DPC Ref: [redacted]
DPC Complaint Ref: [redacted]

Date: 1 September 2025

Complainant: [redacted]

Data Controller: Microsoft Ireland Operations Limited

RE: [redacted] v Microsoft Ireland Operations Limited

This document is a Decision of the Data Protection Commission ("**DPC**") in relation to DPC Complaint reference [redacted] hereinafter referred to as the ("**Complaint**"), submitted by [redacted] ("**Complainant**") against Microsoft Ireland Operations Limited ("**Microsoft**") to the Datatilsynet of Norway ("**NO SA**") and thereafter to the DPC in its capacity as the lead supervisory authority.

This Decision is made pursuant to the powers conferred on the DPC by section 113(2)(a) of the Data Protection Act 2018 ("**the Act**") and Article 60 of the General Data Protection Regulation ("**GDPR**").

Communication of Draft Decision to "supervisory authorities concerned"

In accordance with Article 60(3) GDPR, the DPC was obliged to communicate the relevant information and submit a draft decision, in relation to a complaint regarding cross border processing, to the supervisory authorities concerned for their opinion and to take due account of their views.

In accordance with its obligation, on 9 February 2024 the DPC transmitted a draft decision (the "**Draft Decision**") in relation to the matter to the "supervisory authorities concerned". As Microsoft offers services across the EU, and therefore the processing is likely to substantially affect data subjects in every EU member state, the DPC in its role as LSA identified that each supervisory authority is a supervisory authority concerned as defined in Article 4(22) GDPR. On this basis, the draft decision of the DPC in relation to this Complaint was transmitted to each supervisory authority in the EU and EEA for their opinion.

Relevant and reasoned objections were received from one supervisory authority concerned and comments were received from three other supervisory authorities. Having considered the objection received, the DPC was obliged to submit a Revised Draft Decision to the supervisory authorities concerned for their opinion. A Revised Draft Decision of the DPC in relation to this Complaint was therefore transmitted to each supervisory authority in the EU and EEA for their opinion.

Complaint Handling by the DPC – Timeline and Summary

1. The Complainant's 1 TB OneDrive account (a cloud-based file hosting service), was suspended by Microsoft on 3 February 2020, due to a serious breach of Microsoft's Services Agreement ("**MSA**") arising from the discovery of child sexual exploitation and abuse imagery ("**CSEAI**") by scanning software (PhotoDNA).

2. On 17 August 2020, the Complainant made an access request to Microsoft seeking access to the files contained in the suspended account. On 18 August 2020, a member of Microsoft's Norwegian OneDrive team responded to the access request, noting the account had been locked due to a violation of the Microsoft Services Agreement. On 6 September 2020, Microsoft declined to provide the files or the reason the account was suspended, stating "*Microsoft deactivated the access to our account due to a serious violation against Microsofts'* [sic] *service agreement https://www.microsoft.com/servicesagreement#3_codeOfConduct. As mentioned in the Agreement, you will no longer have access to services which require a Microsoft account.*"

   Further, on 11 September 2020, Microsoft informed the Complainant of the result of his appeal. Microsoft stated *"We have evaluated your appeal and verified that your account was locked due to serious violations against Microsofts' service agreement. https://www.microsoft.com/servicesagreement#3_codeOfConduct. According to our terms, we cannot reactivate your account nor provide information as to why it was locked. This represents Microsofts' final communication in connection with this account."*

3. On 17 November 2020, the Complainant complained to the Norwegian Data Protection Authority, Datatilsynet ("NO SA").

4. On 28 February 2021, the Complainant's data was permanently deleted by Microsoft in line with Microsoft's standard data retention policy.

5. On 10 March 2021, the NO SA passed the Complaint to the DPC.

6. On 20 August 2021, the DPC notified the Complaint to Microsoft asking for the following:
   a. an explanation of why the account was suspended;
   b. an explanation of the investigatory steps taken in suspending the account;
   c. whether there was an appeal mechanism and if it was triggered; and
   d. Microsoft to address the Complainant's concerns regarding his personal data.

7. The DPC notes Microsoft has requested that a number of its submissions remain confidential. However, the DPC considers it necessary that the facts pertaining to the account suspension are outlined in this Decision. The DPC has taken every effort to redact any information it has deemed either commercially sensitive or confidential insofar as that does not limit the DPC's ability to clearly set out the facts of this case and to clearly record its findings.

8. On 20 September 2021, Microsoft responded as follows:
   a. The Complainant's account was suspended for hosting CSEAI, a serious violation of the MSA. Microsoft noted that, in its experience, "*data subjects hosting CSEAI commonly have multiple illegal images, which may be stored on other Microsoft account related services as well as outside our services*".
   b. The CSEAI was detected by an image-matching technology and was then subject to human review.

c. The Complainant appealed the suspension to Microsoft Customer Support but the suspension was upheld.
d. Microsoft declined to provide data in response to the Complainant's access request, relying on the provisions of Article 15(4) GDPR, which states that the right to obtain a copy of the personal data undergoing processing shall not adversely affect the rights and freedoms of others.

9. On 1 October 2021, the DPC sent an amicable resolution letter to the Complainant via the NO SA summarising Microsoft's above response (excluding the reason for the account suspension as requested by Microsoft). The NO SA raised questions about the letter on 6 October 2021 and further questions on 21 October 2021 as follows:
    a. around the applicability of Article 15(4);
    b. whether there had been a police investigation;
    c. whether Microsoft would notify the Complainant of the details of the violation;
    d. whether Microsoft was still processing the Complainant's files or had they been deleted; and
    e. clarification as to the steps taken by Microsoft to amicably resolve the issue.

10. On 1 November 2021, the DPC put these questions to Microsoft. On 8 November 2021, Microsoft responded:
    - Microsoft did not have visibility as to whether a police investigation had taken place.
    - Microsoft does not typically notify the Complainant of the details of the violation, which it said was industry practice.
    - Microsoft confirmed that the data associated with the account was permanently deleted 12 months after the account was permanently suspended, in line with what is described in the MSA.

11. The DPC engaged with the NO SA between 18 November 2021 and 1 February 2022 regarding the above response, following which, on 8 February 2022, Microsoft informed the Complainant why his account had been suspended.

12. On 14 February 2022, the NO SA wrote to the DPC noting that the Complainant had been in contact after receipt of Microsoft's correspondence of 8 February 2022, querying what the next steps were in getting access to his data.

13. On 23 February 2022, the DPC wrote to Microsoft seeking the following information. Microsoft responded on 11 March 2022 (responses set out in italics below):

    a. a timeline including when the Complainant's access request was made and when their data was deleted:
    "*The account in question was suspended for a violation of the Microsoft Services Agreement on 3rd February 2020 at 23:44:13. After this suspension entered into effect, Microsoft's customer service team received multiple contacts from the data subject requesting that the suspension be lifted. Following a review of these contacts*

by our customer service team, they were unable to identify any clear data subject access request and understood these as requests to reactivate the account. Subsequent requests to support, like those shared with Microsoft by the DPC, were also understood as requests to reactivate the account and were not escalated to Microsoft's privacy response team. The data subject did not engage with the privacy response team according to our records. The first support case was raised on the 1st April 2020.

