

EUROPEAN DATA PROTECTION SUPERVISOR

**EDPS Public Paper on
Outcome of own-initiative
investigation into EU
institutions' use of Microsoft
products and services**



2 July 2020

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 52 of Regulation (EU) 2018/1725 responsible for:

- Monitoring and ensuring the application of the provisions of Regulation (EU) 2018/1725 and any other EU act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a EU institution or body;*
- Advising EU institutions and bodies and data subjects on all matters concerning the processing of personal data.*

To this end, the EDPS fulfils its duties in accordance with Article 57 of Regulation (EU) 2018/1725 and exercises the powers granted in Article 58 of Regulation (EU) 2018/1725.

The power to investigate is one of the tools established to monitor and ensure compliance with Regulation (EU) 2018/1725.

Imprint

Luxembourg: Publications Office of the European Union, 2020

© European Union, 2020

Reproduction is authorised provided the source is acknowledged.

PDF	ISBN 978-92-9242-567-8	data.europa.eu/doi/10.2804/14519	QT-03-20-457-EN-Q
HTML	ISBN 978-92-9242-566-1	data.europa.eu/doi/10.2804/300986	QT-03-20-457-EN-Q
EPUB	ISBN 978-92-9242-565-4	data.europa.eu/doi/10.2804/215182	QT-03-20-457-EN-E

Executive Summary

1 This paper presents the issues raised by the EDPS' own-initiative investigation into European institutions', bodies', offices' and agencies' ('EU institutions') use of Microsoft products and services. These findings and recommendations from the investigation are likely to be of wider interest than just of the EU institutions: they may be of particular interest to all public authorities in EU/EEA Member States.

2 The EDPS assessed the compliance of the licensing agreement between Microsoft and the EU institutions against the requirements laid down in Regulation (EU) 2018/1725^a which sets out the rules for data protection in the EU institutions, bodies, offices and agencies as well as the duties and powers of the European Data Protection Supervisor (EDPS).

3 In the interest of a coherent approach to personal data protection throughout the Union, and the free movement of personal data within the Union, the legislators aligned Regulation (EU) 2018/1725 as far as possible with the data protection rules of Regulation (EU) 2016/679^b ('General Data Protection Regulation' - GDPR). Whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of the GDPR, these two sets of provisions should, under the case law of the Court of Justice of the European Union be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of the GDPR.

4 The EDPS made the following key findings in its investigation into the EU institutions' use of Microsoft products and services.

5 First, the licensing agreement between Microsoft and the EU institutions allowed Microsoft to define and change the parameters of its processing activities carried out on behalf of EU institutions and contractual data protection obligations. The discretion that Microsoft had, amounted to a broad right for Microsoft to act as a controller. Given the EU institutions' role as public service institutions, the EDPS did not consider this appropriate. The EDPS recommended to EU institutions that they act to retain controllership.

6 Second, EU institutions needed to put in place a comprehensive and compliant controller-processor agreement and documented instructions of the EU institutions to the processors. Their lack of control over which sub-processors Microsoft used and lack of meaningful audit rights also presented significant issues. The EDPS made recommendations on how to improve the controller-processor agreement and put robust audit checks in place.

7 Third, EU institutions faced a number of linked issues concerning data location, international transfers and the risk of unlawful disclosure of data. They were unable to control the location of a large portion of the data processed by Microsoft. Nor did they properly control what was transferred out of the EU/EEA and how. There was also a lack of proper safeguards to protect data that left the EU/EEA. EU institutions also had few guarantees at their disposal to defend their privileges and immunities and ensure that Microsoft would only disclose personal data insofar as permitted by EU law. The EDPS made recommendations to assist EU institutions in addressing these issues.

8 Fourth, the EDPS considered the technical measures that the Commission had put in place to stem the flow of personal data generated by Microsoft products and services and sent to Microsoft. The EDPS recommended that all EU institutions perform tests using a revised and comprehensive approach, share among them the knowledge and technical solutions they developed to prevent unauthorised data flows to Microsoft and inform each other of any data protection issues they identify with the products or services.

9 Fifth, the EU institutions had insufficient clarity as to the nature, scope and purposes of the processing and the risks to data subjects to be able to meet their transparency obligations towards data subjects. The EDPS recommended that EU institutions seek the clarity and assurances allowing them to keep data subjects properly informed.

^aRegulation (EU) 2018/1725 of the European Parliament and of 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 [2018] OJ L295/60 (<https://eur-lex.europa.eu/eli/reg/2018/1725/oj>).

^bRegulation (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) [2016] OJ L119/1 (<http://data.europa.eu/eli/reg/2016/679/oj/eng>) accessed 7 January 2018.

Contents

1	Introduction	6
1.1	Context	6
1.2	General recommendations	7
1.3	The Inter-Institutional Licence Agreement (ILA)	7
2	Microsoft as controller	8
2.1	Right of unilateral amendment	8
2.2	Limited data protection obligations	9
2.3	Insufficient purpose limitation	11
2.4	Consequences	12
2.5	Recommendations	13
3	The controller-processor agreement	14
3.1	Comprehensiveness of the agreement	14
3.1.1	Assessment	14
3.1.2	Recommendations	15
3.2	Sub-processors	15
3.2.1	Assessment	15
3.2.2	Recommendations	17
3.3	Audit rights	17
3.3.1	Assessment	17
3.3.2	Recommendations	19
4	Data location, transfers and disclosure	20
4.1	Data location	20
4.2	International transfers	21
4.3	Unauthorised disclosure	23
4.4	Consequences	25
4.5	Recommendations	26
5	Technical measures	27
5.1	Context	27
5.2	Recommendations	27
6	Transparency	28
6.1	Recommendations	28
7	Conclusion	29

1 Introduction

1.1 Context

- 10 This paper presents the issues raised by the EDPS' own-initiative investigation into European institutions', bodies', offices' and agencies' ('EU institutions') use of Microsoft products and services. It presents the EDPS' findings and recommendations from the investigation to be shared with a wider audience, applying a high standard of transparency¹, while preserving the necessary confidentiality of certain elements of the EU institutions' contract and of the EDPS' investigation.
- 11 A large amount of personal data is processed through the EU institutions' use of Microsoft products and services. Over 45 000 staff of EU institutions, including the EDPS, are users of those products and services. In addition, staff use Microsoft products and services to process the personal data of people who are not staff.
- 12 The EDPS' investigation focused on the terms of the *Inter-Institutional Licensing Agreement* ('ILA') that EU institutions signed with Microsoft in 2018. The EDPS also considered the technical measures that the European Commission, as the largest EU institution with a great variety of tasks, had implemented affecting the flow of personal data to Microsoft.
- 13 The EDPS issued its findings and recommendations to the EU institutions upon the closure of its investigation in March 2020. The purpose of the EDPS' report was to provide EU institutions with forward-looking assistance in bringing their arrangements into compliance with data protection law. In particular, the EDPS' findings and recommendations were oriented towards supporting the renegotiation of the ILA and EU institutions' contract and implementation of robust technical and organisational measures that should accompany the contract.
- 14 EU institutions' processing of personal data and the EDPS' own supervisory and investigative powers are governed by Regulation (EU) 2018/1725.² The EDPS assessed the compliance of the ILA against the requirements laid down in that regulation. Although Regulation (EU) 2018/1725 is a data protection regime that is tailored to the EU institutions and distinct from the better-known General Data Protection Regulation³ ('GDPR'), the overlap between the provisions of Regulation (EU) 2018/1725 and those of the GDPR is extensive.
- 15 As a consequence, the EDPS' findings and recommendations are likely to be of wider interest than to EU institutions.⁴ Not only is the law the EDPS applied in its investigation based on the same principles and shares the vast majority of provisions with the GDPR, but the agreement signed by

¹The EDPS follows this high standard of transparency with a view to raising awareness on data protection issues more widely, promoting a common understanding of data protection rules and development of data protection culture across the EU/EEA. A high standard of transparency is also generally recommended by the European Ombudsman for the EU institutions in proactive implementation of Regulation (EC) No 1049/2001 and accountability of EU decision-making.

