An Coimisiún um Chosaint Sonraí
Data Protection Commission

DPC Ref: [redacted]

DPC Complaint Ref: [redacted]

Date: 28 February 2024

Complainant: [redacted]

Data Controller: Apple Distribution International Limited (Apple)

RE: [redacted] V Apple

Decision

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 Mr [redacted] ("**Complainant**") against Apple Distribution International Limited ("**Apple**") to the Data Protection Commission, in its capacity as the lead supervisory authority ("LSA").

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, the DPC transmitted a Draft Decision in relation to the matter to the "supervisory authorities concerned". As Apple 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.

Complaint Handling by the DPC – Timeline and Summary

1. On 23 June 2021, the Complainant contacted the DPC and stated that Apple had "blocked" his Apple-ID associated with his Apple user account, and sought the DPC's assistance in getting it unblocked. The DPC advised the Complainant on 24 June 2021 that if his concern related to the processing of his personal data or if he wished to exercise his data protection rights, he should contact the controller's data protection officer in writing, and if he had already done so, to provide a copy of such correspondence to the DPC.

2. The Complainant (through his lawyer) made an access request on 8 July 2021 to Apple.

3. On 23 August 2021, the Complainant emailed the DPC, stating that Apple had not complied with the access request of 8 July 2021 within the allotted timeframe, but had ignored it. He then asked the DPC to enforce Apple to comply with his access request.

4. The DPC notified Apple of the Complaint by email on 20 October 2021 and raised queries in respect of Apple's obligations under Article 15 of the GDPR and provided a timeframe for a response to be received.

5. Apple responded on 3 November 2021 and provided the following answers to the queries raised by the DPC and also provided a copy of exchanges with the Complainant's lawyer up to this point.

   - It had responded to the Complainant's access request on 19 July 2021 and had explained to the Complainant how to access the data associated with the Apple ID via its online service.
   - Regarding blocking the account, this was a system security measure triggered most likely by an incorrect password entry (precise reason unconfirmed).
   - Apple had engaged extensively with the Complainant and his lawyer. The Complainant had been unable to satisfy Apple's verification process: he does not know the date of birth associated with the account and did not have access to the email address to which the reset emails were being sent.
   - Apple said in its response that it had an established process for verifying entitlement to exercise access to the data associated with an Apple ID, which it considered allowed it to satisfy the requirement for controllers to confirm the identity of the natural person in the circumstances outlined in Article 12(6), and to fulfil its security obligations under Article 32 of the GDPR.

     It stated: "*We note that this account is currently in what we refer to as a locked out state. Given the passage of time in this particular case, the logs related to the case have been deleted in accordance with our standard retention policy and so we cannot determine the precise reason for which the account was locked out. However, we can determine that this was not an action initiated by Apple but rather a system security measure triggered for security reasons, typically when a user inputs the incorrect password or other account information too many times. Other examples of security reasons for locking an account are when suspicious activity is detected on an account, possible spam abuse is detected, or unauthorised actions on our online service at privacy.apple.com occur.*

     We note that our Apple Support, Executive Relations and Privacy teams have all already engaged extensively with [the Complainant] *and with his lawyer in relation to his request to unlock his account. It is not the case that Apple has blocked the data subject's Apple ID without due cause, rather it is most likely that* [the Complainant's] *own action has resulted in the account being locked.* [The Complainant] *advised our Executive Relations team on 7 July 2021 that when attempting to answer security*

questions, he was prompted to confirm the date of birth set in the account, the expected date of birth was not accepted and that he was not able to proceed to complete verification. We note that [the Complainant] *confirmed to the Executive Relations team on that same day that he might have set an incorrect date of birth for the account and he does not recall which one.*
Although he also has the option to reset his password at appleid.apple.com, [the Complainant] *has advised the Executive Relations team that he has no access to the email address offered, and that there is no rescue email address added to the account.*

As you know, Apple has an established process for verifying entitlement to exercise access to the data associated with an Apple ID, which we consider allows us to satisfy the requirement for controllers to confirm the identity of the natural person in the circumstances outlined in Article 12(6) and to fulfil our security obligations under Article 32 of the GDPR.