When the case was escalated to Microsoft by the DPC in August 2021, the data within the OneDrive account had already been erased in accordance with our standard data retention schedules. This occurred on the 28th February 2021."

b. an explanation of how the current situation has arisen, including that Microsoft has deleted the Complainant's data and cannot provide that data now;

"*Microsoft has deleted the data subject's OneDrive data and as a result can no longer provide it to the data subject.*"

c. a copy of Microsoft's Terms and Conditions and any applicable policies;

"*Please find the Microsoft Services Agreement here https://www.microsoft.com/en-us/servicesagreement. The section most relevant to account closures and the subsequent removal of data is section 4.a.IV.2 which reads as follows:*

"If your Microsoft account is closed (whether by you or us), a few things happen. First, your right to use the Microsoft account to access the Services stops immediately. Second, we'll delete Data or Your Content associated with your Microsoft account or will otherwise disassociate it from you and your Microsoft account (unless we are required by law to keep it, return it, or transfer it to you or a third party identified by you). You should have a regular backup plan as Microsoft won't be able to retrieve Your Content or Data once your account is closed. Third, you may lose access to products you've acquired.""

d. assurances that robust procedures are now in place to ensure this same situation will not happen again i.e. where data is deleted where there is an open query in relation to an access request:

"*Microsoft is currently evaluating its process for data subject access requests relating to accounts suspended for similar violations of Microsoft's Services Agreement, including the potential preservation of data in accounts where data subject access requests are received. We are also evaluating the language used by Microsoft's customer services and privacy response teams to improve our existing procedures*."

14. The DPC subsequently received, via the NO SA, correspondence from the Complainant (dated 21 February 2022), stating that he was unhappy with Microsoft's position, that not all points had been responded to, that he should not be held responsible for material uploaded by someone else and stating that he wanted access to [i.e. a copy of] the non-offending data [stored on the OneDrive account].

15. On 7 March 2022, the DPC forwarded the Complainant's email to Microsoft and asked for comment.

16. On 26 March 2022, Microsoft responded as follows:
    a. In creating an account, account holders agree to Microsoft's terms, including the Code of Conduct which prohibits any activity that exploits, harms, or threatens to harm children.
    b. Microsoft's Privacy Statement specifies that for some products, Microsoft scans content in an automated manner and explained how scanning technology identified offending material on the Complainant's account and noted that this was upheld on appeal.
    c. Microsoft noted that its MSA specifies that the account holder is responsible for any content uploaded to or shared by their account, including material stored or shared by others.

17. On 3 May 2022, the DPC issued an amicable resolution letter to the Complainant.

18. On 23 June 2022, the Complainant rejected amicable resolution. The Complainant protested that Microsoft:
    a. cannot remove private files from his family's computers without consent;
    b. cannot suspend access to private files which do not contain offending material;
    c. cannot lock his account without giving reasons; and
    d. cannot make him responsible (without warning) for files that others place in his (shared) folders.

19. The Complainant also did not accept that his data has been deleted.

20. On 30 June 2022, the DPC provided the Complainant's email to Microsoft seeking a response.

21. On 15 July 2022, Microsoft reiterated its previous position of 26 March 2022. Microsoft also noted that it had suspended access to the account but had not deleted the account itself; therefore, it would appear to the Complainant that there is still an active suspended account when he attempts to log in. Microsoft confirmed that this OneDrive account is empty and all data associated with the account has been deleted.

22. On 17 August 2022, the DPC sent an amicable resolution letter to the Complainant.

23. On 4 October 2022, the Complainant rejected amicable resolution.

24. On 26 January 2023, the DPC wrote to Microsoft asking it to clarify a number of issues, as underlined below. On 9 February 2023, Microsoft responded as set out below:

a. why it withheld personal data of the data subject, in particular data which did not constitute infringing content, in its response to the access request and its legal basis for doing so:

Microsoft noted that data subjects accept Microsoft terms when subscribing, including that violation of terms may result in account closure, upon which the data associated with the account will be deleted. Microsoft relies on Article 15(4) GDPR in withholding data in this case. Microsoft takes into consideration the child's best interests. The concept of the child's best interests is reflected in Article 24.2 of the European Charter of Fundamental Rights[1]. Microsoft claimed that research has shown that data subjects hosting CSEAI commonly have multiple illegal images.

Microsoft also noted that it relied on the following legal bases:

- Legitimate interest: Victims have a reasonable expectation that responsible companies will take steps to protect their fundamental rights, including by detecting and removing CSEAI from their services.
- Public Interest: In the case of confirmed CSEAI, to protect the interests of the victims and to protect data subject users from harmful, damaging, illegal content, as well as to advance the broader societal interests in preventing proliferation of CSEAI. The fight against CSEAI is an obligation under international law (the United Nations Convention on the Rights of the Child, with the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography).
- Vital Interests: To protect the vital interests of the data subject or natural person. In the case of confirmed CSEAI, Microsoft acts solely after detecting CSEAI (e.g., to share that data with the NCMEC to protect the vital interests of the victims.)

b. if Microsoft is seeking to rely on Article 15(4) GDPR as grounds for restricting the right of access of the Complainant,

i. identify the individuals (the "**Third Parties**") Microsoft considered in making its decision to withhold data pursuant to Article 15(4) GDPR:

Microsoft said the following categories were identified as individuals whose rights and freedoms may be adversely affected, for the reasons outlined:

[1] Article 24(2): "*In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration*." (Charter of Fundamental Rights of the European Union 2000/C 364/01 https://www.europarl.europa.eu/charter/pdf/text_en.pdf)

- Microsoft customers who upload CSEAI: This category of individual was considered as it includes the Complainant exercising the right of access.
- Microsoft's broader customer base, who do not upload CSEAI: This category was considered as there is potential that, if CSEAI were returned to the Complainant, it may be further illegally shared to other Microsoft users.
- Victims included in CSEAI.
- Other individuals included in CSEAI: While not the victim of the CSEAI, CSEAI does contain the personal data of the other individuals portrayed in CSEAI and they therefore warrant consideration in the decision-making process.

ii. identify the rights and freedoms of both the Complainant and the Third Parties considered by Microsoft, bearing in mind that not every interest amounts to a right or freedom for the purposes of Article 15(4).

In the case of confirmed CSEAI, Microsoft stated it does not typically grant customer requests to return account contents. It added that mere possession of child pornography is defined as a crime in most jurisdictions.

"As a result, these materials are the permanent record of the sexual abuse or exploitation of an actual child, and potentially criminal acts. Each further viewing or act of distribution is a distinct crime because it further victimises the child."

