of the Regulation. The EDPS makes several recommendations to assist the ECB in ensuring compliant processing.

¹ Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, L 295, 21.11.2018, pp. 39-98.

Table of Contents

1. PROCEEDINGS	3
2. DESCRIPTION OF THE PROCESSING	3
2.1. The current CRM system [REDACTED]	3
2.2. Description of the new CRM	4
3. PRIOR CONSULTATION PURSUANT TO ARTICLE 40 OF THE REGULATION	6
3.1. The DPIA	6
3.2. Need for prior consultation and scope of the Opinion	9
4. LEGAL AND TECHNICAL ASSESSMENT OF THE MITIGATING MEASURES IDENTIFIED IN THE DPIA	10
4.1. Measures to mitigate the high risk of non-compliance with the rules on international transfers in light of the <i>Schrems II</i> ruling	10
4.1.1. Contractual safeguards and mitigating measures	12
4.1.2. Technical mitigating measures	16
4.1.3. Organisational mitigating measures	19
4.2. Measures to mitigate the high risk of lack of control over Microsoft sub-processors	23
4.2.1. Information on sub-processors	23
4.2.2. Prior authorisation of sub-processors - not freely given	24
4.3. Measures to mitigate the high risk of certain limitations of the contract with Microsoft negotiated by the European Commission.....	25
4.4. Assessment of the alternatives to Microsoft Dynamics 365.....	26
5. WARNING AND CONCLUSIONS	27
6. JUDICIAL REMEDY	29

1. PROCEEDINGS

On 12 May 2021, the EDPS received a request for prior consultation under Article 40 of the Regulation regarding the Data Protection Impact Assessment (the ‘DPIA’) on a new Customer Relationship Management system (the ‘CRM’) for the ECB.

The request for prior consultation sent by the ECB contained:

- a cover letter explaining the background, summarising the DPIA and explaining the need for a prior consultation (the ‘cover letter’);
- the DPIA report on CRM (the ‘DPIA report’); and
- Table II - the assessment of the risks to the rights and freedoms of natural persons and applicable mitigating measures (the ‘Assessment’).

Attached to the request for prior consultation were the following supporting documents:

- CRM Architecture Design Documents, describing the IT architecture of the CRM solution;
- e-CRM Criticality Assessment, conducted by the ECB IT security, providing for an overview and a rating of the confidentiality, integrity and availability of the CRM solution;
- ECB Dynamics 365 Review, describing the review findings by MS Dynamics 365 fast track team (the ‘Dynamics 365 Review’);
- Information provided by Microsoft to the ECB in March 2021 (the ‘Responses to sub-processors’ questionnaire’); and
- CRM brief description of documentation attached.

According to Article 40(2) of the Regulation, the EDPS is to issue his Opinion within a period of up to eight weeks of receipt of the request for consultation, with a possible extension of six weeks. No extensions were necessary in the present case. The Opinion has been issued within the applicable deadline, i.e. by 7 July 2021.

2. DESCRIPTION OF THE PROCESSING

2.1. The current CRM system

[REDACTED]

[REDACTED]

[REDACTED]

2.2. Description of the new CRM

A market vendor assessment launched in 2017 identified **Microsoft Dynamics 365 Public Cloud SaaS** as the CRM solution [REDACTED]. The implementation of the new CRM relies on Microsoft Azure cloud technologies, in particular Microsoft Azure Active Directory services⁴. The new CRM will “*support the ECB to fulfil its mandate to provide information on its activities to the general public.*”⁵

Specifically, the **purpose** of the project is to deliver a solution that provides functionalities and workflows for ECB wide contact, enquiry, and event management, and protocol-related functionalities. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] **The categories of data subjects** affected by the processing will include anyone in contact with the ECB, namely meeting and conference participants, members of the general public who address enquiries to the ECB, ECB employees, and persons visiting the ECB⁹. [REDACTED]

[REDACTED]

³ Cover letter, p. 3 and DPIA report, pp. 24, 39 and 59.

⁴ DPIA report, p. 53.

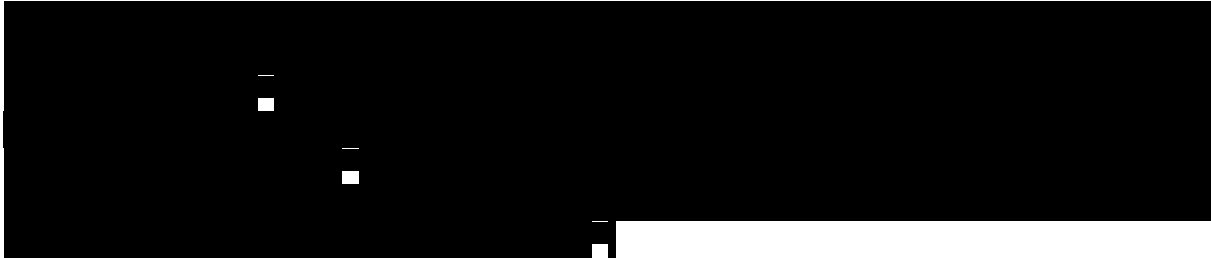
⁵ DPIA report, p. 39.

⁶ DPIA report, p. 38. A table describing the sets of processing operations is included in the DPIA report (pp. 36-38)

⁷ DPIA report, p. 7.

⁸ DPIA report, p. 4.

⁹ DPIA report, pp. 35 - 38.



Personal data will also flow to the CRM from (i) ECB staff, in the context of meeting room booking and meeting organisation; (ii) other EU institutions, in the context of meeting registrations for ECB committee and sub-structure meetings; and (iii) citizens, in the context of event and meeting registrations and related surveys and feedbacks, of public, media and statistical enquiries, and of visits to the ECB.



The DPIA identifies the ECB as the **controller** of the processing operations and Microsoft, a company based in the United States (the 'US'), as the **processor** of the data processed on the CRM.

According to the DPIA, Microsoft ensures that **transfers** of personal data outside the EEA to a third country are subject to the appropriate safeguards provided for in Article 46 of Regulation (EU) 2016/679 (the 'GDPR')¹⁵.

¹⁰ DPIA report, p. 42.

¹¹ <https://www.sap.com/about/company/what-is-sap.html>

¹² DPIA report, p. 24.

¹³ *Ibid.*

¹⁴ DPIA report, pp. 22 and 23.

¹⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1. DPIA report, pp. 25 and 26.

3. PRIOR CONSULTATION PURSUANT TO ARTICLE 40 OF THE REGULATION

3.1. The DPIA

According to the ECB, several elements triggered the need for a DPIA pursuant to Article 39 of the Regulation. First, the processing of data will take place on a large scale¹⁶. Second, it will relate to an innovative use or application of technological or organisational solutions that can involve novel forms of data collection and usage. Third, the CRM will process data concerning possibly vulnerable data subjects, namely the ECB employees who are in an unbalanced relationship vis-à-vis their employer. There may also be limited amounts of special categories of personal data being processed¹⁷.

Among the risks identified by the ECB in the Assessment, the DPIA report focuses in particular on the following three high risks to the rights and freedoms of natural persons: (i) non-compliance with the rules on international transfers in light of the new *Schrems II* judgment¹⁸; (ii) lack of control over Microsoft sub-processors; and (iii) certain limitations of the contract negotiated between the European Commission and Microsoft (an Inter-institutional Licence Agreement, the 'ILA').

The DPIA report identifies contractual, technical and organisational measures that the ECB will take to mitigate the risks it has identified and comply with the provisions of the Regulation.

The DPIA report also refers to the EDPB Recommendations 01/2020¹⁹ and includes some information on an assessment by the ECB of the mitigating measures and other safeguards limiting access to ECB personal data from countries outside the EEA based on the

¹⁶ According to the ECB in respect of the category of data subjects: "*Contacts who had/have/will have a relation with ECB in the context of the business managed via the CRM system.*" [REDACTED]

¹⁷ DPIA report, p. 4.

¹⁸ Judgement of the Court of Justice of 16 July 2020 in case C-311/18, *Data Protection Commissioner v. Facebook Ireland LTD and Maximillian Schrems ("Schrems II")*, ECLI:EU:C:2020:559.