²Regulation 2018/1725 (n *a*).

³GDPR (n *b*).

⁴The EDPS role and competences concern only compliance with Regulation (EU) 2018/01725, not with the GDPR. To help the readers, when this paper makes reference to specific provisions of Regulation (EU) 2018/01725, references to the corresponding provisions of the GDPR have been added.

EU institutions is based on standard Microsoft volume-licensing documents and therefore likely to bear similarities to agreements concluded by other organisations. The EDPS' findings and recommendations may be of particular interest to public authorities in EU member states.

- 16 They are also likely to be of relevance beyond the conclusion and implementation of volume licensing agreements for Microsoft products and services. In the EDPS' view, organisations outsourcing provision or operation of digital services from other service providers are likely to come across similar issues.

1.2 General recommendations

- 17 The EDPS recommended that EU institutions carefully consider any purchases of Microsoft products and services or new uses of existing products and services until after they have analysed and implemented the recommendations of the EDPS. They should involve their Data Protection Officers when deciding how to implement the recommendations of the EDPS. The EU institutions should properly embed data protection in each specific public information and communications technology procurement procedure, specifying the security and data protection measures to be implemented in respect of the particular products and services that are being procured.
- 18 This will help EU institutions, from the start, to procure products and services with appropriate contractual and other organisational measures, technical and security measures so that the processing of personal data through those tools complies with Regulation (EU) 2018/1725, in particular with the principle of data protection by design and by default.⁵

1.3 The Inter-Institutional Licence Agreement (ILA)

- 19 The ILA that the EDPS examined had a complex structure with a multiplicity of interlocking documents supplementing and modifying each other in various ways.
- 20 Broadly, however, the ILA had three main components. The first was an umbrella licence agreement, which was based on a number of standard-form volume licensing documents to which EU institutions negotiated a set of bespoke amendments with Microsoft. The second component comprised several sets of standard Microsoft terms, which were incorporated into the umbrella agreement by reference. In the context of the EDPS' investigation, the most important sets of standard terms were the *Product Terms* and the *Online Services Terms*. The third component comprised the documents by which individual EU institutions adhered to the licensing agreement and subscribed to a package of Microsoft products and services that best suited their needs.
- 21 The terms of the ILA were not fixed. The sets of standard Microsoft terms that were incorporated by the umbrella agreement are regularly changed by Microsoft, with new versions published on its volume licensing website.⁶ For example, Microsoft publishes a new version of the Online Services Terms monthly.

⁵Regulation 2018/1725 (n *a*) recital 48 and art 25.

⁶'Licensing Terms and Documentation' (*Microsoft Volume Licensing*) (<https://aka.ms/licensingdocs>) accessed 19 June 2020.

- 22 Determining what parts of what version of a standard document applied to what aspects of a given Microsoft product or service could be a complex affair. To take the Online Services Terms again as an example, the applicable version of this document varied in respect of each online service, depending on which date the customer concerned first purchased or renewed a subscription to that service.⁷ However, terms introduced in later versions of the Online Services Terms could also apply to new features and supplements of related software not previously included in the subscription.⁸
- 23 In the context of the EDPS' investigation, the latest versions of standard documents that the EDPS analysed were those from January 2020.⁹ For the purposes of this paper, the EDPS only refers to those versions. However, in the investigation, the EDPS also analysed a number of prior versions¹⁰, which were often drafted in similar terms and presented similar or greater compliance issues. Overall, the statements the EDPS makes about the ILA, the non-contractual documents and the factual context represent the position until March 2020.

2 Microsoft as controller

- 24 In the EDPS' view, the scope and terms of the ILA resulted in Microsoft acting as a controller in ways that were not transparent. This was due to a combination of several aspects of the ILA. The EDPS considers three key issues in this regard:
1. Microsoft's right of unilateral amendment,
 2. the limited scope of the data protection obligations in the ILA, and
 3. the lack of specific and explicitly defined purposes for the processing that occurred under it.

2.1 Right of unilateral amendment

- 25 The ILA allowed Microsoft to amend data protection terms unilaterally. There were two aspects to this right.
- 26 First, the ILA granted Microsoft an unlimited right to modify all the sets of standard terms that were incorporated into it by reference.
- 27 It was possible for Microsoft to make far-reaching changes to the data protection terms of the ILA by changing a set of standard terms incorporated into it. This was because the standard terms filled in many gaps in the negotiated umbrella agreements, such that it was often necessary to refer to them to understand how terms in the umbrella agreements would be implemented.

⁷Microsoft, 'Introduction' in *Online Services Terms (OST)* (<https://aka.ms/ost>), s 'Applicable Online Services Terms and Updates'; Microsoft, 'Introduction' in *Data Protection Addendum (DPA)* (<https://aka.ms/dpa>), s 'Applicable DPA and Updates'.

⁸*ibid.*

⁹At the time of the writing of the present paper (May 2020), the latest version of the *Data Protection Addendum* was that of January 2020.

¹⁰The versions both before and after January 2020 may be relevant to the EU institutions.

- 28 Changes made by Microsoft in January 2020 illustrate just how far-reaching such unilateral amendments could be. Microsoft moved a number of important data protection terms out of the Online Services Terms and into a new standard document, called the *Data Protection Addendum*. The content of those data protection terms also underwent substantial revision.
- 29 As a result of this change, it became unclear whether a significant corpus of data protection terms had ceased to apply to the EU institutions' use of Microsoft products and services. Since the Data Protection Addendum did not exist at the time when the ILA was signed in 2018, only the Online Services Terms were incorporated by reference into the ILA, but not the newly separated Data Protection Addendum. Nor, at the time the EDPS concluded its investigation, was there any express contractual link between the Data Protection Addendum and the ILA, such as a statement in the Online Services Terms that the Data Protection Addendum formed part of the Online Services Terms. For the purposes of the EDPS' own-initiative investigation, the EDPS assumed that the Data Protection Addendum did apply in the context of the ILA.
- 30 The second aspect of Microsoft's right of unilateral amendment concerned the order of precedence of the various contractual documents. The ILA contained a number of provisions affecting which documents prevailed over which. Some of those provisions were in direct conflict with each other, leading us to conclude that the precise order of precedence was ambiguous. Nevertheless, there remained in the EDPS' view a high risk that standard documents such as the Online Services Terms, Product Terms and potentially the Data Protection Addendum prevailed over the negotiated terms of the umbrella agreement. Given Microsoft's right to change those standard documents at any time, this amounted to a high risk that Microsoft could amend the whole contractual suite of the ILA unilaterally, including any controller-processor agreement between the parties.
- 31 Overall, the EDPS considered that there was a high risk that Microsoft could change, for example, the purposes for which it processed personal data, the location of data and the rules governing disclosure and transfer of data, without EU institutions having any contractual recourse against the changes. The discretion whether to make such changes rested with Microsoft.
- 32 This level of discretion goes beyond what can be assigned to a processor; it effectively made Microsoft a controller.¹¹

2.2 Limited data protection obligations

- 33 The scope of Microsoft's principal data protection obligations in the negotiated ILA documents was limited to specific types of processing and categories of data. There was a risk that certain data-processing activities under the ILA fell outside of the scope of the negotiated terms and benefited from a lower level of protection determined solely by Microsoft. Some categories of data gathered and used by Microsoft as a consequence of the EU institutions' use of its products and services fell outside of the scope of contractual protections altogether.
- 34 The EDPS' analysis suggested that broadly four categories of personal data were granted different levels of protection under the ILA. The first, most protected, category of personal data was data *provided* through the use of so-called *online services*. The online services were in essence the Microsoft-hosted services provided under the ILA, and included the online component of Microsoft

¹¹Regulation 2018/1725 (n *a*) art 29(10); GDPR (n *b*) art 28(10).

software products. Data falling within this category fell within the scope of the principal negotiated data protection obligations in the ILA and of the Data Protection Addendum.