When making the decision not to provide data in response to such access requests, Microsoft said it takes into consideration the child's best interests. The concept of the child's best interests is reflected in Article 24.2 of the European Charter of Fundamental Rights.

c. Identify the adverse effects to the identified rights and freedoms of the Third Parties which would have occurred had the withheld data been provided to the Data Subject;

Microsoft stated that had the withheld data been provided to the Complainant, there is a real risk that Microsoft may have disseminated CSEAI to the Complainant potentially resulting in serious harm to the victims as well as other individuals included in CSEAI.

It stated that the broader justification for withholding personal data in the case of confirmed CSEAI is to protect the interests of the victims and to protect data subjects from harmful, damaging, illegal content, as well as to advance the broader societal interests in preventing proliferation of CSEAI.

d. detail how Microsoft conducted a balancing test;

Microsoft referred to its responses to (a), (b) and (c) above.

e. outline how Microsoft decided that the balance rested in favour of the Third Parties such that it should not share the Withheld Data with the Data Subject;

Microsoft concluded that individuals identified in the CSEAI would likely suffer a greater harm to their rights and freedoms than the Complainant were the withheld data to be returned to the Complainant. It stated there was also the risk that by returning the data and allowing for the proliferation of CSEAI, Microsoft's broader customer base, who do not upload CSEAI could subsequently be exposed to the material through its continued sharing. Microsoft stated that, in the case in question, "*one egregious instance of CSAM*" was identified on the account.

25. On 1 March 2023, the DPC wrote to the Controller informing it that, as the Complaint had not been amicably resolved, the DPC would now proceed to preparing a draft decision.

26. The following issues remained unresolved at the conclusion of complaint handling:
    a. Whether the Controller complied with Article 12(4) of the GDPR after the Complainant made an access request on 17 August 2020;
    b. Whether the Controller's reliance on Article 15(4) GDPR to withhold all of the Complainant's data was justified; and
    c. Whether the Controller was in compliance with Article 5(1)(a) GDPR in deleting the Complainant's personal data saved on his OneDrive account.

Conduct of Inquiry

27. Acting in its capacity as LSA, the DPC commenced an Inquiry in relation to this matter by writing to Microsoft and to the Complainant on 16 May 2023.

28. The DPC advised Microsoft that the Inquiry commenced by the Commencement Notice would seek to examine and address Microsoft's compliance with Articles 5, 12 and 15 of the GDPR in respect of the relevant processing, and reliance on Article 15(4) GDPR to refuse the Complainant access to his personal data.

29. The DPC advised Microsoft that the scope of the Inquiry concerned an examination of certain details regarding the Complaint, in particular whether or not Microsoft has complied with its obligations under the GDPR and the Act, in particular under Article 5, Article 12 and Article 15 of the GDPR in respect of the relevant processing operations which are the subject matter of the Complaint.

30. In order to progress the matter, the DPC posed specific queries regarding the access request and the manner in which it was handled by Microsoft.

31. The DPC requested Microsoft to demonstrate how it complied with all of the requirements of Article 12(4) GDPR. Microsoft was also asked to cite the relevant research it had indicated that

showed data subjects who host CSEAI imagery commonly have multiple illegal images. The DPC requested that Microsoft, having regard to the accountability requirements of Article 5(2) of the GDPR, outline its internal procedures to ensure the principles of lawfulness, fairness and transparency under Article 5(1)(a), and the principle of integrity under Article 5(1)(f) are complied with where personal data is processed in relation to an account that has been flagged for CSEAI, and in particular where there may be so-called "false positive" detections.

32. On 6 June 2023, Microsoft submitted its responses to the DPC queries in the Commencement Notice. Microsoft stated its records suggested that the data subject had never engaged with its Privacy Response Centre (PRC) and the transcripts of other support interactions had aged out in accordance with its data retention schedules. Microsoft informed the DPC that, had the data subject engaged with its PRC, the privacy response agent would have provided [the Complainant with] a standard response for an account suspended for CSEAI. Microsoft provided a copy of a standard response, cited below:

> "*Hello,*
> *Thank you for contacting Microsoft Privacy. We are writing in response to your request that we received from you.*
>
> *We understand that you wish to access personal data associated with a Microsoft account. Upon review, we have determined that the referenced account violated the Microsoft Services Agreement and has subsequently been suspended. Access to the relevant data is not possible at this time, among other reasons because doing so could pose risk to the rights and freedoms of other individuals. You also have the right to make a complaint to the data protection supervisory authority in Ireland: https://www.dataprotection.ie/.*
>
> *Best Regards,*
> *Microsoft Privacy*"

33. In response to the DPC query in the Commencement Notice asking Microsoft to cite the research on which it relied to support its contention that data subjects hosting CSEAI commonly have multiple illegal images, Microsoft cited the research of the United States Sentencing Commission and its estimates that convicted offenders typically possess an average of ~4,000 CSEAI images, and noted the following:

> *"Facilitated by advancements in digital and mobile technology, non-production child pornography offenses increasingly involve voluminous quantities of videos and images that are graphic in nature, often involving the youngest victims. In fiscal year 2019, non-production child pornography offenses* ***involved a median number of 4,265 images****, with some offenders possessing and distributing millions of images and videos. Over half (52.2%) of non-production child pornography offenses in fiscal year 2019 included images or videos of infants or toddlers, and nearly every offense (99.4%) included prepubescent victims."*

34. As regards the DPC query asking Microsoft to outline its internal procedures to ensure the principles of lawfulness, fairness and transparency under Article 5(1)(a) and integrity under Article 5(1)(f), Microsoft outlined its practices and procedures as regards each principle.

35. In relation to **transparency**, Microsoft informed the DPC that in instances where personal data is being processed in relation to an account that has been flagged for CSEAI, the Microsoft Privacy Statement explains the [different types of] personal data that Microsoft processes, how Microsoft processes it and for what purposes. Microsoft attached the publicly available information as well as standard communications it uses to inform data subjects of CSEAI scanning and their rights. Microsoft advised that data subjects are notified of Microsoft retention practices through the Microsoft Privacy Statement.