¹⁹ [EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data](#), version for public consultation adopted on 20 November 2020 and version after public consultation adopted on 18 June 2021.

information provided by Microsoft having regard US law (US Cloud Act²⁰, 50 U.S.C. § 1881a (FISA 702)²¹ and EO 12333²²).²³

The DPIA report notes that “*even if Standard Contractual Clauses [the ‘SCCs’] are considered a suitable safeguard by the Regulation, they only provide protection on a contractual basis, i.e. put the ECB in a weaker position in case of issues since it would have to try to enforce the contract and this might be difficult.*”²⁴ The DPIA report further notes that Microsoft mentioned SCCs as a transfer tool already implemented for its sub-processors based in third countries, except the US. The DPIA report then refers to a renegotiated contract that the European Commission will sign with Microsoft which will include SCCs for transfers of personal data to the US and that once all SCCs are in place, the next step will be to identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence²⁵.

According to the DPIA report, the ECB decided to store its customer data at rest in the Netherlands and Ireland and it has a policy in place to not allow the usage of Dynamics 365 outside the EEA²⁶. The DPIA nevertheless identifies the high risk that customer and other personal data will be transferred outside the EU/EEA without appropriate safeguards²⁷. Indeed, the DPIA report notes that based on the information provided by Microsoft to the ECB, Microsoft transfers personal data to the US, but also to other third countries (India, China, Russia, and Serbia)²⁸. According to the clarifications received by the ECB, Microsoft has a number of sub-processors operating in those countries²⁹. These sub-processors access customer data for purposes such as support, troubleshooting and service maintenance, and compliance with legal obligations.³⁰ Service generated data and diagnostic data, which may contain personal data, are transferred to Microsoft centralised back-end systems in the US for longer-term storage³¹.

The DPIA report notes that, in the case of a transfer of customer data and personal data that Microsoft processes on the ECB’s behalf out of the EEA to the US or any other country in which Microsoft or its sub-processors operate, Microsoft relies on the SCCs agreed in the

²⁰ US Clarifying Lawful Overseas Use of Data Act (H.R.4943). A bill to amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes, S.2383 — 115th Congress (2017-2018).

²¹ Section 702 of the Foreign Intelligence Surveillance Act. United States Code, 2012 Edition, Supplement 2, Title 50 - WAR AND NATIONAL DEFENSE, CHAPTER 36 - FOREIGN INTELLIGENCE SURVEILLANCE, SUBCHAPTER VI - ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES, Sec. 1881a - Procedures for targeting certain persons outside the United States other than United States persons, S. Res.400 94th Congress.

²² Executive Order 12333, United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)).

²³ DPIA report, pp. 28 to 30.

²⁴ DPIA report, p. 28.

²⁵ DPIA report, p. 30.

²⁶ DPIA report, p. 31.

²⁷ DPIA report, p. 28.

²⁸ DPIA report, p. 30.

²⁹ See responses to sub-processors’ questionnaire, second sheet (‘MS sub-processors list’), row 6.

³⁰ See responses to sub-processors’ questionnaire, third sheet (‘Question and answer’), row 12.

³¹ DPIA report, p. 32.

ILA, and on the technical and organisational measures set forth in the Data Protection Addendum to the ILA (the 'DPA'). If there are any onward transfers to third locations initiated by Microsoft, such transfers are also subject to SCCs. The DPIA report also notes that, as provided in the DPA, customer data and personal data that Microsoft processes on a customer's behalf may not be transferred to, stored or processed in the US or any other country in which Microsoft or its sub-processors operate, except in accordance with the safeguards provided for in the DPA. According to the DPIA report, "*taking into account such safeguards, the customer appoints Microsoft to perform any such transfer of Customer Data and personal data to any such country and to store and process Customer Data and personal data to provide the Online Services*". The DPIA report further notes that after the *Schrems II* ruling, Microsoft no longer relies on the Privacy Shield as legal basis for transfers of personal data to the US. As soon as the Commission adopts new SCCs, Microsoft will rely on them.³²

According to the DPIA report, although Microsoft has presented mitigating measures and other safeguards limiting access to ECB personal data from countries outside the EEA (see above), by taking into consideration:

- the format of the data to be transferred (in plain text/pseudonymised or encrypted; Microsoft holds the encryption key for data in transit and offers the solution to the ECB to hold the encryption key for data at rest but saved in a Microsoft cloud);
- the nature of the data (access might be provided to customer content data which might also include sensitive data);
- the length and complexity of data processing (transfers of personal data for technical development, test, maintenance and support, livesite operations, reliability engineering, customer success, testing and deployments, localisation, Microsoft business operations and legal obligations purposes); and
- the number of actors involved in the processing (Microsoft US, 13 sub-processors, but maybe other sub-processors of Microsoft Azure) and the relationship between them (contracts with Microsoft and SCCs in place),

it is not very clear if the mitigating measures applied by Microsoft ensure an adequate protection of rights and freedoms of the data subjects.³³

The DPIA report concludes that, in light of the mitigating measures, safeguards and mechanisms, compliance with some of the data protection requirements has been partially demonstrated and **that the controls chosen in the DPIA are sufficient to reduce those risks to an acceptable level. The DPIA report equally concludes, however, that high risks still remain** regarding compliance with the rules on international transfers in light of the new *Schrems II* judgment, lack of control of use of sub-processors and certain limitations of the contract with Microsoft.³⁴

Finally, the DPIA report details the further actions to be taken to respond to these three remaining risks, namely (i) collecting detailed information from Microsoft on the Dynamics 365 tool architecture, data management and data protection processes; (ii) the mitigating measures Microsoft implemented already or plans to implement in the next months; and (iii)

³² DPIA report, p. 31.

³³ DPIA report, p. 30.

³⁴ DPIA report, p. 58.

the signature by the Commission of a renegotiated contract with Microsoft in the coming months, which will include SCCs for transfers and other additional measures. [REDACTED]

Following the advice of its Data Protection Officer (the ‘DPO’), the ECB decided to launch a prior consultation with the EDPS “for advice on whether the identified mitigation measures can be considered sufficient to appropriately address the high risks”³⁶.

3.2. Need for prior consultation and scope of the Opinion

Article 40(1) of the Regulation provides that the controller must consult the EDPS prior to processing where a DPIA under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation. The controller must seek the advice of the DPO when carrying out a DPIA and on the need for prior consultation³⁷.

In the present case, the CRM represents a substantial change in the manner in which the ECB manages its customer relations, namely by using a tool hosted in the cloud providing for transfers of personal data outside the EEA, including to sub-processors, procured on the basis of an ILA that is currently under review.

The DPIA on the new CRM, based on Microsoft Dynamics 365, identified a number of high risks. The DPIA further identifies a number of measures by the ECB and Microsoft, as well as other measures, like the new ILA including new SCCs being negotiated by the Commission with Microsoft to address and mitigate those risks. The controller is of the view that

³⁵ DPIA report, p. 59.

³⁶ DPIA report, pp. 58 and 59.

³⁷ See also recital 57 of the Regulation, *in fine*: “[w]here types of processing operations involve using new technologies, or are of a new kind in relation to which no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing... a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation” and recital 58 of the Regulation: “Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the European Data Protection Supervisor should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which could result also in a realisation of damage or interference with the rights and freedoms of the natural person...”

forthcoming mitigating measures will be sufficient, whereas the DPO sees three high remaining risks and advised a prior consultation of the EDPS.

Given the identified high risks and uncertainty or ambiguity in the DPIA conclusions regarding the mitigating measures, the EDPS considers that the prior consultation is admissible to advise “*on whether the identified mitigation measures can be considered sufficient to appropriately address the high risks*” (as requested by the ECB). The Opinion of the EDPS on this prior consultation therefore focuses on the appropriateness of the measures envisaged to mitigate the high data protection risks identified by the ECB³⁸, i.e. (i) non-compliance with the rules on international transfers in light of the new *Schrems II* judgment; (ii) lack of control over Microsoft sub-processors; and (iii) certain limitations of the ILA. This Opinion analyses whether the ECB has sufficiently mitigated these risks.

Following the *Schrems II* judgement, the EDPS has concerns as to the level of protection afforded to transferred data in third countries, and in particular the US, when personal data is transferred by EUIs or on their behalf to Microsoft and sub-processors when EUIs use Microsoft services. The EDPS has an ongoing investigation into the European Commission’s use of Microsoft Office 365³⁹. The investigation will cover the new ILA. The results of that investigation should therefore be instructive for the ECB. Any observations, remarks and recommendations made by the EDPS in this Opinion are without prejudice to any findings, conclusions and action the EDPS may take in the ongoing EDPS investigations.