- 35 A second category included data that were not *provided* to Microsoft but *gathered* by Microsoft when EU institutions used the online services. Processing of this data was partly covered by the Online Services Terms (and potentially, since its creation, by the Data Protection Addendum) and not by the main negotiated obligations of the umbrella agreement.
- 36 A third category of data was data that Microsoft obtained when EU institutions used its so-called *professional services*. This was covered by a separate and lighter set of data protection terms annexed to the Data Protection Addendum. It also fell out of the scope of the main negotiated obligations of the umbrella agreement.
- 37 Microsoft processed data in the first three categories not only as a processor but also as a controller.¹² When it acted as a controller, the Microsoft Privacy Statement applied in addition to contractual documents.
- 38 A fourth category of data existed. These data were both *provided* to and *gathered* by Microsoft when EU institutions used products and software that Microsoft did *not* consider to be online services. Processing of data in this category fell outside of the scope of any meaningful contractual controls. They were processed by Microsoft as a controller and covered by the Microsoft Privacy Statement. Diagnostic data from all versions of Windows and from the Office productivity suite (including the version *Office 2016*) fell into this category. Diagnostic data from locally installed *Office 365 ProPlus* productivity suite applications (e.g. Word, Excel, PowerPoint) which were not online services also potentially fell into this category.
- 39 Overall, there was a lack of transparency concerning which contractual controls, if any, applied to the different categories of data processed by Microsoft under the ILA. The EDPS was unable to delineate the different categories precisely on the basis of the contractual documents.
- 40 Given the inter-connected nature of Microsoft products, online services and professional services, it was also unclear whether it was possible for data falling within the most protected category to move into a less-protected category, or vice versa.
- 41 In the EDPS' view, EU institutions had few or no contractual controls over what personal data was collected by Microsoft from users or what Microsoft could do with those data unless the data had been provided via online services and were certain to remain within that category. As outlined in the previous section, Microsoft also retained the right to amend many, or potentially all, of the controls unilaterally. Microsoft therefore retained broad discretion in this regard.
- 42 When the scope of a processor's data protection obligations is unclear, this can create a risk that the processor will decide to act as a controller in respect of part of all of the data it processes as a result of the business relationship. In the case of the ILA, the lack of clarity surrounding the scope of Microsoft's data protection obligations led us to find a high risk that it could act as a controller in respect of all data processed under the ILA.

¹²Microsoft, 'Data Protection Terms' in *Data Protection Addendum (DPA)* (<https://aka.ms/dpa>), ss 'Processor and Controller Roles and Responsibilities'; Microsoft, 'Attachment 1' in *Data Protection Addendum (DPA)* (<https://aka.ms/dpa>), ss 'Processor and Controller Roles and Responsibilities'.

2.3 Insufficient purpose limitation

- 43 In the EDPS' view, the purpose limitation in the ILA was insufficiently specific and explicit. This created a risk of mismatch between the purpose limitation that EU institutions believed they had imposed on Microsoft under the ILA and the processing that Microsoft considered to be permitted under such agreement.
- 44 The most explicit statement of purpose in the ILA documents for Microsoft's activities as a processor was 'to provide the Product or Professional Services'. The range of processing operations this could encompass was potentially vast.
- 45 In the context of a detailed and complex agreement between sophisticated operators affecting a large number of data subjects, such as the ILA, it is appropriate that specification of permitted purposes for processing leave little doubt as to what is and is not included within the purpose.¹³ The description should also be comprehensive, enabling the customer and supervisory authorities to understand the risks of the processing, and to enable explanation of those risks to data subjects. In the EDPS's view, the statement of purpose in the ILA left far too much room for interpretation.
- 46 The Data Protection Addendum went some way to clarifying what might and might not fall within 'provision' of a service. It defined what it meant to 'provide' an online or professional service, created a list of purposes that were prohibited unless the customer instructed otherwise and explicitly recognised a set of purposes when Microsoft intended to act as a controller. Its publication in January 2020 represented a significant shift towards greater transparency in the contractual documentation of Microsoft's processing operations, and was therefore welcome.
- 47 It was not the whole answer though: as explained, a large amount of processing was not covered by it. It was also unclear whether it applied in the context of the ILA or not.
- 48 In addition, a number of difficulties remained with the clarity of the purpose limitation. For example, the Data Protection Addendum included 'providing personalized user experiences' within the definition of what it meant to 'provide' an online service.¹⁴ This directly conflicted with the default prohibition on 'user profiling',¹⁵ raising a question as to how narrowly Microsoft interprets 'user profiling'.
- 49 'Providing an online service' was also defined in vague enough terms to leave the following questions unanswered.¹⁶ First, the definition was broad enough to include data analytics. As a result it was unclear whether processing for purposes such as training machine learning or artificial intelligence systems was permitted. Second, it was unclear whether providing a particular online or professional service only included 'troubleshooting', 'delivering functional capabilities' and 'ongoing improvement' in respect of that service or also in respect of other or all online or professional services respectively. Third, 'ongoing improvement' of a service was described as

¹³Article 29 Working Party, *Opinion 03/2013 on Purpose Limitation* (2012) (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf) pp 15-16; European Data Protection Board, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* (2019) (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf) pp 6-7.

¹⁴Microsoft, 'DPA Data Protection Terms' (n 12) ss 'Processing to Provide Customer the Online Services'.

¹⁵*ibid.*

¹⁶*ibid.*

including ‘making improvements to user productivity’ and to user ‘efficacy’. It was unclear what productivity and efficacy included.

- 50 A further example of vagueness in the purpose limitation, in the Data Protection Addendum, was the default prohibition it imposed on processing ‘for any advertising or similar commercial purposes.’¹⁷ These terms were not explained. This was significant, as Microsoft had indicated in 2018 that it did not consider serving targeted in-application recommendations to customers for products they do not use or subscribe to as falling within advertising or a similar commercial purpose.¹⁸ If Microsoft still holds such interpretation, it might deem such processing to fall within the permitted purpose.
- 51 The Data Protection Addendum also granted Microsoft the right to act as a controller in respect of its ‘legitimate business operations’, which were defined to cover six purposes.¹⁹ The stated nature of the six purposes suggested a significant overlap with what might under the GDPR qualify as legitimate interests pursued by the controller. It was unclear from the broad and vague language, to what extent those purposes were necessary for the provision of the online and professional services. At the very least, it was questionable why personal data from EU institutions might be necessary to decide on bonuses for Microsoft staff. As explained in the following sub-section, the EDPS did not consider processing by Microsoft as a controller, particularly for its own legitimate interests, appropriate in the context of the EU institutions’ use of Microsoft’s products and services under the ILA.

2.4 Consequences

- 52 In the EDPS’ view, one of the most concerning aspects of the ILA lay in the fact that the level of discretion accorded to Microsoft was largely implicit: the EDPS’ analysis was largely based on identifying gaps in the contractual drafting and drawing out the consequences of leaving gaps or uncertainties in the particular context.
- 53 The EDPS reached its conclusion that the ILA granted Microsoft far-reaching rights of unilateral amendment despite express provision to the contrary in the negotiated documents. The EDPS’ analysis of the discretion granted to Microsoft by limitations on the scope of certain contractual terms rested on identifying what types of processing might *not* be covered, either wholly or partly.
- 54 The EDPS’ concerns with respect to the purpose limitations in the ILA were driven by the understanding that if a contractor is instructed by a controller to process data for vaguely defined purposes, this creates a risk that the contractor will to a greater or lesser extent define those purposes for itself.

¹⁷ *ibid.*

¹⁸ Privacy Company, *DPIA Diagnostic Data in Microsoft Office ProPlus* (techspace rep, Ministry of Justice and Security for the benefit of SLM Rijk (Strategic Vendor Management Microsoft Dutch Government) 2018) (<https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365++20191105.pdf>) 37.

¹⁹ Microsoft, ‘DPA Data Protection Terms’ (n 12) ss ‘Processing for Microsoft’s Legitimate Business Operations’.