36. In relation to **lawfulness**, Microsoft stated that where personal data is being processed in relation to an account that has been flagged for CSEAI, it relies on the following legal bases:

> **Legitimate interest**: Users of Microsoft's Services are informed through the Microsoft Privacy Statement and other public materials (for example, at https://privacy.microsoft.com), which explains that Microsoft scans data subject user generated content for safety and compliance with its Terms of Use, including any applicable code of conduct. Microsoft stated that its policy is that only shared or public content is scanned. Microsoft noted that scanning shared or public data subject user generated content for CSEAI is also a common industry practice within its reasonable expectations. Microsoft stated that victims have a reasonable expectation that responsible companies like Microsoft will take steps to protect their fundamental rights, including by detecting and removing CSEAI from their services. As regards other individuals included in CSEAI, Microsoft stated that the benefits of processing for the victims of CSEAI outweigh the risks associated with the processing not being within the reasonable expectation of such individuals.
>
> **Public Interest:** Microsoft stated that processing is necessary for the performance of a task carried out in the public interest: In the case of confirmed CSEAI, to protect the interests of the victims and to protect data subject users from harmful, damaging, illegal content, as well as to advance the broader societal interests in preventing proliferation of these materials. According to Microsoft, the fight against CSEAI is an obligation under international law (the United Nations Convention on the Rights of the Child ("UNCRC"), in particular with the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography).
>
> **Vital Interests:** Microsoft stated that to protect the vital interests of the data subject or natural person, in the case of confirmed CSEAI, Microsoft takes action solely after detecting CSEAI (e.g., to share that data with NCMEC) to protect the vital interests of the victims.

37. In relation to **fairness,** Microsoft informed the DPC that where personal data is being processed in relation to an account that has been flagged for CSEAI, account owners are notified of the suspension of their account when they attempt to sign into a Microsoft service attached to the suspended account. The account owner can request review and appeal of the suspension through

one of two customer support E-forms. Upon submission of the request for review and appeal, the reason for the suspension is identified by the internal review team. If the internal review team confirms the reason for suspension is CSEAI content, trained human reviewers will re-review the content to confirm the flagged content that resulted in suspension is in fact CSEAI, provided the data has not been deleted following the expiration of the applicable retention period. If Microsoft confirms that the account was suspended due to a CSEAI match, Microsoft notifies the user that the appeal is denied, and that the account is ineligible for reactivation due to a serious violation of the Microsoft Services Agreement. If it is determined that the content is not CSEAI, and does not otherwise violate the Code of Conduct, the suspension will be removed, and the customer will be notified of the change.

38. As regards the DPC query relating to "false positives" Microsoft stated that it was important to note the relative[ly small] scale of the numbers involved. The reasons for certain false positives were not related to errors, but rather reversal of human decisions in "edge cases".

39. On 12 June 2023, the NO SA transferred to the DPC the Complainant's response of 9 May 2023 to the Commencement Notice. In his response, the Complainant attached documentation of his communications with Microsoft (as well as the communications of other users with Microsoft, who appeared to be members of the Complainant's family, and who shared a OneDrive account with the Complainant) between 5 February 2020 and 31 May 2020. The DPC understands these communications to demonstrate efforts on the part of the Complainant (as well as apparent family members) to try and reactivate the OneDrive account and the responses received from Microsoft.

Notification of Preliminary Draft Decision to the Controller

40. The DPC provided Microsoft with a copy of the Preliminary Draft Decision ('**PDD**') on 16 November 2023 and requested that it provide, by 11 December 2023, any final submissions which it wished the DPC to consider when completing its draft decision.

41. Microsoft responded to the DPC on 1 December 2023, requesting confidentiality in relation to certain of its responses to the DPC during the complaint handling and inquiry processes. Microsoft requested that elements of its responses be confidential so as to prevent individuals who may be engaged in criminality from circumventing Microsoft's processes. On 11 December 2023, Microsoft confirmed it had no substantive submissions on the PDD.

42. The DPC has carefully considered Microsoft's response to the PDD and, in that regard, when issuing the PDD to the Complainant, the DPC acceded to Microsoft's request not to share with him certain information for reasons of confidentiality. In summary, that confidential information has been redacted from this Decision.

Notification of Preliminary Draft Decision to the Complainant

43. The DPC provided the Complainant (via the NO SA) with the PDD on 22 December 2023, inviting the Complainant to make any final submissions within two weeks of receipt of the PDD. Following a request by the NO SA for an extension, the DPC received the Complainant's submission on the PDD on 6 February 2024. The DPC has carefully considered the Complainant's submission.

44. The Complainant reiterated a number of arguments he had previously made to the DPC during the complaint-handling and inquiry processes. The Complainant reiterated his argument that Microsoft, in his terminology, cannot remove private files from his family computers without his consent. The DPC notes the similar argument made by the Complainant in correspondence on 26 June 2022, in which he stated: *"Some of the data were stored on the computers of my wife and children, based on my consent (which I hope Microsoft still has available). These files have been removed from the computers of my family (while still being available at Microsoft)".* Further the Complainant stated in his submissions to the PDD that *"Microsoft did not act on his behalf when removing the files from* [the family's] *machines."*

45. The DPC notes that Microsoft responded to the Complainant's argument of 26 June 2022 on 15 July 2022 where it stated: "*Our PhotoDNA technology identified a hash set in the account, resulting in its immediate suspension, and the immediate and automatic restriction of access to all Services used by the account.* ***As a result, access, including by linked devices, was suspended to all files that have been saved only to the account. This would not have impacted files stored locally on the device*** [emphasis added]**.** *For example, the data subject will no longer have access to all files synced to the OneDrive folder. The Microsoft Services Agreement provides additional details in section 4 'Using the Services & Support', items '4.a.iv.2'"* and that as specified by the Microsoft Services agreement, Microsoft services allow users to store or share their content or receive material from others and that users are responsible for their content, "*Therefore, the account holder is solely responsible for any content uploaded to or shared by their account, including material stored or shared by others."*

46. In relation to the date of his access request as outlined in the PDD, the Complainant stated in his submission that there were many and varied access requests before 17 August 2020, and noted an email sent to OneDrive Support on 11 February 2020, submitted as part of the Complainant's responses to the Inquiry Commencement Notice. The Complainant stated that the reason Microsoft understood all of his requests for data as requests to lift the suspension was because the only way to communicate with Microsoft was to complete a form related to account suspension issues. The Complainant stated that in other attempts to contact Microsoft about the issue, he did not receive a response. The Complainant stated: *"Microsoft provides a routine to send requests IF you have a working account"* and that due to the fact his account was suspended, the only way of communicating with Microsoft was to complete the form to lift the suspension. The DPC notes however, at paragraph 13.a (above), that Microsoft stated it was unable to identify any clear access request and therefore the DPC does not propose to change its analysis as regards the date of a single identifiable access request made by the Complainant.

47. The Complainant in his submission on the PDD stated that he was not provided with evidence for the claim that CSEAI was found on his account. He stated that, in his view, the minimum

requirement would have been for Microsoft to have provided the Complainant with a file name or to have contacted the police if the case was as serious as indicated by Microsoft. The Complainant noted he was informed of the reason for his account suspension after 18 months.

48. The Complainant referred to Microsoft's reliance on Article 15(4) GDPR not to provide him with the files on his OneDrive account and referenced paragraph 80 of the Court of Justice of the European Union judgment in case C-579/21[2]. This states that "*in the event of a conflict between, on the one hand, the exercise of a right of access which ensures the effectiveness of the rights conferred on the data subject by the GDPR and, on the other hand, the rights or freedoms of others, a balance will have to be struck between the rights and freedoms in question.*" It states that, wherever possible, means of communicating personal data that do not infringe the rights or freedoms of others should be chosen [and that] 'the result of those considerations should not be a refusal to provide all information to the data subject'.