Without us being confident that a person is the account owner, we cannot proceed with a request to provide access to the personal data associated with an Apple ID.

When a customer first registers with Apple, they must choose an Apple ID, i.e. their user name. Each Apple ID is assigned only once, so that all Apple IDs are unique. The Apple ID is the identifier that is assigned to a customer. The registration process is fully automated. In line with the principle of data minimisation, Apple does not require copies of an ID card or other official documents to verify that the name has been provided truthfully and correctly and that the registered person actually resides at the address provided by them. This is due to the fact that Apple in this context is not seeking to verify the identity of a customer, but solely to associate certain data to a specific customer by using an Apple ID.

As [the Complainant] *has not been able to satisfy our security requirements, we consider that he has not provided the information necessary to demonstrate his clear entitlement to access the data on the account in question. We would note that having a consistent, established and secure means to verify identity of our users is at the core of how we meet our GDPR security obligations in this respect.*

Allowing individual users to dictate the identity criteria that should or should not be used in specific cases, such as by accepting the name and ID linked to [the Complainant's] *account, would seriously undermine our ability to meet those security obligations. ...*

We are of course happy to assist [the Complainant] *to unlock his Apple ID. In this regard, we would suggest that* [the Complainant] *follows the steps at https://iforgot.apple.com, in order to reset his account.* [the Complainant] *may also be interested in our article titled "If your Apple ID has been locked or disabled", available at https://support.apple.com/en-ie/HT204106, and our article titled "If you*

have forgotten your Apple ID password", available at https:// support.apple.com/en-ie/HT201487.."

6. The DPC reverted to the Complainant on 3 December 2021 outlining Apple's position in order to attempt to amicably resolve the issue. On 31 December 2021, the Complainant's lawyer rejected this, stating that Apple's response was not satisfactory under Article 15 of the GDPR.

7. The DPC contacted Apple on 25 January 2022 asking for a list of information the Complainant would need to provide to Apple in order to have his account verified and access regained. Apple responded on 4 February 2022 and reiterated its position regarding the fact that ID is not required to set up an Apple ID. *"When a customer first registers with Apple, they must choose an Apple ID, i.e. their user name. Each Apple ID is assigned only once, so that all Apple IDs are unique. The Apple ID is the identifier that is assigned to a customer. The registration process is fully automated. In line with the principle of data minimisation, Apple does not require copies of an ID card or other official documents to verify that the name has been provided truthfully and correctly and that the registered person actually resides at the address provided by them. This is due to the fact that Apple in this context is not seeking to verify the identity of a customer, but solely to associate certain data to a specific customer by using an Apple ID. As we do not require copies of documents from users when they set up an Apple ID, there is no list of information which we can provide to your Office that* [the Complainant] *can in turn provide to us, in order for us to be able to verify his control over the account in question and so provide him with the personal data associated with that Apple ID. The way for* [the Complainant] *to access the personal data associated with the Apple ID in question is by logging in to the account based on the information he himself provided during account set up."*

8. The DPC outlined Apple's position in a letter to the Complainant on 17 February 2022 seeking to establish if the response might amicably resolve the issue. It outlined the fact that the only form of verification that Apple can accept is a user logging into an account using the information they provided when setting up their account. The response included links to policy documents from Apple that had previously been sent both to the DPC and to the Complainant. On 13 April 2022 the Complainant rejected the attempt at amicable resolution.

9. On 15 July 2022, the DPC wrote to Apple asking the following questions:

   - Please confirm to the DPC whether the Data Subject has two-factor authentication enabled on this account;

   - Please provide the DPC with the steps taken so far by Apple to verify the Data Subject's identity;

   - Please outline to the DPC, as per the requirements of Article 12(6) GDPR, the reasonable doubts Apple has concerning the identity of the Data Subject as the account holder of the account in question.

- Please provide the DPC with a copy of all pertinent correspondence that it has shared with the Data Subject, or their legal representative, in relation to the complaint, which may not have been previously provided to the DPC.

- With reference to the Data Subject's attached correspondence of 13 April 2022, please outline to the DPC why Apple believes that the Data Subject's credit card statements – showing a regular charge for the account in question – are not suitable to assist it in verifying the Data Subject's identity.