4. LEGAL AND TECHNICAL ASSESSMENT OF THE MITIGATING MEASURES IDENTIFIED IN THE DPIA

4.1. Measures to mitigate the high risk of non-compliance with the rules on international transfers in light of the *Schrems II* ruling

The ECB has identified the risk of a transfer of personal data to the US, and for support services offered by sub-processors in third countries such as India, China, Russia and Serbia, as of probable likelihood and of maximum severity⁴⁰. The risk, according to the Assessment, is that personal data, such as that included in customer data or diagnostic data, is transferred to a third country without adequate safeguards, which would imply that data subjects are not guaranteed an adequate level of data protection under the Regulation. The residual risk, after mitigation, remained, in accordance with the ECB’s analysis, still probable in likelihood and maximum in severity⁴¹.

³⁸ These risks are identified in the DPIA report (pp. 59 and 60) and further described in the Assessment (pp. 20 to 25, 44 to 50, and 72 to 82).

³⁹ https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en

⁴⁰ The ECB based its analysis on the Matrix of the French Data Protection Authority (CNIL) (see Assessment, p. 1).

⁴¹ Assessment, pp. 20-23, further repeated in pages 44-47 and 72-75, and DPIA report, p. 30.

The EDPS recalls that absent an adequacy decision for transfers to, among other destinations, the US, controllers and processors may transfer personal data to a third country⁴² only if appropriate safeguards are provided, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available⁴³. Such safeguards may be provided in SCCs or another transfer tool. The transfer tool relied on must ensure that data subjects, whose personal data are transferred to a third country pursuant to that transfer tool, are afforded a level of protection in that third country that is essentially equivalent to that guaranteed within the EU by EU data protection law, read in the light of the Charter.⁴⁴

However, the use of SCCs or another transfer tool (e.g. *ad hoc* contractual clauses) does not substitute the individual case-by-case assessment that an EUI must, in accordance with the *Schrems II* judgement, carry out to determine whether, in the context of the specific transfer, the third country of destination affords the transferred data an essentially equivalent level of protection to that in the EU. The EUI, where appropriate in collaboration with the data importer in the third country, must carry out this assessment of the effectiveness of the proposed safeguards before any transfer (including by way of remote access) is made or a suspended transfer is resumed.

The assessment by the EUI should take into consideration the specific circumstances of the transfer (e.g. categories of transferred data, purposes for which they are transferred and processed in the third country and how) and all the actors participating in the transfer (e.g. controllers, processors and sub-processors processing data in the third country), as identified in the mapping of the transfers. The EUI will also need to factor into this assessment any envisaged onward transfer.⁴⁵

Where the required essentially equivalent level of protection for the transferred data is not effectively ensured, because the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the used SCCs for transfers or another transfer tool, the EUI must implement contractual, technical and organisational measures to effectively supplement the safeguards in the transfer tool, where necessary together with the data importer.⁴⁶

This process of assessing the level of protection in the third country and whether supplementary measures are needed, and then identifying effective supplementary measures, is commonly called a ‘transfer impact assessment’. The methodology to be used is available in the EDPB Recommendations 01/2020 and, as regards the assessment of access by public authorities for surveillance purposes, in the EDPB Recommendations 02/2020 on European Essential Guarantees⁴⁷. The ECB must thus perform a transfer impact assessment

⁴² Remote access by an entity from a third country to data located in the EEA is also considered a transfer.

⁴³ Article 48(1) of the Regulation.

⁴⁴ See paragraphs 96 and 103 of the *Schrems II* judgement and recitals 65 and 70 and Article 46 of the Regulation.

⁴⁵ See Article 46 of the Regulation and paragraphs 33 and 34 of the EDPB Recommendations 01/2020.

⁴⁶ See paragraphs 54 and Annex 2 of the EDPB Recommendations 01/2020.

⁴⁷ [EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020.](#)

taking into account full information on all the circumstances of the transfer (including information yet to be provided by Microsoft and the Commission). Following this, it must, if necessary, implement effective supplementary measures in order to ensure an essentially equivalent level of protection for the personal data that will be transferred to a third country in the ECB's use of Microsoft Dynamics 365.

In light of the information in the DPIA, in particular that mentioned above in section 3.1.⁴⁸, the EDPS takes the view that the DPIA carried out by the ECB does not appear to be based on all the information necessary to fully assess all the risks concerning international transfers, identified as high by the ECB. In particular, the assessment by the ECB does not seem to consider all the actors and all the third countries involved for transfers in the ECB's use of Microsoft Dynamics 365, which is the minimum essential information for a meaningful 'transfer impact assessment' in line with the *Schrems II* judgement and the EDPB Recommendations 01/2020⁴⁹.

The EDPS stresses that in principle, non-compliance by an EUI with EU data protection law as interpreted by the Court of Justice should not be an "acceptable" risk for an EUI. Every EUI aware of risks for data subjects should continuously seek to implement effective mitigating measures to ensure that the data subjects, as the ultimate affected parties, are provided with an essential equivalence of protection when data is transferred, as required by the Charter of Fundamental Rights.

In order to provide useful comments to the ECB, the EDPS has decided to assess the measures envisaged in the DPIA for mitigation of risks relating to international transfers relying on the recommendations made by the EDPB in its Recommendations 01/2020. The information on measures relating to sub-processors is analysed in detail in the dedicated section 4.2. below. However, certain measures relating to sub-processors are also relevant for mitigation of risks relating to international transfers, when those sub-processors are located in third countries. The assessment of those risks is thus included in the current section. The EDPS therefore makes in particular the following observations and remarks on certain technical, organisational and contractual mitigating measures and actions identified by the ECB in the DPIA that are relevant for international transfers.

4.1.1. Contractual safeguards and mitigating measures

Contractual commitments in the ILA and SCCs for transfers

⁴⁸ See also e.g. statements: "Investigate which data is transferred to third countries" on pp. 21, 45 and 74 of the Assessment and "Investigate which data is transferred to third countries by subprocessors" on pp. 23, 47 and 75 of the Assessment.

⁴⁹ See in particular Step 1 'Know your transfers' of the roadmap in the EDPB Recommendations 01/2020. In line with existing obligations in Articles 4, 5, 6, 9, 26, 29, 30 and Chapter V of the Regulation, the EUIs need to know and control data flows within and outside the EU.

The EDPS understands from the DPIA that the ECB decided, in principle, to store its Dynamics 365 customer data at rest in the EEA⁵⁰. However, the DPIA also acknowledges that transfers and onward transfers of customer data and other categories of personal data to third countries to Microsoft or its sub-processors are nevertheless possible, subject to **SCCs** and **commitments on technical and organisational measures as agreed in the initial ILA and the DPA**.⁵¹ The DPIA refers to the ongoing negotiations on a **new ILA** that will cover the data protection issues reported in the *Schrems II* ruling as a strong mitigating measure⁵². According to Microsoft, all transfers of personal data out of the EU by the platforms to be used by the ECB in its CRM tool will be governed by SCCs, as described in the ILA⁵³. According to the DPIA, the new contract between the Commission and Microsoft, which the ECB expected to be signed by the end of June 2021, will provide for the use of SCCs for transfers of personal data to the US, as well as some additional safeguards⁵⁴. Microsoft has committed to provide all necessary information to the ECB allowing for an overview of how data is processed outside the EEA in the CRM⁵⁵. Microsoft will also rely on **new SCCs for transfers adopted by the Commission**⁵⁶.