49. Further, the Complainant made reference to what he believed was the possibility for Microsoft to retrieve a subset of his files which did not contain "*problematic content*" by retrieving the files he had on his OneDrive account some days prior to the incident. However, Microsoft, in its responses to the DPC on 8 November 2021, noted that differentiated access to data would be service dependent, but this was not possible in this instance as the data had already been deleted.

50. As regards the finding of one image of CSAM on the Complainant's account, the Complainant noted in his submission that Microsoft had argued that offenders typically possess an average of 4000 images. He stated that, as Microsoft had found only one such image on his account, that this was a clear indication "*that some kind of mistake has happened*" and that "*a more detailed consideration of the data is in place*". In relation to Microsoft's argument regarding the provision of the data to the Complainant and a risk of dissemination of CSAM to the Complainant, the Complainant argued that Microsoft must assume that the Complainant had access to his own files and thus, by "*giving back some files does not make a difference*" and the "*risk seems not valid in the light that the local files of the main account holder stay put* [i.e. on their own device(s)]."

51. In his submission, the Complainant also stated that his account was not "*closed*" within the meaning provided in the Microsoft Services Agreement and that it remained merely "*suspended*". He stated that the term "*permanently suspended*" was not included in the Microsoft Services Agreement. He also submitted that this position was backed by his communications with Microsoft's telephone service support, which he stated he had no written documentation to back up, but that such records might be held by Microsoft in the form of call recordings.

Communication of Revised Draft Decision to the Controller

52. The DPC provided Microsoft with a copy of the Revised Draft Decision on 1 May 2025. Microsoft reverted on 15 May 2025 with one minor amendment, which is reflected in this Revised Draft Decision.

[2] CURIA - Documents (europa.eu)

Communication of Revised Draft Decision to the Complainant

53. On 22 May 2025, the Complainant reverted to the NO SA, who on 26 May 2025, thereafter provided the DPC with the submissions to the Revised Draft Decision, which have been given fair and thorough consideration by the DPC. The DPC notes the Complainant "*denies that there was CSEAI in the account*." The DPC notes that elements of the submissions as provided by the Complainant contain information that is out of the scope of the DPC's inquiry, and which do not pertain to the issues investigated/examined in this Revised Draft Decision. In addition, the Complainant's submissions reiterated arguments which had previously been made both at response to Commencement Notice stage, and in submissions to the Preliminary Draft Decision. In reviewing these submissions, the DPC finds that the Complainant has not raised any new points that would change the outcome of this Revised Draft Decision.

Communication of Revised Draft Decision to Concerned Supervisory Authorities

54. A revised draft of this Decision was submitted to the Concerned Supervisory Authorities (CSAs) across the EU and EEA pursuant to Article 60(5) of the GDPR. No "relevant and reasoned" objections were received on the Revised Draft Decision. One comment was received from the Berlin SA which the DPC has taken into consideration when finalising this decision.

Applicable Law

55. For the purposes of its examination and assessment of this Complaint, the DPC has considered the following Articles of the GDPR:

- Article 5
- Article 12
- Article 15

The relevant legal provisions are as follows:

According to Article 5(1)(a) of the GDPR, personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

Article 12(4) of the GDPR stipulates that if the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Article 15(4) of the GDPR states that the right of the data subject to obtain a copy [of the personal data undergoing processing] shall not adversely affect the rights and freedoms of others.

Analysis and Findings

a. Whether the Controller complied with Article 12(4) of the GDPR after the Complainant made an access request on 17 August 2020;
b. Whether the Controller's reliance on Article 15(4) to withhold all of the Complainant's data was justified; and
c. Whether the Controller was in compliance with Articles 5(1)(a) in deleting the Complainant's personal data (i.e. any personal data contained in the relevant OneDrive account).

a. Whether the Controller complied with Article 12(4) of the GDPR after the Complainant made an access request on 17 August 2020

56. Article 12(4) requires that the controller is to inform the data subject without undue delay of any actions not taken and the reasons for such as regards the data subject's request. Article 12(4) also stipulates that the controller is to inform the data subject of the possibility to lodge a complaint a supervisory authority and to seek judicial remedy.

57. The Complainant submitted a valid access request on 17 August 2020, stating he wanted to "*get access to* [his] *files*". According to Microsoft, the Complainant's access to his OneDrive account was suspended due to a breach of the Microsoft Services Agreement. Microsoft informed the Complainant on 6 September 2020 that his account was deactivated due to serious violation of Microsoft's Service Agreement and that the Complainant would no longer have access to the services requiring a Microsoft account.

58. The Complainant on 7 September 2020 requested again to have access to his files, stating *"I would like to have my files back.*" On 11 September 2020, Microsoft stated *"We have evaluated your appeal and verified that your account was locked due to serious violations against Microsofts'* [sic] *service agreement…According to our terms we cannot reactivate your account nor provide information as to why it was locked. This represents Microsofts'* [sic] *final communication in connection with this account*."

59. When the DPC requested Microsoft to provide a timeline of the facts of the case including when that access request was made, Microsoft made reference to communications between the Complainant and Microsoft prior to receipt of the access request on 17 August 2020 (specifically Microsoft made reference to a timeline between February and April 2020). Microsoft also stated it was unable to identify any clear data subject access request [from these communication exchanges between February and April 2020]. The DPC has received correspondence from the Complainant in which he provided copies of numerous exchanges between him, what appear to members of the Complainant's family, and Microsoft during this time period. These exchanges appear to be between the Complainant, his family members and members of Microsoft OneDrive Support team, Microsoft Online Safety team, as well as Microsoft Premier Support team. However, as it has been ascertained that an access request was made on 17 August 2020, the relevant communications under consideration as regards adherence to Article 12(4) GDPR for the purpose of this Decision is any correspondence exchanged between Microsoft and the Complainant after 17 August 2020. In its responses to the Complainant, Microsoft did not fully

engage with the access request nor did its correspondence to him refer to any of the provisions of the GDPR that Microsoft was relying on in deciding not to provide access to his data on the OneDrive account.

60. Therefore, it is clear to the DPC from reviewing the correspondence between the Complainant and Microsoft as regards the access request of 17 August 2020, that Microsoft did not inform the Complainant of his rights pursuant to Article 12(4) of the GDPR, notably the right to lodge a complaint with a supervisory authority and the separate right to seek a judicial remedy.