- 55 Implied discretion of ambiguous scope and vaguely defined purposes effectively grant a processor licence to act as a controller in ways that may remain entirely hidden to an organisation that procures its services.
- 56 In a contract involving large-scale or other high-risk processing, this exposes data subjects significantly. It could lead to a large amount of personal data being processed in ways determined by the contractor, rather than by the procuring organisation's instructions. To the extent that the contractor acts as a controller, the procuring organisation's ability to hold the contractor to account for its processing activities will be very limited.
- 57 If a public organisation procures services from a contractor and grants it the discretion to act as a controller under the GDPR, this creates an additional risk that is particular to that organisation's public-interest mandate. Under the GDPR, processing may be carried out lawfully in pursuit of a controller's legitimate interests. As explained, the Data Protection Addendum allows Microsoft to carry out processing as a controller which would appear to fall within this ground. However, the GDPR does not permit processing on grounds of a controller's legitimate interests to be carried out by public authorities in the performance of their tasks. Nor are there any legitimate interests grounds for processing by EU institutions under Regulation (EU) 2018/1725. **Recital 25 and Article 6 of Regulation (EU) 2018/1725** [see also recital 50 and Article 6(4) of the GDPR] suggest that when EU institutions use IT products and services to carry out tasks in the public interest entrusted to them by EU law, any processing for other tasks and purposes should be compatible with the tasks and roles of the EU institutions. When EU institutions act as controllers, they must ascertain whether the purposes for which other or further processing is undertaken is compatible under **Article 6 of Regulation (EU) 2018/1725** [see also Article 6(4) of the GDPR].
- 58 Public authorities may wish to consider whether, in light of the tasks they carry out in the public interest, they consider it appropriate that a contractor becomes a controller—even a joint controller—of staff's and citizens' personal data simply by virtue of the authority's need to outsource IT to carry out its tasks. In its investigation, the EDPS found a risk that protections designed for the public interest context in which personal data was entrusted to EU institutions would be circumvented by means of the outsourcing process.

2.5 Recommendations

- 59 In the EDPS' view, the risks associated with Microsoft exercising controllership outweighed the benefits that any such an arrangement could offer EU institutions. The course of action the EDPS recommended to EU institutions included the following.

Recommendation Set 1: act as sole controller

- Each EU institution should act as sole controller in respect of its use of Microsoft products and services when performing tasks in the public interest or in the exercise of official authority.
- The umbrella licence agreement should provide for an unambiguous order of precedence of the contractual documents.

- The amendments that EU institutions negotiated to Microsoft’s standard terms should be included in the highest-ranking contractual document. So should all the provisions necessary to comply with Regulation (EU) 2018/1725.
- It should only be possible to change provisions in the ILA affecting data protection by common agreement.
- The scope of provisions in the ILA affecting data protection should be broadened to cover all personal data not only provided to Microsoft but also generated by Microsoft, as a consequence of the EU institutions’ use of all Microsoft products and services.
- EU institutions should negotiate a specific, explicit and exhaustive set of purposes to cover all types of personal data involved in their use of Microsoft products and services. The purposes should be limited to those that were necessary for EU institutions to use those products and services. Other purposes should be expressly prohibited.

3 The controller-processor agreement

3.1 Comprehensiveness of the agreement

3.1.1 Assessment

- 60 In the EDPS’ view, if EU institutions were to remain the only controllers of personal data processed under the ILA, their controller-processor agreement with Microsoft needed to be substantially reinforced. Many of the necessary elements were either inadequately implemented or absent.
- 61 The requirements for a compliant controller-processor agreement are set out in **Article 29 of Regulation (EU) 2018/1725** [*see also Article 28 of the GDPR*]. They permeate the whole of this paper. Article 29(3) of Regulation (EU) 2018/1725 requires the controller-processor agreement to be ‘binding on the processor with regard to the controller’.²⁰ There is therefore no place for a processor to have an unlimited right of unilateral amendment in a controller-processor agreement. A processor should only process on the basis of documented instructions from the controller.
- 62 Article 29(3) of Regulation (EU) 2018/1725 requires the controller-processor agreement to set out ‘the type of personal data and categories of data subjects and the obligations and rights of the controller’.²¹ The EDPS’ analysis had concluded that it was unclear which contractual controls, if any, applied to the different categories of data processed by Microsoft under the ILA. As the EDPS has seen, although Microsoft had obligations and rights attributable to a controller under the ILA, they were generally not expressly stated. Following that, EU institutions’ obligations and rights as controllers were not fully set out. There was no mention in the negotiated ILA documents of categories of data subjects, although they were mentioned in the Data Protection Addendum.

²⁰GDPR (n *b*) art 28(3).

²¹ibid art 28(3).

- 63 Article 29(3) of Regulation (EU) 2018/1725 also requires the controller-processor agreement to set out ‘the subject-matter [...], the nature and purpose of the processing’.²² The EDPS’ analysis of the contractual purpose limitation showed that this was done with insufficient precision.
- 64 In this section, the EDPS focuses on two further key failures to comply with Article 29 of Regulation (EU) 2018/1725: first, the lack of control accorded to EU institutions over Microsoft’s use of sub-processors; and second, the absence of effective audit rights accorded to EU institutions.

3.1.2 Recommendations

- 65 The EDPS recommended that EU institutions take the following actions.

Recommendation Set 2: have a comprehensive controller-processor agreement

- Draw up a comprehensive controller-processor agreement that includes the roles and responsibilities of the processor and the controller, the subject matter, duration, and nature of the processing, the types of personal data concerned, the categories of data subjects concerned, obligations and rights of controllers and processors.
- The types of personal data and categories of data subjects should be specified in as much detail as possible to ensure compliance with basic principles, such as data minimisation, purpose limitations and lawfulness of processing.
- EU institutions’ documented instructions under the ILA should cover for example which types of data may be processed, who may access the data, how and where it is stored, what security measures are in place, whether transfers to third countries are allowed and if yes to which recipients, countries and under what conditions. Instructions should be included in the contract and in respect of further instructions, the necessary templates and procedures should be agreed and annexed to the contract.

3.2 Sub-processors

3.2.1 Assessment

- 66 Controllers are required to allow processing on their behalf only by processors providing sufficient guarantees that they will take measures to protect data subjects.²³ As a processor, Microsoft is only permitted to engage a sub-processor on the basis of a prior written authorisation from the controller.²⁴ If it does so on the basis of a general written authorisation, it must give the controller a meaningful opportunity to approve a list of sub-processors at the time the general authorisation

²²GDPR (n *b*) art 28(3).

²³Regulation 2018/1725 (n *a*) art 29(1); GDPR (n *b*) art 28(1).

²⁴Regulation 2018/1725 (n *a*) art 29(2); GDPR (n *b*) art 28(2).

is signed, and a meaningful opportunity to object to any subsequent changes in the sub-processors it engages.²⁵

- 67 As a processor, Microsoft must also pass its data protection obligations under the licensing agreement on to its sub-processors contractually.²⁶ Among the obligations to be passed on are Microsoft's commitments to implement the technical and organisational measures the controller considers necessary.²⁷ In light of controllers' duty of accountability,²⁸ they should be able to demonstrate that it has done so.
- 68 The intention behind the provisions of Regulation (EU) 2018/1725 (and GDPR) on sub-processors is to put controllers in control, so that they can live up to their obligations to protect data subjects. In the EDPS' view, the ILA did not allow EU institutions to exercise control over the sub-processors that Microsoft engages. It therefore posed a risk to data subjects.
- 69 The lack of control that EU institutions had was apparent from the following three elements.
- 70 First, the negotiated data protection terms of the umbrella agreement contained what appeared to be a general authorisation to engage sub-processors. However, like many of the data protection obligations under the ILA, it only applied to personal data *provided* through use of the *online services*. The EDPS saw no authorisations in place covering the other categories of data processed by Microsoft, by virtue of the ILA.
- 71 Second, the EDPS' understanding was that in practice, the information provided to EU institutions on new sub-processors consisted of the name of the sub-processor, the general type of service it provided and the country of its corporate location.²⁹ The EDPS did not consider this information sufficient. In the EDPS' view, for a system of general authorisation to provide EU institutions with a meaningful opportunity to object to new sub-processors, EU institutions would also need to know what types of processing prospective sub-processors were to be entrusted with, in relation to which specific products and services, and with which data protection safeguards and security measures in place. Without this information, EU institutions could not show why they were right to approve to the sub-processors in question, and so could not be accountable for their decision.
- 72 Third, if EU institutions did not approve of a new sub-processor, their only recourse under the negotiated terms of the ILA was to terminate their subscription to the affected online service. If the affected online service was part of a suite, the EU institutions' only recourse was to terminate their subscription for the entire suite.
- 73 This contractual remedy risked being meaningless in practice. In the EDPS's view, there was a risk that EU institutions would find themselves with no realistic alternative to using an affected Microsoft service or suite if they disapproved of a new sub-processor. In such circumstances, they would effectively have no say over the choice of sub-processor.