10. Apple responded to the DPC's letter on 15 August 2022, providing cases notes and also providing answers for the questions that the DPC posed in its letter of 15 July 2022.

- Apple stated that the Apple ID [redacted]@mac.com did not have [redacted] enabled on this account. It also did not have [redacted] set up.

- Apple stated that, as the DPC was aware, Apple had an established process for verifying entitlement of customers to exercise data subjects' rights. It referred in this regard to page 3 of a previous letter to the DPC in relation to this complaint, dated 3 November 2021, quoting as follows:

"Apple has an established process for verifying entitlement to exercise user data protection rights, which we consider allows us to satisfy the requirement for controllers to confirm the identity of the natural person in the circumstances outlined in Article 12(6) and to fulfil our security obligations under Article 32 of the GDPR. [...]"

After logging in to Data & Privacy Page at privacy.apple.com, a customer can manage their data, not only to request copies of the stored and processed data, but also to deactivate the account or delete the account. Without us being confident that a person is the account owner, we cannot proceed with a deletion request (or other data protection rights).

Where a customer cannot confirm control of an Apple ID to proceed with a data protection request, they can contact Apple Support who will try to assist that customer to progress through our verification process and recover access to their account.

In that instance, [the Complainant] has not been able to log into the relevant account and was not able to progress through the verification and security steps that would confirm his control of the Apple ID in question.

As evidenced by the case notes which we provide in response to your query (point 4 below), over several interactions from 4 May 2021 to 27 July 2021, Apple Support proceeded to assist the customer in several respects, highlighting the following:

i. *The customer could not remember his password, and was advised to visit https://iforgot.apple.com. However, the customer could not verify his control of the account due to his inability to access emails received on the email address registered with that account.*
ii. *The customer was provided with information on how to recover access to the account in particular through the articles "If you've forgotten the answers to your Apple ID security questions" and "How to use account recovery when you can't reset your Apple ID password" respectively available at https://support.apple.com/HT201485 and https://support.apple.com/HT204921.*
iii. *The customer could not reset the password on the account due to his inability to provide the date of birth registered on that account. Apple Support assisted the customer and confirmed to the customer that the birthday set on the account had never been edited, i.e. it is the date of birth that was entered when setting up the Apple ID.*

- *In the case at hand, it is not possible for Apple to determine whether this is a legitimate customer request or a malicious request from an unauthorised third party.*
Our reasonable doubts are due in particular to the following facts:

i. *The Apple ID has been locked because of security issues. For the reasons set out in page 2 of our aforementioned letter of 3 November 2021 to your Office, we are unable to confirm the specific reason for which the access was locked out. Unlocking the account requires a password reset.*
ii. *The Complainant has not been able to access emails sent to [redacted]@mac.com including emails that are automatically sent by Apple through https://iforgot.apple.com to request a password reset of the Apple ID. Also, the Apple ID account does not have a rescue email address set up.*
iii. *The Complainant has not been able to provide the date of birth registered on the account and thus has not been able to progress through the alternative password reset methods.*

We consider that in this respect, the Complainant has not provided the information necessary to demonstrate his clear entitlement to access or erase the data on the account in question.

We would also highlight that our security process would be extremely weakened if any person could access an account even if they don't have access to the email address on the account and are also unable to respond to basic questions such as the date of birth.

We would further note that we don't capture any alternative credentials by collecting documents such as passports, photo IDs or any other material when an individual creates an Apple ID, so there is no alternative system which is a source of truth that we can use to validate the Complainants [sic] *identity or his date of birth at this time, and we cannot do so in future without from our perspective requiring a disproportionate further collection of personal data from all users based on the possibility that they may in future forget the account details to access their account.*

- *We attach to this letter our case notes the Complainants* [sic] *queries in relation to verification and deletion of an Apple ID. As some of the information therein is in German, we are of course happy to provide your Office with a courtesy translation if you require it.*

- *The current reset methods for accounts with security questions do not incorporate any means to verify credit card charges. It is also clearly the case that credit card payments do not in any way indicate that a person is the account holder and therefore data subject of any personal data in an account. Such payments only convey the making of payments. The Complainant could be doing so on behalf of any other person.*

  Having a consistent, established and secure means to verify the control of accounts by users is at the core of how we meet our GDPR security obligations in this respect. With respect, allowing individual users to dictate the identity criteria that should or should not be used in specific cases would seriously undermine our ability to meet those security obligations...