61. **Finding 1: On the basis of the above, the DPC finds that Microsoft infringed Article 12(4) of the GDPR as it failed to provide the Complainant with information that he had a right to lodge a complaint with a supervisory authority and to seek a judicial remedy when it did not take action on his access request of 17 August 2020.**

b. Whether the Controller's reliance on Article 15(4) to withhold all of the Complainant's data was justified

62. Article 15 of the GDPR provides the data subject the right of access to personal data concerning them that is processed by the controller. Article 15 prescribes the categories of information to be provided to the data subject. However, the right to obtain a copy of the personal data undergoing processing, as provided in Article 15(3), may be subject to an exception provided in Article 15(4) of the GDPR, which outlines that the right of the provision of the personal data shall not "*adversely affect the rights and freedoms of others*".

63. According to the EDPB (European Data Protection Board) guidelines[3], the provision of personal data is subject to exemption as per Article 15(4) GDPR, in which the guidelines provide:

> "*The right of access is subject to the limits that result from Art. 15(4) GDPR (rights and freedoms of others) and Art. 12 (5) GDPR (manifestly unfounded or excessive requests).*"
>
> Further, *"That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software*."

The EDPB guidelines specify Article 15(4) applies to the right to obtain a copy of the data. The guidelines also specify that if the controller is to rely on Article 15(4), the controller must be able to demonstrate in the concrete situation that the rights and freedoms of others would be impacted. Microsoft has provided details on the considerations of the risks to the rights and freedoms of other users, as well as the possible impacts, should it have provided access to the Complainant to the data, which included the infringing content.

[3] European Data Protection Board (EDPB) '*General Guidelines 01/2022 on data subject rights - Right of access*' Version 2.0 Adopted on 28 March 2023, available at: https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

64. In response to a query posed by the NO SA on the possibility of differentiated access assessment (such as the possibility to provide certain personal data but not all personal data to the Complainant), dependant on the different types of, and origins of, personal data in relation to the justification for the application of Article 15(4), Microsoft responded stating that as the data had been deleted, differentiated access was not possible in this case, however in other cases differentiated access to the data would be service dependent.

65. The DPC understands that human review took place on the Complainant's account, as stated by Microsoft in its correspondence to the DPC on 15 July 2022: "*Microsoft evaluated the appeal that the data subject raised and trained human reviewers verified that the account was locked due to serious violations of the Microsoft Services Agreement*."

66. As outlined in paragraph 24, the DPC requested on 26 January 2023, that Microsoft explain its reasoning for withholding all personal data from the Complainant, in particular data which did not constitute infringing content, and that it provide the legal bases on which Microsoft contended it was justified to restrict right of access to the Complainant. The DPC also requested that, if Microsoft was seeking to rely on Article 15(4) of the GDPR as grounds for restricting access to the Complainant for obtaining a copy of the account data, that it provide details of the factors taken into account, as well as how it conducted a balancing test, in deciding to refuse the Complainant access to his account data.

67. In response to the DPC's query on the withholding of all data from the Complainant, in particular non-infringing content, Microsoft referred to section 3(b) of the Microsoft Services Agreement (MSA), which provides that a violation of the terms of the MSA, including the rules outlined at section 3(a) *Code of Conduct*, may result in the closure of a Microsoft account. Microsoft further referred to Section 4(a)(iv)(2) which stated that when a Microsoft account is closed, "Data" and "Content" associated with the Microsoft account will be deleted. Microsoft stated it relied on Article 15(4) of the GDPR to withhold the Complainant's personal data. In addition, Microsoft stated it takes into account the child's best interests when reviewing such cases, and the legal bases it relied on were legitimate interest, public interest and vital interests. Microsoft referred to research data that it stated had shown data subjects hosting CSAM [child sex abuse material] commonly have multiple illegal images. Microsoft expanded further on this point in its responses to the Commencement Notice, outlined at paragraph 33 of this Decision. Microsoft's submissions to the Inquiry stated that it identified the categories of individuals, as well as the rights and freedoms of those individuals that could be impacted, if it were to provide the Complainant with access to his personal data on the OneDrive account.

68. It must be noted that where a controller does have concerns about the impact of complying with an access request, the controller should not refuse to provide all information to the individual but should endeavour to comply with the request insofar as possible whilst ensuring adequate protection for the rights and freedoms of others. Article 15(4) GDPR does not provide a blanket exemption for a controller to refuse to act on an access request. Microsoft outlined to the DPC its reasons for its reliance on Article 15(4) of the GDPR, such as the implication of adverse effects to the rights and freedoms of identified third parties should Microsoft provide the Complainant with

access to his data, as well as the importance of ensuring safety for minors and other users of Microsoft, to protect them from any potential risk of harm or damage.

69. In the case at hand, the DPC understands that Microsoft's channels did not recognise the Complainant's request as an access request and that, having been notified of the Complaint by the DPC, Microsoft then (i) retrospectively appears to have accepted that there was an access request and (ii) stated that it was then going to rely on the exemption under Article 15(4) to provide no data to the Complainant.

70. The DPC accepts that, in principle, Microsoft established that there was a risk to the rights and freedoms of others in providing data that had been saved on the OneDrive account to the Complainant. However, in this specific case, the data on the account had already been deleted and Microsoft was therefore not able to demonstrate in a concrete sense that a balancing test actually took place. Microsoft outlined what it stated were the potential risks to other Microsoft users should the Complainant have been provided with his data, including the risks to the victims depicted in what Microsoft described as the "*egregious*" content detected on the account. However, no documentary evidence as to the conduct of the balancing test was provided to the DPC and it therefore appears to have been merely hypothetical in this specific case.

71. Based on the above, and in view of the fact that the data was deleted on 28 February 2021, the DPC cannot ascertain whether or not Microsoft was entitled in this specific case to rely on the exemption under Article 15(4) GDPR to refuse to provide the Complainant with a copy of his personal data, namely any personal data saved in his OneDrive account. The DPC has taken into consideration in its findings the particular details of the case, such as the discovery by means of automated scanning of CSAM in the Complainant's OneDrive account, which Microsoft stated was confirmed upon further human review. However, as the Complainant's data had already been deleted and it would not have been possible for Microsoft to provide it to him in any case, its reliance on Article 15(4) was in fact moot. By the same logic, it is therefore not possible for the DPC to establish whether or not there was any infringement of Article 15(3) of the GDPR in this specific case.

c. Whether the Controller complied with Article 5(1)(a) in deleting the Complainant's personal data

72. Article 5 of the GDPR sets out the fundamental principles of data protection which a controller must adhere to. Article 5(1)(a) of the GDPR refers to the principles of lawfulness, fairness and transparency.

73. Microsoft has stated it has deleted any data associated with the Complainant's account, in line with its terms and conditions as well as its procedures. On 11 March 2022, Microsoft confirmed that the deletion of the Complainant's data occurred on 28 February 2021, which was 6 months after the access request of 17 August 2020 had been received. Microsoft stated that the deletion of the Complainant's data was in accordance with Microsoft data retention schedules. The deletion of the data had, based on the timeline, taken place during the month prior to the Complaint being notified to the DPC in March 2021.