²⁵Regulation 2018/1725 (n *a*) art 29(2); GDPR (n *b*) art 28(2); also relevant in this context is European Data Protection Board, *Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)* (2019) (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf) para 29.

²⁶Regulation 2018/1725 (n *a*) art 29(4); GDPR (n *b*) art 28(4).

²⁷Regulation 2018/1725 (n *a*) art 29(4); GDPR (n *b*) art 28(4).

²⁸Regulation 2018/1725 (n *a*) art 26; GDPR (n *b*) art 24.

²⁹The EDPS' understanding is based on the information available on: 'Trust Center' (Microsoft) (<https://www.microsoft.com/en-ww/trust-center>).

- 74 In the EDPS's view, it was essential that EU institutions should be in a position to withhold approval of a certain sub-processor if they had grounds to believe that it posed a risk to compliance. This could be the case if, for example, audits revealed compliance concerns in respect of that sub-processor.
- 75 Indeed, it is likely that any controller outsourcing large-scale or other high-risk processing will need to be able to give meaningful approval of sub-processors used by the contractor if that controller is to meet its own compliance obligations.

3.2.2 Recommendations

- 76 The EDPS recommended that EU institutions take the following actions.

Recommendation Set 3: control use of sub-processors

- Assess the risks posed to data subjects by sub-processors currently used by Microsoft.
- Ensure that the use of sub-processors in respect of all personal data processed by Microsoft by virtue of the ILA (and any changes of sub-processor) were subject to a prior written authorisation.
- Introduce in the ILA an obligation on Microsoft to provide complete information first, on which sub-processors were used in respect of each product or service provided to EU institutions and in respect of each processing activity and category of personal data; and second, on the data protection safeguards and security measures (i.e. technical and organisational measures) in place in respect of each sub-processor. This should include an obligation on Microsoft to provide on request the relevant parts of its contract with a particular sub-processor.
- Introduce guarantees in the ILA to ensure that prior authorisation is freely given in respect of each sub-processor engaged by Microsoft. EU institutions should be able to refuse to authorise a particular sub-processor without suffering any loss of service as a result.

3.3 Audit rights

3.3.1 Assessment

- 77 Under **Article 29(3)(h) of Regulation (EU) 2018/1725** [*see also Article 28(3)(h) of the GDPR*], a controller-processor agreement must contain two obligations on the processor. First, the processor must make available to the controller all the information that is needed to demonstrate compliance with the whole of Article 29 of Regulation (EU) 2018/1725. Second, the processor must submit to audits and inspections from the controller. These obligations are cumulative: by implication, the processor must comply with any reasonable request falling within either obligation. They must also be passed on contractually to any sub-processors.³⁰

³⁰Regulation 2018/1725 (n *a*) art 29(4); GDPR (n *b*) art 28(4).

- 78 In light of the controller’s duty of accountability under **Article 26 of Regulation (EU) 2018/1725** [see also *Article 24 of the GDPR*], the detail and reach of the audit rights in the contract should reflect the ‘nature, scope, context and purposes of processing as well as the risks [...] for the rights and freedoms of natural persons’. Given the large amount of data processed by virtue of the EU institutions’ use of Microsoft products and services, the large number of data subjects involved and the lack of clarity surrounding exactly what was processed, where, how and for what purposes, the circumstances in which the EDPS carried out its investigation called for EU institutions to implement robust, effective audit provisions. The provisions needed to act as a clear, binding and detailed set of instructions from EU institutions to Microsoft as regards the conduct of audits.
- 79 Under the second subparagraph of Article 29(3) of Regulation (EU) 2018/1725, an additional obligation on the processor is to inform the controller immediately if it considers an instruction breaches the Regulation or EU or Member State data protection law.³¹ In light of the processor’s own compliance obligations, this amounts to an obligation on the processor to be proactive in informing the controller if it identifies a compliance issue with any instructions it receives from the controller.
- 80 The negotiated terms of the ILA reproduced the wording of the statutory obligations under Article 29(3) of Regulation (EU) 2018/1725 just cited.³² They provided no details of what EU institutions could expect from Microsoft to fulfil them.
- 81 Some further details were provided in the Data Protection Addendum. The EDPS learned that Microsoft would arrange for so-called *security audits* to be performed at least yearly by external *security auditors* selected and paid by Microsoft.
- 82 The texts did not explain the extent to which such security audits would cover data protection compliance. This was a significant omission: it is possible to perform highly in a security audit while failing a data protection audit because of a lack of transparency, unlawful further processing or other data protection issues.
- 83 Nor did they confirm whether the security audits would cover all processing activities falling within the scope of the Online Services Terms or only some, or also cover processing outside of the scope of the Online Services Terms. They did not explain whether sub-processors were covered. Professional Services Data appeared to be excluded from the scope of the security audits,³³ together with a number of Online Services.³⁴
- 84 Read as a whole, the audit provisions in the Data Protection Addendum also suggested that Microsoft’s own security audits were the baseline for achieving ‘auditing compliance’.³⁵
- 85 In the EDPS’s view, this was an incorrect assumption to make. Data protection audits, which assess compliance with the obligations imposed by Regulation (EU) 2018/1725, are of a wider

³¹See also GDPR (n *b*) art 28(3) subpara 2.

³²see also *ibid* art 28(3).

³³See the section on ‘Scope’ of the *Data Protection Addendum*, which excludes the Online Services mentioned in Attachment 1 of the *Data Protection Addendum* (namely Professional Services) from the scope of the *Data Protection Addendum*. See also the ‘Scope’ sub-section of the ‘Data Protection Terms’ section in 2019 versions of the Online Services Terms.

³⁴See ‘Attachment 1’ in the *Online Services Terms*. See also the ‘Scope’ sub-section of the ‘Data Protection Terms’ section in 2019 versions of the *Online Services Terms*.

³⁵See Microsoft, ‘DPA Data Protection Terms’ (n 12) ss ‘Auditing Compliance’, read as a whole.

scope and apply different standards to security audits. Moreover, audits mandated by Microsoft *itself* with a (limited) scope of *its* choosing could never amount to the effective audit rights for controllers envisaged by Regulation (EU) 2018/1725. This is because Article 29(3)(h) of Regulation (EU) 2018/1725 requires a contractual obligation on Microsoft to allow for audits ‘conducted by the controller’ or ‘mandated by the controller’.³⁶

- 86 The Data Protection Addendum contained a commitment from Microsoft to ‘promptly respond’ to any additional audit instructions, ‘[t]o the extent Customer’s audit requirements [...] cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers’.³⁷
- 87 The EDPS recognised two issues with this drafting. First, information provided by Microsoft and auditors instructed by Microsoft might provide EU institutions with some level of assurance. But it could not replace EU institutions’ ability to gather and check the evidence for Microsoft’s statements themselves. Information from Microsoft and its auditors were not therefore a means by which EU institutions’ own audit requirements could be ‘reasonably satisfied’. They were instead a means by which EU institutions could identify the areas on which to focus their checks.
- 88 Second, it was not enough for Microsoft to ‘respond’ promptly to EU institutions’ audit instructions. A response could be a refusal to allow an audit by EU institutions that overlapped with its own audits in scope. Such discretion properly belongs to a controller.
- 89 Overall, EU institutions’ audit rights under the ILA were insufficiently robust in light of the risks posed by the processing. There was also a marked lack of detail as to how Microsoft was to fulfil its obligation to allow for and contribute to audits. They were, finally, too narrow in scope. EU institutions risked being unable to hold Microsoft accountable and, consequently, unable to discharge their own duty of accountability.
- 90 The EDPS appreciated that a hyperscale service provider would wish to avoid an unmanageable number of different audits conducted by different customers. But Regulation (EU) 2018/1725 is clear: controllers must be able to audit processors and sub-processors. The EDPS also considered that it should be possible to organise audits that satisfied multiple customers at once.