  There is a risk that any departure from our verification processes would open the door to malicious actors trying to delete, or to obtain access to, someone else's account."

11. In its reply, Apple added: *"Access to this account would imply access to a significant portion of private information stored within, including but not limited to, calendar events, iCloud Drive data, iCloud Mail data, photos and videos, etc. We believe therefore that Apple cannot process the request of the Complainant without compromising the security of our process in light of the substantial high risks for data subjects if a third party gains access to the content available on the account."*

12. On 14 December 2022, the DPC wrote to Apple to inform it that it had not been possible to reach an amicable resolution to this complaint and that the DPC was obliged to comply with the requirements of Section 113(2) of the Act to make a Draft Decision under Article 60 of the GDPR.

13. The following issues remained unresolved at the conclusion of complaint handling:

i. Whether Apple's handling of the Complainant's access request of 8 July 2021 complied with Article 15 of the GDPR.
ii. Whether Apple complied with Article 12 of the GDPR in refusing to provide the Complainant with access to the personal data associated with the AppleID [redacted]@mac.com.

Conduct of Inquiry

14. The DPC commenced an Inquiry in relation to this matter by writing to Apple on 9 February 2023.

15. The DPC advised Apple that the Inquiry commenced by the Commencement Notice would seek to examine and assess whether Apple had complied with its obligations under the GDPR and the Act, in particular under Articles 12 and 15 of the GDPR in respect of the relevant processing operations, which are the subject matter of the complaint.

16. The DPC advised Apple that the scope of the Inquiry concerned an examination and assessment of the following:

- **Issue 1:** An examination of whether Apple's handling of the Complainant's access request was compliant with the GDPR and the Act.

- **Issue 2:** An examination as to whether Apple acted in accordance with Article 12(6) GDPR in handling the Complainant's request as regards its reasonable doubts concerning the identity of the Complainant.

17. The DPC asked a series of questions of Apple in respect of both Issue 1 and Issue 2. Apple responded to the DPC on 3 March 2023 with its submissions in response to the questions put by the DPC on 9 February 2023. Apple also provided exhibits in both English and German and also a copy of an email from the Complainant's solicitor in both German and English. The responses were as follows:

Issue 1:

- Apple stated that it received an access request from the Complainant, through his lawyer on 8 July 2021. Apple's submission included a copy of the email received.
- Apple stated that it responded to the access request on 19 July 2021, by email to the Complainant's lawyer and it included a copy of the email that issued.
- Apple's response was that it replied to the access request without delay.
- Apple provided an email exchange between itself and the Complainant's lawyer, dated 20 July 2021 and 21 July 2021. Copies of both emails were provided by Apple. In addition, Apple provided copies of interactions the Complainant had with it through

its Apple Support Team. This team attempted to assist the Complainant to verify his entitlement to obtain access to the Apple ID account [redacted]@mac.com.

- Apple stated in its response that it had not provided any personal data to the Complainant or his lawyer as the Complainant *"has been unable to progress through the security steps required to access an account". "Apple did provide responses to the informational aspects of* [the Complainant's] *request in compliance with Articles 15(1) and (2) GDPR in its email of 19 July 2021 by directing [the Complainant] to our page outlining how Apple uses personal data, which is available at https://privacy.apple.com/data/privacyinfo, as well as to Apple's Privacy Policy at https://www.apple.com/legal/privacy/en-ww/. These pages describe the purposes of collecting personal data, the types of information we collect, the circumstance in which we share user data, the basis on which we assess retention periods for personal information, details of measures in place to legitimise international transfers and confirmation that we do not take any decision involving algorithms or profiling that produces legal effects on end users".*

Issue 2:

- Apple stated that the Complainant's initial complaint was that the Apple ID account, which the Complainant claimed his personal data was associated with, was disabled and that he was unable to unlock it. Apple stated it *"has an established process for ensuring account security, and for verifying entitlement to exercise access to the data associated with an Apple ID, which we consider allows us to satisfy the requirement for controllers to both confirm the identity of the natural person in the circumstances outlined in Article 12(6) GDPR and to fulfil our security obligations under Article 32 GDPR".*