74. The DPC will now analyse the provision of information to the Complainant at all stages of the process, in furtherance of Microsoft's obligations under Article 5(1)(a). The DPC proposes to analyse the information provided to the Complainant during his interactions with the Privacy Response Channel (after the date of the 17 August 2020 access request), the information provided in the Microsoft Services Agreement, and the information provided in the Microsoft Privacy Statement.

Complainant's engagement with OneDrive Support / Microsoft Services Agreement

75. Following the Complainant's access request of 17 August 2020, the Complainant was informed by a team member of the Norwegian OneDrive support team on 18 August 2020 that his account was "*temporarily locked*" due to a violation of the Microsoft Services Agreement (to which a link was provided). During the inquiry process, the DPC was informed that the Complainant would have been aware of the Microsoft Services Agreement when he set up a Microsoft account, as well as the Code of Conduct. The Microsoft OneDrive support team member included a link to the Microsoft Services Agreement in the response of 18 August 2020. The Microsoft Services Agreement outlines to Microsoft users that users are responsible for their content, as evident in paragraph 2 of the services agreement under the section *Your Content* which stated *"We don't claim ownership of Your Content. Your Content remains Your Content and you are responsible for it."*

76. Microsoft users are also made aware from the Services agreement that certain repercussions may occur in the event a user violates any of the terms of service outlined in the agreement. The Microsoft Services Agreement stated as of 1 August 2020[4] in *Section 3. Code of Conduct (b)Enforcement*:

> *"In addition, if you violate any of the obligations listed in section 3(a) above or otherwise materially violate these Terms, we may take action against you including (without limitation) stopping providing Services or closing your Microsoft account immediately for good cause or blocking delivery of a communication (like email, file sharing or instant message) to or from the Services. We also reserve the right to remove or block Your Content from the Services at any time if it is brought to our attention that it may violate applicable law or these Terms."*

77. Later on 18 August 2020, the Complainant responded to Microsoft's OneDrive support channel and stated that he had thought the account was "*temporarily locked*" but that "*after a while it was confirmed that Microsoft had permanently locked the account, and I have not been able to do anything about it*". Microsoft's agent responded and stated that they understood that "*the situation is problematic"* and stated that they would escalate the case internally for further review and that this "*might take a couple of days*".

78. The Complainant was again informed on 6 September 2020, that his account had been disabled due to a "serious violation" of the Microsoft Services Agreement and he was provided a link

[4] https://web.archive.org/web/20201216093621/https://www.microsoft.com/en-ie/servicesagreement/

specifically to the *Code of Conduct* section of the Microsoft Services Agreement which states that the user is accountable for the conduct and content when using the [Microsoft] Services and specifies the terms of the agreement as well as the rules a user is to abide by. The Complainant was further made aware of the Code of Conduct section of the Services Agreement following his access request. Microsoft stated in its response to the Complainant on 6 September 2020:

> *"Microsoft deactivated the access to your account due to a serious violation against Microsofts' service agreement https://www.microsoft.com/servicesagreement#3_codeOfConduct.*
>
> *As mentioned in the Agreement, you will no longer have access to services which require a Microsoft account."*

79. The Complainant appears to have submitted an appeal, to which in response Microsoft informed the Complainant on 11 September 2020, that it had evaluated his appeal "*and verified that your account was locked due to serious violations against Microsofts'* [sic] *service agreement. According to our terms, we cannot reactivate your account nor provide information as to why it was locked. This represents Microsofts' final communication in connection with this account."*

80. The DPC notes that the Microsoft Services Agreement, in referring to circumstances where an account may be "reactivated", refers only to circumstances where a data subject requests that Microsoft close their account and then seeks to reactivate it themselves. In such circumstances, the Microsoft Services Agreement states that the account will be "*put into a suspended state for 60 days just in case you change your mind*". However, it does not explain the circumstances in which Microsoft itself might "suspend" access to an account which it might later decide to reactivate, such as in circumstances where an individual appeals against that suspension.

81. Microsoft outlined to the Complainant the various parts of the agreement to which the Complainant would have agreed to when he set up a Microsoft account, specifically the Code of Conduct. Microsoft stated to the Complainant in correspondence on 26 March 2022:

> "*By creating a Microsoft account and using the services to which the account is linked, account holders agree to Microsoft's terms, including our Code of Conduct. The Code of Conduct details the activities that are prohibited when using our services and enforcement actions that may be taken if the terms or the Code of Conduct are violated.*
>
> *Specific to your case we ask you kindly to refer to the Microsoft Services Agreement, section 3 'Code of Conduct'. The detection of child sexual exploitation and abuse material within your account resulted in a determination that item 3.a.ii. of the Code of Conduct, "Don't engage in any activity that exploits, harms, or threatens to harm children" had been violated. section 3 'Code of Conduct'*."

82. In Section 4 of the Microsoft Services Agreement, *Using the Services and Support*, Microsoft outlines what occurs should a user's account be "*closed*" by Microsoft:

4(a)(iv)(ii) "*If your Microsoft account is closed (whether by you or us), a few things happen. First, your right to use the Microsoft account to access the Services stops immediately. Second, we'll delete Data or Your Content associated with your Microsoft account or will otherwise disassociate it from you and your Microsoft account (unless we are required by law to keep it, return it or transfer it to you or a third party identified by you). As a result, you may no longer be able to access any of the Services (or Your Content that you've stored on those Services) that require a Microsoft account. You should have a regular backup plan. Third, you may lose access to products you've acquired*."

83. The Microsoft Services Agreement available to the Complainant outlines certain actions that may be taken by Microsoft in response to a violation of the terms of service, which may include **closing the relevant Microsoft account immediately**. However the DPC finds that, in the current case, the communications to the Complainant during his engagement with the Microsoft channels were not sufficiently clear as to the fact that his account had been closed (and not just "suspended" or "locked") and that his data had been, or would subsequently be, deleted. There was also no information provided to the Complainant in relation to the length of time for which his data would be retained by Microsoft before it was irretrievably deleted. This resulted in a lack of transparency as to the procedure that would be followed by Microsoft in relation to the data saved on the Complainant's account. This lack of clarity about whether the account was, in fact, closed without the possibility of retrieval, or whether it was merely in a "locked" or "suspended" state, allowed the Complainant to hold on to the expectation that it would ultimately be possible for him to get his data back, when this was not in fact the case. Indeed, as is clear from the chronology of this Complaint, the data on the OneDrive account had already been deleted just 10 days before the Complaint was received by the DPC on 10 March 2021.

Complainant's engagement with OneDrive Support / Microsoft Privacy Statement

84. The Microsoft Privacy Statement outlines the various different retention periods for specific categories of data, and stated: "*Microsoft retains personal data for as long as necessary to provide the products and fulfil the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types, the context of our interactions with you or your use of products, actual retention periods can vary significantly."*

85. Microsoft referred to the privacy statement in communication with the Complainant, outlining how it uses data. It referred the Complainant to the following section: *"[W]e use data to protect the safety of our products and our customers, and specify that for some of our products, we systematically scan content in an automated manner*."