3.3.2 Recommendations

- 91 The EDPS made the following recommendations to EU institutions.

Recommendation Set 4: ensure effective audit rights

- The ILA should be amended in order to provide detailed, effective and enforceable audit rights for the controller and for the EDPS.
- The ILA should also require Microsoft to make available to EU institutions all the information that is needed to demonstrate compliance with Article 29 of Regulation (EU) 2018/1725. The contractual provisions should in the EDPS’ view cover information on

³⁶See also GDPR (n *b*) art 28(3)(h).

³⁷Microsoft, ‘DPA Data Protection Terms’ (n 12) ss ‘Auditing Compliance’.

the functioning of the systems used, access to data and recipients, sub-processors, security measures, retention of personal data, data location, transfers of personal data or any further processing of the personal data. Microsoft should also be required to notify EU institutions if it made substantial changes that were relevant from a data protection perspective, so as to prompt EU institutions to access and evaluate the information on those changes.

- The ILA should include provisions detailing how Microsoft is to apply in practice its obligations under the second subparagraph of Article 29(3) of Regulation (EU) 2018/1725.
- As controllers, EU institutions should establish an audit programme consisting of regular audits carried out by their internal or external audit team. The scope and frequency of the audits should reflect the scale of the processing and the risks for data subjects.
- Audits conducted under the ILA should collect factual evidence of Microsoft's compliance with its obligations.
- Meaningful audit results should be communicated to the appropriate levels of management within the EU institutions. The results should allow EU institutions to identify and act upon any compliance issues. They should also be provided to the EDPS at its request.

4 Data location, transfers and disclosure

- 92 The EDPS' investigation found that EU institutions were unable to control the location of a large portion of the data processed by Microsoft. Nor did they have full control over what was transferred out of the EU/EEA and how. There was also a lack of proper safeguards to protect data that left the EU/EEA. This had a negative practical impact on EU institutions' ability to hold Microsoft accountable.
- 93 EU institutions also had few guarantees that they were in a position to defend the privileges and immunities granted to them under the *Treaty on the Functioning of the European Union* ('TFEU'), and that Microsoft would only disclose personal data insofar as permitted by EU law.
- 94 In this section the EDPS considers the overlapping issues of data location, international transfers and disclosure in turn.

4.1 Data location

- 95 At the time the EDPS closed its investigation in March 2020, the (storage) location of (some) data was specified in the Online Services Terms.³⁸ Under the Online Services Terms, the obligation to store data in the EU applied only to a *subset* of the data *provided* through use of certain 'core online services'.

³⁸Microsoft, 'Attachment 1' in *Online Services Terms (OST)* (<https://aka.ms/ost>), s 'Location of Customer Data at Rest for Core Online Services'.

- 96 The *core online services* included Microsoft Office 365 services and certain *Microsoft Azure services*.³⁹ Microsoft committed to store only part of the data provided through use of those services in the EU. For Office 365 services, Microsoft committed to store only the *Exchange Online* mailbox content, the *SharePoint Online* site content and files uploaded to *OneDrive for Business* in the EU. Data provided through use of other Office 365 services did not appear covered, nor did user-identity information or metadata. For *Microsoft Azure Core Services*, such as *Azure Active Directory* (used for the management of user identities in Microsoft Online Services), the Online Services Terms expressly provided that: ‘Certain services may not enable Customer to configure deployment in [the EU/EEA] or outside the United States and may store backups in other locations.’⁴⁰
- 97 The Data Protection Addendum also made clear that ‘[e]xcept as described elsewhere in the DPA, Customer Data and Personal Data that Microsoft process on Customer’s behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Subprocessors operate.’⁴¹
- 98 The obligation to store data in the EU/EEA therefore applied only to a subset of the data processed by Microsoft when it provided ‘core online services’. The storage location of data falling outside of that subset was unclear, as was the location of data that was transferred out of the EU/EEA.
- 99 The negotiated terms of the umbrella agreement allowed data *collected* by Microsoft to be located anywhere Microsoft chose.
- 100 Insofar as Microsoft collected personal data from products and services as a controller, the Microsoft Privacy Statement was non-committal.⁴²
- 101 EU institutions were therefore not free to decide where to store their data. Nor were they free to decide on transfers out of the EU/EEA. In the EDPS’ view, the ILA provisions and Microsoft Privacy Statement did not even allow EU institutions to identify the location of all the different types of personal data processed under them.

4.2 International transfers

- 102 Where international transfers to third countries or international organisations are necessary, they should be carried out only in strict observance of the applicable transfer rules⁴³ and following a documented assessment of the risks to the rights and freedoms of data subjects. It is for controllers to decide whether to permit a transfer or not.
- 103 The EDPS’ understanding was that EU institutions had signed the ILA with Microsoft Ireland. The EDPS’ understanding was also that in the context of the ILA, any safeguards that had been put in place pursuant to international transfer rules had so far been contractual. To the EDPS’ knowledge, the Microsoft group had no binding corporate rules in place authorised under the GDPR or predecessor instruments.

³⁹Microsoft, ‘OST Attachment 1’ (n 38).

⁴⁰*ibid.*

⁴¹Microsoft, ‘DPA Data Protection Terms’ (n 12) s ‘Data Transfers and Location’, ss ‘Data Transfers’.

⁴²‘Privacy Statement’ (*Microsoft*) (<<https://aka.ms/privacy>>) s ‘Where we store and process personal data’.

⁴³Regulation 2018/1725 (n *a*) chapter V and in particular art 46; GDPR (n *b*) chapter V and in particular art 44.

- 104 Under the Data Protection Addendum, by executing the ILA, EU institutions were also deemed to have executed a set of standard contractual clauses ('SCCs') for international transfers of data, with Microsoft Corporation.⁴⁴ As a result, EU institutions had both a direct relationship with an EU-based processor (Microsoft Ireland) that could carry out international transfers to its sub-processors, and a direct relationship with Microsoft Corporation as a non-EU/EEA-based processor that could also carry out onward international transfers to its sub-processors. It was the EDPS' understanding that the vast majority of processing of personal data was in practice done by Microsoft Corporation and its sub-processors, not by Microsoft Ireland and its sub-processors.
- 105 Given this contractual matrix, EU institutions needed the following two layers of contractual safeguards. First, they needed to give instructions to Microsoft Ireland and Microsoft Corporation in the ILA on the extent to which personal data could be transferred out of the EU/EEA, under what conditions and subject to which safeguards. These needed to be mirrored in the SCCs for transfers signed by EU institutions with Microsoft Corporation. In light of this scenario, it would be appropriate to use SCCs adopted under Article 48(2)(b) or (c) of Regulation (EU) 2018/1725⁴⁵ between the EU institutions and Microsoft Corporation. Since, however, there are no such SCCs yet available, the EU institutions could, as an interim measure, make use of the provisions in SCCs such as those adopted under Commission Decision 2010/87/EU, subject to authorisation from the EDPS under Article 48(3)(a) of Regulation (EU) 2018/1725.
- 106 The position under the ILA was different, in so far that it presented, in the EDPS' view, the following issues.
- 107 First, as explained in the preceding sub-section on data location, the instructions under the ILA on what personal data Microsoft could transfer out of the EU/EEA, when and for what purposes were limited in scope and weak.
- 108 Second, EU institutions' instructions on the safeguards to which such transfers were to be subject to lacked precision. The negotiated umbrella agreement essentially committed Microsoft to observing its statutory obligations and gave no further detail as to how they were to be implemented.
- 109 Third, it was not clear whether the EU institutions' instructions in the negotiated documents of the ILA were intended to bind Microsoft Corporation as well as Microsoft Ireland. Microsoft Corporation was not expressly bound and as far as the EDPS was aware, not a signatory of those documents. In light of the contractual matrix, the EDPS considered it necessary for EU institutions' instructions to be unambiguously binding on both entities.
- 110 Fourth, the SCCs for transfers countersigned by Microsoft Corporation were not compliant. The EDPS' concerns were as follows.
- 111 **Controllers wishing to use SCCs for transfers adopted by the European Commission (such as SCCs adopted under Commission Decision 2010/87/EU) need to complete the appendices** to specify with precision the subject-matter, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, and the security measures to

⁴⁴Microsoft, 'Attachment 2' in *Data Protection Addendum (DPA)* (<https://aka.ms/dpa>).