    - Apple's response added: *"After logging in to our Data & Privacy Page at https://privacy.apple.com/ , a customer can manage their data, not only to request copies of the stored and processed data, but also to deactivate the account or delete the account.*

    - *However, typically when a user inputs the incorrect password or other account information too many times, or otherwise where suspicious activity is detected on an account, possible spam abuse is detected, or unauthorised actions on our online service at https://privacy.apple.com/ occur, system security measures may be triggered for security reasons and lock an account.*

    - *Without us being confident that a person is the account owner, we cannot proceed with an access request (or other data protection rights).*

    - *A situation where an individual indicates that an account is locked, that they cannot access the account and appear unable or unwilling to take the straightforward steps that we have provided to retrieve access to the account, is precisely one where we consider that adopting a cautious approach to such*

a significant event as providing access to an account is fully warranted and is, in fact, expected under the GDPR.

- *As noted in our aforementioned letter to your Office of 3 November 2021 in relation to this complaint, the account that* [the Complainant] *seeks access to, is in what we refer to as a 'locked out' state. The precise reason for which the account was locked out cannot be determined due to the related logs having been deleted in accordance with our standard retention policy before we received the complaint filed under the reference* [redacted] *however, we can determine that this was not an action initiated by Apple but rather a system security measure triggered for security reasons as described above.*

- *We note that our Apple Support, Executive Relations and Privacy teams have all engaged extensively with* [the Complainant] *and with his lawyer in relation to his request to unlock this account. It is not the case that Apple has blocked the relevant Apple ID without due cause, rather it is most likely that* [the Complainant's] *own actions have resulted in the account being locked.* [the Complainant] *advised our Executive Relations team on 7 July 2021 that when attempting to answer security questions set on the account, the date of birth he supplied did not match the one supplied when setting up the account and so he was not able to proceed to complete verification. We note that* [the Complainant] *confirmed to the Executive Relations team on that same day that he might have set an incorrect date of birth for the account and he does not recall which one. Although he also has the option to reset his password at https://privacy.apple.com/ ,* [the Complainant] *has advised the Executive Relations team that he has no access to the email address offered, and that there is no rescue email address added to the account."*

- Apple further stated that the email address associated with the Complainant did not have two-factor authentication enabled. As the Complainant was unable to progress through the security steps to verify control of the account in question, Apple considered that he had not demonstrated clear entitlement to access the account data. Apple stated that *"having a consistent, established and secure means to verify the entitlement of our users to exercise data protection rights is at the core of how we meet our GDPR security obligations in this respect"*.

- Apple outlined that when a customer contacts it in regards to a data protection request and they cannot confirm control of an Apple ID, they can contact Apple Support, who will try to assist the customer to progress through the security steps and verification process to recover access to their account. Apple stated that it is *"unable to take any action on the user's account, as changes are required to come from users, and not Apple, for logging and security purposes"*.

- It added: *"When a customer first registers with Apple, they must choose an Apple ID, which is their user name. Each Apple ID is assigned only once, so that all Apple IDs are unique. The Apple ID is the identifier that is assigned to a customer. The registration process is fully automated. In line with the principle of data minimisation, Apple does not require copies of an ID card or other official document to verify that the name, or the date of birth, has been provided truthfully and correctly, and that the registered person actually resides at the address provided by them. This is due to the fact that Apple in this context is not seeking to verify the identity of a customer, but solely to associate certain data to a specific customer using an Apple ID. We also don't capture any alternative credentials by collecting documents such as passports, photo IDs or any other material when an individual logs in with an Apple ID, so there is no alternative system which is a source of truth that we can use to validate* [the Complainant's] *identity or his date of birth at this time, and we cannot do so in future without from our perspective requiring a disproportionate further collection of personal data from all users based on the possibility that they may in future forget the account details to access their account."*

Apple stated that its reset methods for accounts with security questions did not incorporate any means to verify credit card charges. Apple stated that a credit card payment did not in any way indicate that a person was the account holder and, therefore, the data subject of any personal data in the account. Apple stated that such statements only conveyed the making of payments and used the example of a person paying on behalf of any other person, such as an estranged spouse.