SCCs for transfers (under Article 46 GDPR or Article 48 of the Regulation) mainly contain appropriate safeguards of a contractual nature that may be applied to transfers to all third countries.⁵⁷ In this respect, the EDPS notes that, according to the DPIA, personal data may be transferred to any third country where Microsoft or its sub-processors operate.⁵⁸ These could be third countries where SCCs, may, together with safeguards and measures (e.g. those in accordance with Articles 33 and 36 of the Regulation) already foreseen by the controller and processor, ensure an essentially equivalent level of protection. Such may be the case for transfers to Serbia, which, while not benefitting from an adequacy decision of the Commission has, as a candidate country for accession to the EU, signed binding international commitments and is in the process of transposing EU legislation into its national legislation

⁵⁰ DPIA report, p. 31, section "Data locations in the EEA": "With Dynamics 365, customers can specify the region where their **customer data at rest** will be stored. Therefore, ECB has decided to store their data within the EEA only, specifically **in the locations of West Europe (Netherlands) and North Europe (Ireland)**." (emphasis added)

⁵¹ DPIA report, p. 31, section 3.6.3 "Transfer tool": "[C]ustomer Data and personal data that Microsoft processes on a customer's behalf may not be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its subprocessors operate, except in accordance with the safeguards provided below in this section. Taking into account such safeguards, the customer appoints Microsoft to perform **any such transfer of Customer Data and personal data to any such country** and to store and process Customer Data and personal data to provide the Online Services. In case of a transfer of Customer Data or personal data out of the European Union and the European Economic Area to the United States or any other country in which Microsoft or its subprocessors operate, Microsoft relies on the Standard Contractual Clauses as agreed in the initial ILA and included as Attachment 2 to the DPA and on appropriate technical and organizational measures as set forth in detail in the DPA..." (emphasis added)

⁵² DPIA report, p. 30 and Assessment pp. 20, 25, 44, 50, 73 and 78.

⁵³ See responses to sub-processors' questionnaire, third sheet ('Question and answer'), row 22.

⁵⁴ DPIA report, p. 59.

⁵⁵ Assessment, pp. 20-21, 45, and 73.

⁵⁶ DPIA report, p.31.

⁵⁷ See paragraph 23 of the EDPB Recommendations 01/2020.

⁵⁸ DPIA report, p. 31.

to harmonise it to that of the EU *acquis*⁵⁹. However, there are third countries (such as the US, Russia, China and India) to which personal data may be transferred through use of Microsoft Dynamics 365 where there is a high risk that the SCCs are unlikely alone to provide essentially equivalent protection. Additional contractual, technical and organisational measures (“*supplementary measures*”) to ensure the required level of protection will thus be required for such countries.⁶⁰ Some measures may be effective in one situation while not effective in another. The situation in different third countries to which personal data will be transferred may therefore require different approaches and different combinations of supplementary measures.

The Commission issued new SCCs on 4 June 2021⁶¹. The EDPS and the EDPB have issued joint opinions on the draft SCCs between controllers and processors⁶² and on the draft SCCs for the transfer of personal data to third countries under the GDPR⁶³, as proposed by the Commission. The EDPS notes that the new SCCs for transfers include that parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer prevent the data importer from fulfilling its obligations under the SCCs.⁶⁴ In this respect, the EDPS stresses that such an assessment and implementation of any necessary safeguards and measures to supplement⁶⁵ those present in the SCCs is to be done *before* the SCCs are in place and not, as stated in the DPIA, once all SCCs are in place⁶⁶.

Privileges and immunities

Relatedly, and although not identified as a high risk, the DPIA mentions that with the adoption of the US Cloud Act there is a risk that Microsoft be required to provide personal data to a US authority. In this respect, the DPIA considers as an appropriate mitigating measure the fact that the **ECB enjoys extensive privileges and immunities** under US law, according to the US Executive Order 13307 of May 29, 2003⁶⁷, by which: (i) in particular, the ECB’s archives and official correspondence enjoy an absolute inviolability, and the US Government is obliged to respect that inviolability and to prevent its infringement by other

⁵⁹ The Stabilisation and Accession Agreement with Serbia provides obligations of harmonisation with EU law, including fundamental rights and data protection law.

⁶⁰ See Step 4 ‘Adopt supplementary measures’ of the roadmap in the EDPB Recommendations 01/2020. “*Supplementary measures*” are by definition supplementary to the safeguards the Article 48 of the Regulation - or Article 46 GDPR - transfer tool already provides and to any other applicable security requirements (e.g. technical security measures) established in the Regulation or the GDPR.

⁶¹ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

⁶² https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en

⁶³ https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en

⁶⁴ See Section III, Clause 14 of the new SCCs for transfers under the GDPR.

⁶⁵ Any contractual supplementary measures and contractual commitments to implement technical and organisational measures that the EUIs identified during the transfer impact assessment.

⁶⁶ DPIA report, p. 30.

⁶⁷ US Executive Order on the ECB <https://www.federalregister.gov/documents/2003/06/03/03-14117/european-central-bank>

parties; and (ii) in addition, absent explicit waiver by the ECB, the ECB's property and assets, wherever located and by whomsoever held, are immune from attachment, execution, search and confiscation.

Hence, according to the DPIA, providers of electronic communications and remote computing services to the ECB are not required to disclose any ECB data to US governmental entities under the US Stored Communications Act (as amended by the US CLOUD Act), as this would infringe the ECB's privileges, exemptions and immunities under US law. The DPIA mentions that Microsoft publishes a transparency report bi-annually on the number of law enforcement requests it has received.⁶⁸ The DPIA further notes that Microsoft acknowledged in the ILA signed with the Commission that the Customer is subject to the privileges and immunities outlined in Protocol 7 of the Treaty on the Functioning of the European Union⁶⁹ as an appropriate mitigating measure⁷⁰.

The EDPS considers that respect of the privileges and immunities of the EUIs, as recognised in the Treaties and by a third country, in particular e.g. the inviolability of their archives, contributes to the protection of personal data that EUIs process or that is processed on EUIs' behalf in the EU and outside the EU. However, the EDPS has already had the opportunity to also emphasise to EUIs that they had few guarantees under the 2018 ILA that they were in a position to defend their privileges and immunities against disclosure requests from third-country governments and processors subject to their jurisdiction⁷¹. This was contrary to Articles 4(1)(f) and 49 of the Regulation.

Microsoft and the European Commission concluded a revised version of the ILA in May 2021. If the ECB has adhered to this amended ILA or intends to, it should conduct a thorough review to assess whether the ECB now meets its obligations under Articles 4(1)(f) and 49 of the Regulation.

EUIs must ensure that transferred data are afforded an essentially equivalent level of protection as in the EU/EEA when that data is transferred to a third country. Therefore, as part of the transfer impact assessment, the ECB should establish without legal ambiguity how and to which extent:

- (i) the privileges and immunities, as extended to the ECB by the US Executive Order 13307 of May 29, 2003, apply to and are binding upon the public authorities in the US and are not rendered ineffective by the concurrent application of other obligations of US Intelligence Community authorities⁷²;
- (ii) the ECB (as owner of the data transferred to and held by Microsoft and its sub-processors on the ECB's behalf) is in a position to effectively defend against disclosure

⁶⁸ <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>

⁶⁹ DPIA report, p. 28.

⁷⁰ Assessment, pp. 24-25, 49, and 77-78.

⁷¹ See pp. 45-49 of EDPS report of March 2020 on the investigation into the use of Microsoft products and services by Union institutions, bodies, offices and agencies (the 'the March 2020 Investigation Report'), section 7 'Unauthorised disclosure' and respective recommendations.

⁷² As defined by the relevant US legislation, e.g. 50 U.S.C. § 3003(4).

requests⁷³ not authorised by EU law from third country governments, by relying on its privileges and immunities; and

(iii) Microsoft and its sub-processors subject to third country jurisdiction can notify and redirect disclosure requests they receive to the ECB and legally challenge disclosure requests by invoking privileges and immunities extended to the ECB.

If it considers it appropriate, the ECB should convey the results of its assessment to the European Commission and taking follow-up actions with it.

4.1.2. Technical mitigating measures

Encryption

According to the DPIA, personal data transferred outside of the EU/EEA is encrypted.