86. The Complainant was therefore made aware via the privacy statement of how his personal data was going to be used by Microsoft, how it was processed and the security that Microsoft applied to users' personal data as well as the fact that Microsoft retained personal data "for as long as necessary" to provide certain products. The information provided in the privacy policy provided all of the relevant information required by Article 15(1) and 15(2) of the GDPR.

87. Whilst Microsoft outlined some of the actions that could potentially occur if a user were to violate the terms of service specified in the Microsoft Services Agreement, the policy did not specify the exact procedure that occurs if an account is locked, suspended, closed or deleted. Rather, the MSA just informs the user that, if the account is either closed by Microsoft or the user, the data will be deleted, or otherwise disassociated from the data subject and their account. It does not specify within what timeframe this action will be completed, or how a user may appeal a closure initiated unilaterally by Microsoft. Further, during the Complainant's interactions with the Microsoft customer service channel, the Complainant was never informed of the procedure that would occur following the suspension of his Microsoft account. He was not informed when engaging with customer service that his data would be deleted, nor was he informed of any timeframe in which his data would be deleted, or disassociated from his account. As noted in paragraph 21, Microsoft confirmed it had communicated to the data subject his access to his account had been suspended, and that for this reason, when the Complainant tried to gain access to his Microsoft account it appeared to just be suspended. However, the DPC notes the data associated with the account had actually been deleted, leading to confusion for the Complainant when he tried to regain access to what he believed was his suspended account which, in actuality, was a closed account.

88. For the reasons explained above, there was a lack of transparency in the information provided by Microsoft as regards the particular definitions of the terms "locked", "closed", "suspended" or "deleted". In addition, there was a lack of transparency to the Complainant in relation to the duration for which a user's data, where their account had been "closed" or "deleted", would be retained and then subsequently deleted irretrievably in line with a clear retention policy.

89. The DPC also recalls that the Complainant's data was erased by Microsoft on 28 February 2021, in circumstances where Microsoft had received an access request from him and where Microsoft had not complied with the requirements of Article 12(4) of the GDPR, as outlined above at paragraph 59 of this Decision. The DPC accordingly finds that the erasure of the Complainant's data took place a) despite a lack of clarity and transparency about whether the account was closed and the data scheduled for deletion, and b) in circumstances where the controller had failed to provide all of the required information in response to an access request. The deletion of the account data therefore lacked in the elements of lawfulness, fairness and transparency required under Article 5(1)(a) of the GDPR.

90. **Finding 2: On the basis of the above, the DPC finds that, in the specific circumstances of the Complaint, Microsoft infringed the lawfulness, fairness and transparency principle under Article 5(1)(a) of the GDPR in its handling of the Complainant's access request and in its decision to delete his data.**

Decision on infringements of the GDPR

91. Following this Inquiry into Microsoft Operations Ireland Limited, the DPC is of the opinion that Microsoft Operations Ireland Limited infringed the General Data Protection Regulation as follows:

- **Article 12(4)**

The DPC finds that, in the specific circumstances of this Complaint, Microsoft infringed Article 12(4) of the GDPR by failing to inform the Complainant of the possibility to lodge a complaint with a supervisory authority and to seek a judicial remedy, following his access request of 17 August 2020.

- **Article 5(1)(a)**

The DPC finds that, in the specific circumstances of the Complaint, Microsoft infringed the lawfulness, fairness and transparency principle under Article 5(1)(a) of the GDPR in its handling of the Complainant's access request and in its decision to delete his data.

Remedial measures undertaken by Microsoft

92. Microsoft has stated it is evaluating its process for data subject access requests relating to accounts suspended for similar violations of Microsoft's Services Agreement, including the potential preservation of data in accounts where data subject access requests are received. Microsoft stated it is evaluating the language used by Microsoft's customer services and privacy response teams to improve its existing procedures. Microsoft has also stated it has worked to improve its process in the provision of a designated appeals process.

Exercise of Corrective Power by the DPC

93. In deciding on the corrective powers that are to be exercised in respect of the infringement of the GDPR outlined above, I have had due regard to the Commission's power to impose administrative fines pursuant to Section 141 of the 2018 Act. In particular, I have considered the criteria set out in Article 83(2)(a) – (k) of the GDPR. When imposing corrective powers, I am obliged to select the measures that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures, for example re-establishing compliance with the GDPR or punishing unlawful behaviour (or both)[5]. I find that an administrative fine would not be necessary, proportionate or dissuasive in the particular circumstances in relation to the infringements of the Article of the GDPR as set out above.

94. **In light of the infringements identified above, the DPC hereby issues a reprimand to Microsoft Operations Ireland Limited, pursuant to Article 58(2)(b) of the GDPR.**
[Note: In a Decision of the DPC in the case of [redacted] an order was made with regard to the revision of Microsoft's internal policies and procedures as regards the information to be provided to data subjects pursuant to Article 12. The order in that Decision, when complied with by Microsoft, will prevent infringements of Article 12(4) occurring to data

[5] See the Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679', at page 11.

subjects in the future similar to those that occurred in this case. Accordingly, a further order is not now required in this Decision in respect of the Article 12(4) infringement.]

95. In light of the infringement of Article 5(1)(a) in the case of this data subject, I find it necessary that the controller bring its processing into compliance to prevent similar infringements occurring with regard to data subjects in the future in similar circumstances. Accordingly, the DPC proposes to order Microsoft to revise its policies and procedures as follows:

    i. to clarify in its user-facing policy documentation the retention policies regarding data associated with accounts that have been terminated by Microsoft due to infringement of Microsoft's Services Agreement.
    ii. to clarify the circumstances in which the data associated with an account is permanently deleted by Microsoft.
    iii. to outline in its user-facing policy documentation the appeal processes available to the account holder where Microsoft terminates the service due to an alleged infringement of the Terms of Service.

This order is made pursuant to the DPC's corrective powers under Article 58(2)(d) of the GDPR. Microsoft is requested to provide details of its proposals to revise its policy documentation to the DPC by 30 November 2025.

Judicial Remedies

96. In accordance with Article 78 of the GDPR, each natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. Pursuant to Section 105(5) of the Act, an appeal to the Irish Circuit Court or the Irish High Court may be taken by a data subject or any other person (this includes a data controller) affected by a legally binding decision of the DPC within 28 days of receipt of notification of such decision. An appeal may also be taken by a data controller within 28 days of receipt of notification; under Section 150(1) against the issuing of an enforcement notice and/or information notice by the DPC against the data controller; and under Section 142, against imposition upon it of an administrative fine by the DPC.

Signed:

Elizabeth Finn
Deputy Commissioner

On behalf of the Data Protection Commission