⁴⁵See also GDPR (n *b*) art 46(2)(c) and (d).

apply to the data that are transferred.⁴⁶ The content of the appendices should be tailored to each **product and service concerned and each recipient (including subcontractors)**. Only then can the description fit the specific controller-processor relationship concerned.

- 112 In its standard implementation of those SCCs for transfers, Microsoft pre-populated the description of the processing in the appendices.⁴⁷ The lists of data subjects and categories of data were generic and broadly drafted, as they were designed to be the same for any customer. Depending on the operational needs of each EU institution, it might be that some of the categories did not apply, or that some fell within the catch-all category of ‘[a]ny other personal data’. The language of the appendices sought to overcome the generic nature of the lists by stating that ‘[c]ustomer may elect to include personal data from any of the following [types of data subjects/categories] in the Customer Data’. Yet this defeated the purpose of clearly describing the scope of the transfer.
- 113 Given that SCCs for transfers should be specific to each controller-processor relationship, it was also inappropriate that they should be negotiated (or imposed by Microsoft) at the level of incorporation into an umbrella agreement covering a large number of EU institutions.
- 114 Each controller should be able to specify the processing at issue in any SCCs for transfers it concludes with Microsoft Corporation. One option to move towards compliance would be a set of clauses that included a system of checkboxes in the appendices, to be completed and countersigned by individual controllers.
- 115 As with many other commitments in the ILA, these SCCs for transfers only applied to data provided through the use of online services. The EDPS was unaware of the existence of any corresponding contractual mechanism in respect of products and services that were not online services, or of data collected and processed by Microsoft as a controller. In the EDPS’ view, if such data were to be processed or transferred at all, it needed to be regulated at the level of the ILA. The EU institutions’ instructions at that level then needed to be reflected in any SCCs for transfers signed with Microsoft Corporation and in any further SCCs that Microsoft Corporation concluded with sub-processors regarding the transfers made to them.
- 116 Finally, given that the SCCs were only compliant if the parties made no changes to these terms (other than to fill out the appendices), the SCCs needed to prevail over other contractual terms in the contractual hierarchy of the ILA. This was not certain given the ambiguous order of precedence established in other contractual documents forming the ILA.

4.3 Unauthorised disclosure

- 117 Protocol No 7 to the TFEU provides for the inviolability of the property, assets, archives, communications and documents of the EU. It follows from the Protocol No 7 that a processor engaged by EU institutions must only disclose personal data that it processes on behalf of EU institutions if it either notifies the EU institution concerned and obtains its agreement, or with the authorisation

⁴⁶Article 29 Working Party, *Letter to Microsoft on a new version of the Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement and its Annex I* (2014) (https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf).

⁴⁷Microsoft, ‘DPA Attachment 2’ (n 44) appendix 1 and 2.

of the Court of Justice.⁴⁸ The protection offered to EU institutions by the Protocol does not end simply because they rely on an external provider for certain services.

- 118 **Article 49 of Regulation (EU) 2018/1725** [*see also Article 48 of the GDPR*] sets out that third-country administrative or court orders to disclose personal data are only to be given effect if they are based on an international agreement to which the EU is a party.⁴⁹
- 119 Article 4(1)(f) of Regulation (EU) 2018/1725 requires EU institutions to ensure the integrity and confidentiality of personal data processed on their behalf.⁵⁰
- 120 These legal obligations sat uneasily with the ILA's provisions on disclosure. The Data Protection Addendum permitted Microsoft to respond positively to requests for access to data where it considered that it had a legal obligation to do so.⁵¹ Microsoft would not even inform customers of a request if 'legally prohibited from doing so'.⁵² Of course, the Data Protection Addendum only covered a subset of the personal data processed under the ILA. As far as the EDPS was aware, there were no contractual commitments concerning disclosures that covered personal data falling outside of this subset.
- 121 In light of the EDPS' analysis that Microsoft retained discretion to process data as a controller, at least a part of that data was likely to be subject to the Microsoft policies referred to in the Microsoft Privacy Statement. This allowed Microsoft to disclose personal data (including Customer Data, Administrator Data, Payment Data and Support Data) to third parties, including law enforcement or other government agencies.⁵³
- 122 The Protocol No 7 and Regulation (EU) 2018/1725 protect EU institutions against disclosure requests that processors engaged by them may receive from EU Member State Governments. The Protocol and Regulation may not protect EU institutions against disclosure requests from third-country governments and processors subject to their jurisdiction. Depending on the laws of that third country and their extra-territorial reach, such processors may be faced by a conflict of laws and deem it prudent to comply with the laws of the third country even if this puts them in breach of EU law.
- 123 Consequently, if EU institutions make use of processors with links to third-country governments, they may in effect be choosing to forego the protections offered by the Protocol and Regulation against unauthorised disclosure.

⁴⁸See in this regard EDPS, *Guidelines on the use of cloud computing services by the European institutions and bodies* (2018) (https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf) para 60.

⁴⁹EDPB and EDPS, *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection* (2019) (https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en).

⁵⁰See also GDPR (n 6) art 5(1)(f).

⁵¹Microsoft, 'DPA Data Protection Terms' (n 12) s 'Disclosure of Processed Data'.

⁵²*ibid* s 'Disclosure of Processed Data' or in pre-2020 versions s 'Disclosure of Customer Data and Personal Data'.

⁵³'Privacy Statement' (n 42) s 'Reasons we share data', 'Where we store and process data' and 'Skype - Partner companies'. The data that is subject to disclosure includes 'Customer Data', 'Administrator Data', 'Payment Data' and 'Support Data'.

4.4 Consequences

- 124 In light of the position under the ILA and the circumstances of the EU institutions' relationship with Microsoft, the following practical difficulties arose.
- 125 If the personal data of EU institution users and other data subjects were located and processed outside of the EU/EEA, it became much more challenging for EU institutions to put in place effective measures to ensure compliance with Regulation (EU) 2018/1725 and to verify compliance in their capacity as controllers.
- 126 A lack of information about and control over data in transit was also concerning. Cross-border flows of personal data threaten the continuity of the level of protection guaranteed in the EU.⁵⁴ Without an accurate picture of the countries through which the data are likely to transit, it becomes very difficult for EU institutions to assess what technical, organisational, security and contractual safeguards they need to implement before a transfer is initiated. Therefore, they risk compromising their implementation of data protection principles (e.g. data minimisation, purpose limitation) and the confidentiality and security of the data that are transmitted. Yet, the Advocate General Saugmandsgaard Øe has recently underlined the need for controllers to ensure the protection of personal data, not only after they arrive in a third country, but after the transfer has been initiated, thus also during transit.⁵⁵
- 127 Once personal data is outside of the EU/EEA, in the absence of an adequacy decision covering the third country of destination or appropriate safeguards, data subjects might also find it difficult to exercise their rights. In those circumstances, data subject rights, the right to complain to an independent supervisory authority, the right to seek judicial redress and the right to claim compensation, could all be affected.
- 128 The Court has repeatedly held that effective control explicitly required by Article 8(3) of the Charter by an independent data protection authority is an essential component of the protection of personal data.⁵⁶
- 129 Microsoft and its sub-processors therefore risked not being held sufficiently to account for processing under the ILA.
- 130 If the data was not processed in the EU/EEA, it also risked becoming very difficult for EU institutions to enforce EU law to prevent disclosure. In particular, if the data were located in a third country, competent authorities in that country might request access to the data in the context of an enforcement action or under data retention legislation.⁵⁷
- 131 In this context, the EDPS's strong preference is that as a rule, the processing of personal data entrusted by EU institutions to Microsoft take place in the EU/EEA.