Microsoft offers to encrypt data at rest through disk encryption using customer-managed keys and infrastructure encryption using platform-managed encryption keys. The ECB's DPIA notes that it is not possible for it to manage the encryption keys for data in transit⁷⁴. As concerns data at rest, it also points out the keys are stored within Microsoft Azure Key Vault⁷⁵. The DPIA states that *"For clarity, the Dynamics 365 and Power Platform services in scope for ECB's CRM tool utilize Dataverse to store Customer Data at rest, and ECB can manage encryption keys as described in the above documentation link. However, such encryption key would be saved in a Microsoft Azure cloud."*⁷⁶

On 30 June 2021, the ECB informed the EDPS that *"the Customer Managed Key solution was discarded..."*⁷⁷ The ECB explained that *"the increase on the level of security it would generate (i.e. possibility for the ECB to autonomously revoke the key) does not compensate for the risks it would introduce from an operational and availability perspective"* and that *"the key created by the ECB will have anyway to be given to Microsoft to operate the CRM solution (key stored in MS key vault) with increased security risks"*. The ECB noted also that *"the measures proposed by Microsoft do not in any way offer additional technical assurance that "lawful requests"/"foreign intelligence access" is hampered or prevented"*. It expressed the view that *"[n]on-technical controls exist for this, to name the immunity of the ECB, as well as ensuring*

⁷³ In actions or appeals against such disclosure requests as provided in the third country laws, applicable obligations under international law and principles of international comity.

⁷⁴ DPIA report, p. 20.

⁷⁵ DPIA report, p. 30.

⁷⁶ DPIA report, p. 20.

⁷⁷ The ECB provided a summary of its security assessment: *"- If Microsoft manages the TDE encryption key, it would be generated and stored in the respective AKV following Microsoft's key lifecycle management; - If the ECB manages the TDE encryption key, we would not have full control over the key lifecycle. It will be generated on ECB premises using ECB equipment, but it will be exported to a Microsoft controlled AKV which is outside the ECB tenant hosting the CRM; - It is supposed to prevent a malicious admin acquiring the data at rest and using access to the key infrastructure to read the data. Not taking into account that this requires collusion from distinct operational groups in Microsoft as well as extensive failure of their existing security control layers, we would not realistically be able to respond with a key revocation as the ECB would need to be aware of the malicious act taking place; - These observations do not take into account the increased operational burden."*

the locality of live and backup data for the CRM tenant and the Azure AKV handling encryption are within the EEA, and at least from a pure security perspective they are sufficient controls so we can be confident risks of transfer outside the EU are minimized.”

The EDPS has commented on the ECB’s privileges and immunities in the previous section. The EDPS recalls that US data importers that fall under FISA 702 are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible. Hence, as stated in the EDPB Recommendations 01/2020, in situations where the keys are not retained solely under the control of the data exporter, or where the processing by cloud services providers or other processors requires access to data in the clear, encryption does not provide for an effective supplementary measure necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence⁷⁸. The same can be said when such encryption is already foreseen as a safeguard contained in the transfer tool relied on to transfer personal data.

The ECB has decided to allow Microsoft to manage its encryption keys. Even if it had opted for the customer-managed key solution offered by Microsoft, the fact that the key would be saved in the Azure cloud would allow Microsoft to access the keys in response to an order or request for access from US public authorities. Encryption solutions that do not give the ECB sole control of the encryption keys do not provide a means of complying with the *Schrems II* judgement or associated EDPB recommendations.

Pseudonymisation

According to the DPIA, service generated data typically contains either user identifying information or **pseudonymous identifiers** at time of creation, each of which are personal data. Service generated data is moved from the data centres where they are initially created to centralised Microsoft back-end systems for longer-term storage. These systems are located in the US. Prior to transfer, end user identifying information is pseudonymised as a privacy protective measure, so that any personal data in service generated data transferred out of the EEA is limited to pseudonymous data. Any personal data contained in service generated data remains subject to the protections contracted in the DPA.⁷⁹

Additionally, the DPIA notes that some online services include software that is installed locally to customer client devices. Microsoft collects diagnostic data from such client software. The data is transferred to Microsoft centralised back-end systems in the US for longer-term storage to enable Microsoft to ensure software is performing. In some cases, the diagnostic data contains personal data in the form of pseudonymous identifiers. Any personal data contained in diagnostic data remains subject to the protections contracted in the DPA⁸⁰.

⁷⁸ See paragraphs 81, 84, 94 and 95 of the EDPB Recommendations 01/2020.

⁷⁹ DPIA report, pp. 31 to 33.

⁸⁰ Ibid.

According to the DPIA, to process personal data for its business operations, Microsoft relies on processing of service generated data or diagnostic data that may contain pseudonymous identifiers to calculate aggregate metrics or measures (e.g., monthly active users for a service), where the service generated data and diagnostic data have already been transferred to the US to provide the online services. Processing of customer data for business operations includes such activities as measuring volume of data for consumption-based billing and does not involve either access to content of customer data or transfer of such customer data from the locations in which it is hosted, unless required to fulfil Microsoft's legal obligations. This applies for both Microsoft employees and for sub-processors.⁸¹

The EDPS recalls that for pseudonymisation to be considered an effective mitigating measure and safeguard when personal data is transferred to a third country, a number of conditions should be present, in particular as regards additional information, with the main aim of reducing the possibility of singling out data subjects, linkability and inferences⁸². The DPIA does not assess whether the pseudonymisation measure in place is an effective supplementary measure in light of the conditions described in the EDPB Recommendations 1/2020. The EDPS furthermore notes that, based on the information in the DPIA, the necessity of collecting and processing diagnostic data is neither clear nor sufficiently demonstrated in line with the principle of accountability with respect to the purposes. The EDPS recalls that controllers must verify that the data transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.⁸³

Access control

According to the DPIA, Microsoft has implemented organisational and technical **measures to control access by Microsoft personnel to customer data** in the services. In this respect, the EDPS recalls that where the processing by cloud services providers or other processors requires access to data in the clear and where the power granted to public authorities of the recipient country to access the transferred data in question goes beyond what is necessary and proportionate in a democratic society, the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent such access by public authorities from infringing on the data subject's fundamental rights.⁸⁴ Furthermore, access controls, access logs and other similar trails that do not or cannot⁸⁵ distinguish between accesses due to regular business operations and accesses due to orders or requests for access from third country public authorities do not constitute an effective measure.

The DPIA notes that Microsoft has implemented 'just in time' access for the 13 contract staff sub-processors directly involved in Dynamics 365 service provision. The contract staff are

⁸¹ DPIA report, pp. 32 and 33.

⁸² See paragraphs 85 to 89 of the EDPB Recommendations 01/2020. See also [Article 29 Working Party. "Opinion 05/2014 on Anonymisation Techniques" \(WP 216\)](#).

⁸³ Article 4 of the Regulation.

⁸⁴ See paragraphs 94 and 96 of the EDPB Recommendations 01/2020.

⁸⁵ E.g. because the legislation of the third country (such as in the US) prohibits the data importer from informing the controller about the disclosure request received.

assigned to a “*secure workstation for a limited period of time only with management approval*”.⁸⁶ Microsoft has stated that: “*The network traffic to/from these Secure Admin Workstations is tightly locked down and controlled only allowing the interaction that is needed to support the service and therefore to prevent further transmission from these workstations for other purposes or destinations.*”⁸⁷ Microsoft has also advised that: “*access granted is based on role-based access controls; multi-factor authentication is required; Just-In-Time ‘JIT’ access ensures any elevated access is temporary and least-privileged; production access is limited to secure admin workstations and isolated identities, as detailed in Microsoft’s recent presentation to the ECB; access requests are audited, logged and monitored; and risky elevations are alerted 24x7x365 to Microsoft’s security personnel.*”⁸⁸

Based on the information available, the EDPS considers these ‘JIT’ mitigating measures to be of best-practice standard. It must be noted, however, that even limited access by sub-processors constitutes access. Any type, level or duration of access is open to exploitation by state actors in the jurisdictions to which those sub-processors are subject. As a result, the JIT measures do not provide a means of complying with the *Schrems II* judgement or EDPB Recommendations 01/2020.

Microsoft has also implemented its ‘Customer Lockbox’ solution, which will allow the ECB to directly approve individual requests for access to data⁸⁹. This is positive. The EDPS notes, however, that this solution only applies in respect of the few occasions on which it is necessary for a support engineer to access more data than Microsoft already collects through extensive telemetry and debugging tools.⁹⁰ It is also unclear to the EDPS what information is provided to the ECB in the approval request or what the ECB’s options are should it not wish to approve the access. If the consequences of refusing an access request are that the system will not work or will work only with reduced functionalities, the ECB may have no real choice but to approve access.

4.1.3. Organisational mitigating measures

Provision by processor of information on data transferred to sub-processors

Another mitigating measure identified in the DPIA is the fact that **Microsoft has provided the ECB with information** related to which type of data is transferred, which sub-processors are involved and to what extent they have access to data⁹¹.

⁸⁶ DPIA report, p. 59.

⁸⁷ See responses to sub-processors’ questionnaire, third sheet (‘Question and answer’), row 8.

⁸⁸ See responses to sub-processors’ questionnaire, third sheet (‘Question and answer’), row 11. The ECB has further confirmed the implementation of the ‘JIT’ access approach in an e-mail sent to the EDPS on 30 June 2021.

⁸⁹ The ECB has confirmed the implementation of the ‘Customer Lockbox’ solution in an e-mail sent to the EDPS on 30 June 2021.

⁹⁰ <https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide>

⁹¹ DPIA report, p. 59, and Assessment, pp. 20-21, 44-45 and 73.

The EDPS recalls that provision of such information by a processor to a controller is not a measure to mitigate a risk, but the necessary prerequisite information for the controller to identify and assess a risk in order for that risk then to be addressed by certain actions. Without this information, a controller cannot appropriately carry out a DPIA in line with Article 39 of the Regulation nor can it carry out a meaningful transfer impact assessment to comply with Chapter V of the Regulation.

Processing of personal data as instructed by the controller

The DPIA notes that **customer data is processed as instructed** by users. The processing may entail data transfers in two general categories: (i) where relevant software is not present in the hosting location there will be transfer of the relevant customer data for transient processing in another location to return the result requested by the user; or (ii) users may initiate an affirmative transfer of data to a third country, such as by sending an e-mail to a recipient located in another country. However, the DPIA reveals that Microsoft does not only act under instructions but may also process and transfer personal data of its own accord.⁹²

The EDPS recalls that processing of personal data by a processor or sub-processor as instructed by the controller is an obligation stemming from data protection law.⁹³ Under Article 29(3)(a) and Article 30 of the Regulation, the processor and any person acting under the authority of the controller or of the processor is to process personal data only on documented instructions from the controller, including with regard to transfers of personal data⁹⁴, unless required to do so by EU or Member State law to which the processor is subject⁹⁵. A processor or service provider transferring personal data without or not in line with instructions of the controller is infringing data protection law.⁹⁶

Transparency reports by Microsoft

According to the DPIA, the ECB requested the following clarifications:

“1) For Microsoft and its US and non-US sub-processors, whether: a. They are subject to 50 U.S.C. § 1881a (= FISA 702) or to any other law that could be seen as undermining the protection of personal data under the Regulation 2018/1725 (Article 46); b. They cooperate in any respect with US authorities conducting surveillance of communications under EO 12.333, should this be mandatory or voluntary; and c. They have implemented appropriate

⁹² DPIA report, pp. 31 to 33.

⁹³ See section 1.3.1 ‘The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR’ of the [EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR](#).

⁹⁴ See in this regard paragraph 116 of the EDPB Guidelines 07/2020: “*The duty for the processor to refrain from any processing activity not based on the controller’s instructions also applies to transfers of personal data to a third country or international organisation. The contract should specify the requirements for transfers to third countries or international organisations, taking into account the provisions of Chapter V of the GDPR.*”

⁹⁵ The processor has an obligation to inform the controller of such requirement before starting the processing. In any case, any transfer or disclosure may only take place if authorised by Union law, including in accordance with Article 49 of the Regulation. See in this regard paragraph 118 of the EDPB Guidelines 07/2020.

⁹⁶ See in this regard paragraph 117 of the EDPB Guidelines 07/2020: “[i]f the instructions by the controller do not allow for transfers or disclosures to third countries, the processor will not be allowed to assign the processing to a sub-processor in a third country, nor will he be allowed to have the data processed in one of his non-EU divisions.”

technical and organisational measures (see Article 33 Regulation 2018/1725) for every step of the processing operations which ensure that mass and indiscriminate processing of personal data by or on behalf of authorities in transit (such as under the “Upstream” program in the US) is made impossible. If so, a brief description on which technical and organisational measures (including encryption) have been taken shall be included.

Although Microsoft also publishes bi-annual reports about orders from the security agencies, through FISA-orders, these reports only provide total aggregate estimates, not split per country or per type of customer (consumer or Enterprise).

2) For sub-processors processing data in a third country, other than the US, whether they have any reason to believe that the legislation applicable prevents them from fulfilling the instructions received from the ECB and their obligations under the contract.”

The DPIA notes that Microsoft is willing to provide a **Transparency report** concerning access of data by US authorities. These reports can be provided at any point in time, when needed⁹⁷.

The EDPS notes that Microsoft’s biannual reports concerning legal demands from the US Government pursuant to national security laws since 2011 are already available online⁹⁸. This report provides, according to Microsoft, “*the greatest amount of transparency allowed by law*”⁹⁹. The EDPS further notes that the DPIA does not include any information concerning disclosure requests by other third country authorities.

The EDPS recalls that in order for a published transparency report to be effective, it should provide for information that is as relevant, clear and detailed as possible. When legislation in the third country prevents disclosure of detailed information, the data importer should employ its best efforts to publish statistical information or similar type of aggregated information¹⁰⁰. The EDPS notes, in this respect, that the DPIA qualifies the information provided by Microsoft as “*aggregate estimates, not split per country or per type of customer (consumer or Enterprise)*”¹⁰¹.

In the EDPS’s view, without any information in the DPIA about the scope of the proposed Transparency report, or the conditions for it being considered as “*needed*”, or yet about how any information other than that already provided online would be “*allowed by law*”, the value of this Transparency report as an appropriate mitigating measure to address the identified high risk remains unclear.¹⁰²

In addition, the EDPS notes that Microsoft’s responses to the ECB’s questions state that: “*In light of the limited access by subprocessors and stringent controls (contractual and technical) in place to prevent physical transfers or copying of data when remote access occurs, Microsoft is*

⁹⁷ DPIA report, p. 59.

⁹⁸ <https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report>

⁹⁹ See responses to sub-processors’ questionnaire, third sheet (‘Question and answer’), row 26.

¹⁰⁰ See paragraphs 135 and 136 of the EDPB Recommendations 01/2020.

¹⁰¹ DPIA report, p. 29.

¹⁰² See paragraph 47 and Annex 3 of the EDPB Recommendations 01/2020.

not aware of any regulation in the covered jurisdictions that would require subprocessors to take data from remote locations and provide those to intelligence, law enforcement, administrative and regulatory agencies.”¹⁰³

The EDPS is not satisfied with this response. It is unclear on what basis Microsoft has made this assessment.¹⁰⁴ Its reference to sub-processors’ limited access suggests that an important factor is how likely it considers access by third-country authorities to ECB data to be. In view of the EDPB Recommendations 1/2020, a risk-based or likelihood-of-access approach to assessing third-country laws raises serious concerns regarding the level of protection afforded to data subjects.

Disabling of optional connected experiences

Finally, the DPIA refers to implemented alternative solutions to **avoid transfers of data** related to “*connected and optional connected experience*”¹⁰⁵. According to the DPIA, “*In order to be compliant with ECB Data Protection rules, the project team has implemented a workaround to switch off the telemetry settings as part of Office 365 Connected Experiences. To enable Dynamics 365 App for Outlook, ECB will make sure ‘Optional Connected Experiences’ are disabled and turned off in order to avoid sending data to third parties add-ins which are part of the Connected Experiences package. Therefore, the ECB and MS agreed upon using the ‘Admin deployed’ approach so that email information is exclusively transferred to Dynamics 365. Technically the ECB has deployed in the on-premises exchange server a so-called Custom Manifest file which will enable the add-in while turning off the Connected Experiences settings.*”¹⁰⁶

Controllers are required to implement technical and organisational measures to ensure data protection by design and by default and to meet their duty of accountability.¹⁰⁷ The EDPS has issued guidelines to EU institutions to assist them in doing so.¹⁰⁸

The EDPS welcomes the efforts the ECB has made to minimise the personal data processed in the context of Microsoft’s ‘connected experiences’ offering. The EDPS nevertheless stresses the need for the ECB to be accountable on the necessity of the processing associated with *all* connected experiences it makes use of, not just the optional connected experiences. The EDPS has seen no evidence that the ECB assessed the need of having such functionalities at all, even in the reduced configurations it has decided to deploy.

¹⁰³ See responses to sub-processors’ questionnaire, third sheet (‘Question and answer’), row 24.