⁵⁴Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* EU:C:2019:1145, [2018] OJ C249/21 (Opinion of AG Saugmandsgaard Øe) paras 1 and 204.

⁵⁵*ibid* paras 234–237.

⁵⁶Case C-614/10 *Commission v Austria* EU:C:2012:631, [2012] OJ C72/13, para 37; Joined Cases C-293/12–C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:236, para 68; Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650, para 41.

⁵⁷*EDPS web services guidelines* (n 48) para 63.

4.5 Recommendations

132 The EDPS recommended the following to EU institutions.

Recommendation Set 5: control data location, international transfers and disclosures of data

- The ILA should include provisions detailing, in respect of each Microsoft product and service provided under it, the location of data collected and processed when EU institutions used that specific product or service.
- The ILA should explicitly require Microsoft to implement appropriate contractual, organisational and security safeguards in case of international data transfers. In particular, the ILA should require Microsoft to put in place robust security measures to cover data in transit.
- Any use of SCCs for transfers should comply with the applicable Union legislation.
- The ILA should prohibit Microsoft (and sub-processors) from disclosing personal data to Member State authorities, third-country authorities, international organisations or other third parties, unless this was expressly authorised by EU law, or by Member State law to the extent that the conditions laid down in EU law for such disclosure were fulfilled.
- The ILA should require Microsoft to inform affected EU institutions of any request Microsoft or sub-processors received for access to data, immediately upon receipt of the request. As a rule, Microsoft should redirect requests to the EU institution concerned and seek its instructions. In any event, Microsoft should challenge access requests, exhausting all available legal remedies. No disclosures of data by Microsoft or sub-processors should be permitted to take place without the prior notification, agreement and direction of the relevant EU institution and appropriate safeguards being in place. Should an EU institution choose not to disclose data, those data should only be disclosed upon order of the European Court of Justice.
- In addition to requiring notice of requests for access to data from Microsoft, EU institutions should request information from Microsoft once a year on whether any disclosures of EU institution data had taken place and if so, what action was taken in response. The relevant data controllers and their Data Protection Officers should assess the information received. The EU institutions should then take any further measures necessary to ensure that the contractual prohibition of disclosure, notification procedures and agreed safeguards were respected.
- Unless the EDPS' recommendations concerning sub-processors, data location, international transfers and unauthorised disclosure were implemented, the ILA should require that any processing of any personal data entrusted to Microsoft or its sub-processors by EU institutions should as a rule take place within the EU/EEA. This requirement should cover processing for the purposes of backing up data, business continuity and performing remote operations.

- In the medium term, if EU institutions wished to maintain the protections afforded by Protocol No 7 to the TFEU and Regulation (EU) 2018/1725 against unauthorised disclosure, they should seriously consider:
 - first, ensuring that data processed on their behalf is located in the EU/EEA, and
 - second, only using service providers that were not subject to conflicting third-country laws with extra-territorial scope.

5 Technical measures

5.1 Context

- 133 In 2016, the Commission identified a security and data protection issue posed by Microsoft’s collection of diagnostic data from its software. The software concerned was principally Office Pro Plus 2016 and *Windows 10 Enterprise*. This software did not offer built-in means by which EU institutions could completely manage or stop the flows of diagnostic data to Microsoft.
- 134 The Commission’s work in detecting and mitigating the security and data protection issues posed by Microsoft software illustrated the fact that on a technical (so not just contractual) level, Microsoft’s approach to providing its products and services was not fully compliant with the principles of data protection by design and by default.⁵⁸
- 135 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.⁵⁹ The EDPS has issued guidelines to EU institutions to assist them in doing so.⁶⁰
- 136 In general, the EDPS recommends that controllers should also evaluate the need for an assessment of data protection risks when they plan to use products or services offered by third-party providers, which will process large amounts of personal data.

5.2 Recommendations

- 137 In the particular context of the ILA and the products and services EU institutions were using at the time of the investigation, the EDPS issued the following recommendations.

⁵⁸Regulation 2018/1725 (n *a*) art 27; GDPR (n *b*) art 25.

⁵⁹Regulation 2018/1725 (n *a*) art 26 and 27; GDPR (n *b*) art 24 and 25.

⁶⁰EDPS, *Guidelines on the protection of personal data in IT governance and IT management of EU institutions* (2018) (https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf); *EDPS web services guidelines* (n 48).

Recommendation Set 6: implement measures to mitigate risks

- All EU institutions should perform tests to check the flow of personal data to Microsoft from its current and future products and services, following a comprehensive and documented approach. This approach should, in particular:
 - cover the normal usage patterns of their users involving the Microsoft products and services to be tested;
 - analyse all traffic exiting user computers and all its destinations so as to single out data flows from Microsoft software to Microsoft servers or its subcontractors.
- EU institutions should also monitor releases of Microsoft products updates and liaise with the company for their configuration to eliminate any unlawful transfer of personal data.
- Where an EU institution negotiates the procurement of software products or services on behalf of other EU institutions, the negotiating EU institution should inform the other EU institution of any data protection issues it identifies with the products or services.
- EU institutions should share with each other technical expertise and solutions to eliminate any unlawful transfer of personal data to Microsoft.
- Where EU institutions planned to use Microsoft products and services they did not already use (such as Microsoft Office 365 or Microsoft Azure cloud services), they should perform comprehensive assessments of the data protection risks posed by those products and services prior to deploying them.

6 Transparency

- 138 The abundance of contractual documents, the overlapping and conflicting terms within them, the lack of a clear order of precedence and the monthly updates to terms make it, at the very least, difficult for EU institutions, bodies, offices and agencies to discharge their information obligations to data subjects, as required by **Article 4(1)(a) of Regulation (EU) 2018/1725** [*see also Article 5(1)(a) of the GDPR*].

6.1 Recommendations

- 139 In the particular context of transparency towards the data subject, which enables them to exercise their data protection and other rights, the EDPS issued the following recommendations.

Recommendation Set 7: be transparent towards data subjects about how their personal data is processed

- Gain a sufficient level of assurance as to the subject matter and duration of processing, the nature, scope and purposes of the processing, the categories of personal data and data subjects concerned and the risks to data subjects to enable EU institutions to meet their transparency obligations.
- Prepare a data protection notice as part of the information to be made available to data subjects in accordance with Articles 15 and 16 of Regulation (EU) 2018/1725.

7 Conclusion

- 140 The EDPS advises organisations not to consider engaging any processor (or sub-processor) that is not willing to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of EU data protection rules and ensure the protection of the rights of data subjects. To comply with the principle of data protection by design and by default, organisations should verify both when processing is planned and during the processing, if no other alternative software solutions allow for higher privacy safeguards.
- 141 The EDPS recognises that the course of action recommended to EU institutions may appear a tall order for many, if not most, of Microsoft's volume licensing customers.
- 142 There were certainly concerns among controllers in the EU institutions that a hyperscale service provider would find acceptance of contractual changes such as those the EDPS was advocating either contrary to commercial sense, or impractical, or both. The EDPS has seen that Microsoft has shown itself, to a certain extent, ready to entertain some solutions to meet the compliance needs of EU institutions.
- 143 Where a contractor is committed to data protection, it does appear possible to bolster the protection of data subjects in a way that is commercially acceptable and can accommodate numerous customers at once.
- 144 The EDPS would therefore encourage controllers not to be disheartened at the prospect of negotiating instructions with a processor that they consider necessary to protect the rights and freedoms of data subjects; even when faced with a business partner of considerable heft.