¹⁰⁴ See in this regard paragraphs 105 to 108 of the EDPB Recommendations 01/2020.

¹⁰⁵ DPIA report, p. 59.

¹⁰⁶ DPIA report, pp. 47 and 48.

¹⁰⁷ Articles 4(2). 26 and 27 of the Regulation.

¹⁰⁸ EDPS, [Guidelines on the protection of personal data in IT governance and IT management of EU institutions](#); EDPS [Guidelines on the use of cloud computing services by the European institutions and bodies](#).

4.2. Measures to mitigate the high risk of lack of control over Microsoft sub-processors

The ECB has further identified as of probable likelihood and of maximum severity the risk of there being a lack of control over Microsoft sub-processors. The exact risks and impact on individuals is, according to the ECB, threefold: (i) unauthorised access to personal data by third parties with no DPA with the ECB; (ii) location of sub-processors outside the EEA; and (iii) data subjects' personal data might be transferred outside the EEA and not offering an adequate level of protection as required by the Regulation. According to the ECB's analysis, the residual risk after mitigation still remained probable in likelihood and maximum in severity¹⁰⁹.

4.2.1. Information on sub-processors

The EDPS notes that the ECB sent a detailed questionnaire to Microsoft concerning sub-processors and obtained information regarding the 13 sub-processors specifically engaged to deliver Dynamics 365 services.

Microsoft specifies that these sub-processors access customer data for principally two purposes.¹¹⁰ First, when necessary for service operations such as support, troubleshooting, or service maintenance, and only under approval by a member of Microsoft management. Second, it may be accessed for the business operation of compliance with legal obligations.

The information provided by Microsoft suggests that the 13 sub-processors can process a wide range of personal data that could give a detailed picture of an individual. Microsoft's responses suggest that data transferred to processors could include information on the position people external to the ECB hold in an organisation, their speaking engagements, interviews and appointments and the content of their e-mails.¹¹¹

As part of its answers to the ECB sub-processors' questionnaire, Microsoft also provided a table showing the personal data to be processed in the ECB's configuration of Dynamics 365.¹¹² It is not clear how this granular categorisation of the personal data to be processed in Dynamics 365 tallies with the broader and vaguer categories Microsoft identifies as likely to be transferred to non-EEA sub-processors.¹¹³

In the EDPS's view, it is not clear exactly what personal data is likely to be transferred to the 13 sub-processors covered in Microsoft's responses.

¹⁰⁹ Assessment, pp. 23-24, 47-49, and 75-77.

¹¹⁰ See responses to sub-processors' questionnaire, third sheet ('Question and answer'), row 12.

¹¹¹ See responses to sub-processors' questionnaire, first sheet ('Personal data vs subprocessors'), column D.

¹¹² See responses to sub-processors' questionnaire, fourth sheet ('Supplementary clarifications'), Excel table embedded in row 1.

¹¹³ Compare the categories of data set out in (i) the Excel table embedded in row 1 of the fourth sheet ('Supplementary clarifications') of the responses to sub-processors' questionnaire and (ii) column D of the first sheet ('Personal data vs subprocessors') of the responses.

In addition, the documentation received from Microsoft suggests that these are not the only sub-processors potentially engaged through the ECB's use of Dynamics 365. This is because Dynamics 365 is built on Azure cloud services. The answers provided by Microsoft to the ECB's questionnaire suggest that the ECB's use of Dynamics 365 potentially engages all but 8 of the 87 sub-processors listed in the ILA.¹¹⁴ The ECB should satisfy itself that it is in a position to make an informed decision to approve all sub-processors engaged by virtue of its use of Dynamics 365 - not just those specifically involved in the delivery of Dynamics 365 - and any changes to those sub-processors.

The information provided by Microsoft suggests that the sub-processors directly involved in Dynamics 365 service provision are all of 'Type 1', that is to say that they provide contract staff to work alongside Microsoft employees. These contractors typically access ECB data from the EU, US and India.¹¹⁵ Microsoft has advised that it is not currently possible for the ECB to choose not to use sub-processors in India and China. It has, however, advised that contract staff sub-processors based in China only have access to service generated data and diagnostic data.¹¹⁶ It is not clear from the information provided whether any contract staff in China will access ECB data in practice.

Overall, the EDPS considers that the ECB has not yet obtained a complete picture of the sub-processors likely to be involved in delivery of Dynamics 365. The EDPS reminds the ECB that a processor must make available to the controller all information necessary to demonstrate compliance with its obligations set out in Article 29 of the Regulation.¹¹⁷

4.2.2. Prior authorisation of sub-processors - not freely given

The DPIA notes that if the ECB does not approve of a sub-processor, its only contractual recourse is to terminate its subscription to Dynamics 365. It also states that "*it does not seem possible for the ECB to select or to ban any of these subprocessors*".¹¹⁸ The DPIA also states that the ECB considers it "*essential*" to have a market-leading CRM tool in place and has concluded that alternatives to Dynamics 365 pose similar risks for data subjects.¹¹⁹ The ECB's right to withhold prior authorisation of a given sub-processor does not, therefore, appear to be meaningful in practice. This is in breach of Article 29(2) of the Regulation.¹²⁰ The EDPS agrees with the ECB that, given its current circumstances, it poses a high risk.

¹¹⁴ See responses to sub-processors' questionnaire, third sheet ('Question and answer'), row 14, and ECB Scenarios Review, p. 21.

¹¹⁵ See responses to sub-processors' questionnaire, second sheet ('MS Subprocessors List'), rows 8 and 28.

¹¹⁶ See responses to sub-processors' questionnaire, third sheet ('Question and answer'), row 11.

¹¹⁷ The EDPB Guidelines 07/2020 further detail obligations and the sufficient guarantees to be provided by processors. See also [EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA](#), [Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA](#), [EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors](#), and [Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA](#).

¹¹⁸ DPIA report, p. 35.

¹¹⁹ DPIA report, p. 53.

¹²⁰ See pp. 30-31 of March 2020 Investigation Report, section on 'No meaningful controls'. For further clarifications on the obligation of the processor to not engage another processor without prior written

The EDPS understands that Microsoft and the European Commission concluded a revised version of the ILA in May 2021. The EDPS understands that the ECB has seen this amended ILA. If the ECB intends to adhere to it in the future, it should carefully review it to identify whether the contractual issues it has identified have been resolved and voice any remaining concerns pertaining to usage of sub-processors to the Commission so that it properly address them in its negotiations with Microsoft. The EDPS's understanding is that the high risk identified by the ECB in respect of its right of prior authorisation has not been addressed.

The EDPS' ongoing investigation into the European Commission's use of Microsoft Office 365 will cover the contractual controls on sub-processors in the new ILA. The results should be instructive for the ECB.

4.3. Measures to mitigate the high risk of certain limitations of the contract with Microsoft negotiated by the European Commission

Finally, the ECB has identified as of probable likelihood and of maximum severity the risks of (i) lack of contractual obligations of the processor and sub-processors; (ii) non-compliance with the EDPS recommendations as regards institutions' use of Microsoft products and services; (iii) non-compliance with contractual obligations by Microsoft sub-processors; and (iv) lack of safeguards as regards international transfers. The concrete risk and impact on individuals is, according to the ECB, that there is a lack of legal basis for international transfers to the US. The residual risk, in accordance with the ECB's analysis, still remained probable in likelihood and maximum in severity after mitigation¹²¹.

The ECB identifies the ILA's lack of compliance with the EDPS' recommendations on EUIs' use of Microsoft products and services as posing a high risk to data subjects.¹²² As a mitigating measure, the ECB cites the planned signature of a new version of the ILA, which it says "*will cover the Data Protection issues reported by the SCHREMS II judgement.*"¹²³

The EDPS has seen no evidence that the ECB reviewed the draft ILA under negotiation prior to finalising the DPIA. Nor has EDPS seen evidence that the ECB obtained assurances that the new ILA would address issues other than a lack of compliance with the *Schrems II* ruling. The DPIA notes that the Commission is responsible for negotiating contractual amendments with Microsoft, but that "*if any deemed necessary amendments are identified by the ECB, these are communicated to the EC*".¹²⁴ Nothing in the DPIA suggests that the ECB contacted the European Commission to request amendments.

authorisation of the controller see also the EDPB Guidelines 07/2020, [EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA](#) and [EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors](#).

¹²¹ Assessment, p. 25, 49-50, and 78.

¹²² *Ibid.*

¹²³ *Ibid.*

¹²⁴ DPIA report, p. 27.

On the contrary, the DPIA suggests that the ECB took a conscious decision not to review the ILA or engage with the renegotiation process. The DPIA states that: “*At the framework contract level the ECB has no necessity to review any of the terms, as this contract management is not under the ECB's responsibility (acting only as a participating institution).*”¹²⁵

As a consequence, the EDPS does not consider the renegotiation of the ILA between the Commission and Microsoft to be a mitigating measure taken by the ECB. Given the ECB’s professed lack of control over the process, it may be a risk factor.

4.4. Assessment of the alternatives to Microsoft Dynamics 365

The DPIA states that the ECB considered two alternative providers for its CRM system, offered ██████████ but considered that they “*presented similar risks for data subjects as regards use of a cloud solution and transfers to the US*”.¹²⁶

The EDPS understands that the ECB started analysing Microsoft Dynamics 365 and negotiating with Microsoft for its use as the basis of a new CRM of the ECB in 2017. Microsoft Dynamics 365 might have seemed a possible suitable solution at that time. However, in December 2018, the Regulation entered into application, along with obligations on controllers as regards accountability (Articles 4(2) and 26 of the Regulation) and implementing data protection by design and by default (Article 27 of the Regulation). In addition, in March 2020, the EDPS concluded its investigation into the EUIs' use of Microsoft products and services. The *Schrems II* judgement of the Court of Justice followed in July 2020. Consequently, in accordance with Articles 4(2), 26 and 27 of the Regulation, the ECB should have conducted a thorough assessment of the alternatives available to meet its specific needs, together with an assessment of the effectiveness of these alternatives and their level of compliance.

The EDPS has not been provided with evidence that the ECB conducted any detailed assessment of the alternative options available to it in this regard, or that it sent questionnaires on data protection and security to potential providers. This is despite the existence before the completion of the ECB's assessment of a number of elements indicating a meaningful level of risk of non-compliance, such as the outcome of the EDPS investigation mentioned above and the *Schrems II* judgement.

It is the EDPS’s understanding that the ECB intends to make use of only a subset of the functionalities offered by Dynamics 365. We advise that the ECB draw on the experience of other EUIs through inter-institutional governance and cooperation networks to check whether an EU-based provider (or one in a jurisdiction offering an adequate level of protection) would be able to satisfy the ECB’s compliance needs when procuring a system to help manage its relations with external stakeholders¹²⁷.

¹²⁵ *Ibid.*

¹²⁶ DPIA report, p. 53.

¹²⁷ Such as the Interinstitutional Committee for Digital Transformation (ICDT) and the Data Protection Officers Network.

5. WARNING AND CONCLUSIONS

Based on all of the above, the EDPS is of the view that the ECB has correctly identified the high risks related to the adoption of the new CRM solution tool based on Microsoft Dynamics 365. However, the EDPS is concerned that the contractual and other safeguards identified by the ECB may not be sufficient to mitigate the risks identified in the DPIA.

Pursuant to Article 58(2)(a) of the Regulation, the EDPS therefore issues a warning to the ECB that the envisaged processing operation is likely to infringe Articles 29, 46, and 48 of the Regulation. This is in view of the lack of demonstration from the ECB that it has put in place sufficient guarantees and appropriate safeguards that the processing by, and transfers of personal data to Microsoft and its sub-processors in the ECB's use of Microsoft Dynamics 365 will meet the requirements of the Regulation and ensure an essentially equivalent level of protection to that in the EEA. In addition, the ECB did not demonstrate either that it has assessed alternative providers in detail, pursuant to Articles 4(2) and 27 of the Regulation.

As part of its written advice under Article 40(2) of the Regulation, the EDPS makes the following recommendations to ensure compliance of the envisaged processing with the Regulation.

In order for the ECB to ascertain whether the high risks identified in the DPIA can be effectively mitigated, the EDPS expects the ECB to **assess of the new ILA, taking into account the remarks of the EDPS in the present Opinion, to check whether it provides effective contractual safeguards and commitments on technical and organisational measures. The ECB should focus on the following points:**

With regard to sub-processors:

1. whether the terms oblige Microsoft to provide the ECB with complete information regarding all sub-processors involved in the delivery of Dynamics 365 and supporting services;
2. whether the scope of the ECB's prior authorisation for sub-processors and of Microsoft's contractual obligations regarding sub-processors covers all of the data that Microsoft engages sub-processors to process;¹²⁸
3. whether the ECB is effectively able to refuse to authorise a particular sub-processor without suffering any loss of service as a result;¹²⁹

With regard to international transfers to Microsoft or its sub-processors, including by remote access:

¹²⁸ In light of Article 29(1) and (3)(h) of the Regulation. For further information see pp. 30-31 of March 2020 Investigation Report, in particular section on 'Limited scope of Microsoft's obligations' and Recommendation 13.

¹²⁹ This stems from Article 29(2) of the Regulation. See Recommendation 16 of March 2020 findings, p. 32.

4. whether a transfer impact assessment has been carried out by the Commission, where necessary with Microsoft's assistance, to establish the gaps that need to be filled in;
5. whether the ILA provides for effective supplementary measures to fill those gaps following the EDPB Recommendations 01 and 02/2020, to ensure that essentially equivalent level of protection to that in the EU is afforded when the ECB uses Microsoft Dynamics 365 (contractual supplementary measures and commitments to implement identified technical and organisational supplementary measures);
6. whether the new ILA contains binding commitments from Microsoft to notify to the ECB and redirect disclosure requests it or its sub-processors receive and legally challenge disclosure requests invoking privileges and immunities extended to the ECB (see also below);
7. whether the commitments regarding Transparency reports in the ILA ensure provision of information that is as relevant, as clear and as detailed as possible within the limits of the applicable law, with any limitations made clear in reports, and that they are made available to the ECB periodically or every time the ECB requests them;
8. whether the new ILA includes clear obligations and commitments that cryptographic keys are managed and retained solely under the control of the ECB and never stored or shared with Microsoft;
9. whether the new ILA includes clear obligations and commitments that any specific authorisation of access such as that given through use of the Customer Lockbox is based on sufficient information and that the ECB has realistic alternatives to giving approval.

Regarding the impact of Privileges and immunities of the ECB on the overall level of protection of personal data, the ECB should establish without legal ambiguity how and to which extent:

10. the privileges and immunities, as extended to the ECB by the US Executive Order 13307 of May 29, 2003, apply to and are binding upon the public authorities in the US and are not rendered ineffective by the concurrent application of other obligations of US Intelligence Community authorities¹³⁰;
11. the ECB (as owner of the data transferred to and held by Microsoft and its sub-processors on the ECB's behalf) is in a position to effectively defend against disclosure requests¹³¹ not authorised by EU law from third country governments, by relying on its privileges and immunities; and

¹³⁰ As defined by the relevant US legislation, e.g. 50 U.S.C. § 3003(4).

¹³¹ In actions or appeals against such disclosure requests as provided in the third country laws, applicable obligations under international law and principles of international comity.

12. Microsoft and its sub-processors subject to third-country jurisdiction can notify and redirect disclosure requests they receive to the ECB and legally challenge disclosure requests invoking privileges and immunities extended to the ECB.

If the ECB is not satisfied by the result of this assessment, it should:

13. voice any concerns it has to the Commission so that the latter properly addresses them in future negotiations with Microsoft;

With regard to the assessment of alternatives to Microsoft Dynamics 365:

14. In parallel with its assessment of the new ILA, the ECB should conduct a thorough assessment of the alternatives available to meet its specific needs, together with an assessment of the effectiveness of these alternatives and their level of compliance with the Regulation.

Pursuant to Article 59, the EDPS expects the ECB to provide its views and describe the measures it has taken to comply with the Regulation by **15 January 2022**.

6. JUDICIAL REMEDY

Pursuant to Article 64 of the Regulation, any action against this Opinion shall be brought before the Court of Justice of the European Union within two months of its adoption, and according to the conditions laid down in Article 263 TFEU.

Done at Brussels on 7 July 2021

(e-signed)

Wojciech Rafał WIEWIÓROWSKI