Apple provided case notes to the DPC of its interactions with the Complainant on 3 and 4 May 2021, and 10, 19 and 24 June 2021 to assist him in trying to access his account or with related queries. The Complainant was provided with links to Apple's support pages to assist in accessing the account. Apple stated it assisted the Complainant in attempting to regain access through https://iforgot.apple.com. However, the Complainant could not verify control of the account due to his inability to access emails received on the email address registered with that account. The Complainant was also provided with links to Apple web pages titled *"If you've forgotten the answers to your Apple ID security questions"* and *"How to use account recovery when you can't reset your Apple ID password"*. It reiterated that the Complainant could not reset the password on the account due to his inability to provide the date of birth registered on that account.

In emails on 19 and 21 July 2021 Apple further directed the Complainant to the iforgot link. Apple noted that on 3 November 2021 it had provided further suggestions to assist the Complainant via correspondence to the DPC, as part of its efforts to come to amicable resolution. These suggestions included links to the same support pages listed above, to assist a person who had become locked out of their Apple ID account or forgotten their password.

- Apple stated that the Complainant had not been able to log into the relevant account and had not able to progress through the verification and security steps that would confirm control of the account in question. Therefore he had not demonstrated his clear entitlement to access the data on the account due to facts provided to the DPC as follows:

    - The Apple ID in question was locked out due to security issues. Apple could not confirm the specific reason why the account was locked out, however, it said it was most likely that the Complainant's own actions, such as inputting an incorrect password too many times, could have caused the account to lock. It said that in such situations, a password reset was required to unlock an account.

    - The Complainant had not been able to access emails associated with the Apple ID in question, and as a result he had been unable to access the emails that automatically issue through the process on https://iforgot.apple.com. Apple also pointed out that the email associated with the Apple ID did not have a rescue email address set up (i.e. a second email address to assist with account recovery in the event that a user could not access the main email address associated with their account).

    - Apple further stated that the Complainant had not been able to provide the date of birth that was registered with the account in question and as a result had not been able to progress through the alternative password reset methods.

Apple stated that, without the Complainant being able to complete the standard verification process in order to access his Apple ID account, Apple was not in a position to allow the Complainant to access the account in question without seriously undermining its legal obligations as a data controller. Apple also outlined that providing access to an account where it was concerned about the possibility that a request was malicious would breach its obligations under Articles 12 and 32 of GDPR. It further stated that its security process would be extremely weakened if any person could access an account without access to the email address associated with it and were also unable to answer basic questions such as date of birth. It stated: *"To do so would mean providing access to the personal data on an account based on a claim of one person without a clear means of verifying that the request is not in fact malicious."*

- Apple stated it appeared that the issue lay with the Complainant being unable to input the password set on the account, not remembering the date of birth entered when the account was created, not having access to the emails sent to the address associated with the account and not having set up a recovery email (i.e. a second email address to assist with account recovery in the event

that a user could not access the main email address associated with their account).

- It further stated that it was the customer's responsibility to ensure that the date of birth entered is correct, or at least one that they remember, and to keep their passwords secure.

Apple said that logs relating to the case had been deleted in accordance with Apple's standard retention policy so it could not be certain of the precise basis that the account was locked out. However, the Complainant's engagements with Apple Support regarding the inaccurate date of birth set on this account were consistent with the account being locked out because of incorrect information being input by the customer. Apple stated that if a customer is unable to confirm control of an Apple ID to proceed with a data protection request, they could contact Apple Support, who will then try to assist the customer to progress through the verification process and recover access to their account. The Complainant was not able to log into the account in question nor was he able to proceed through the verification and security steps that would confirm his control of the Apple ID. Apple said that, in such cases, it was not possible for Apple to determine whether this was a legitimate customer request or a malicious request from an unauthorised third party. Apple said it believed that it could not process the Complainant's request without compromising the security of its process in light of the substantial high risks for data subjects if a third party were to gain access to content available on an account.

18. The Complainant was issued with a Commencement Notice by the DPC on 9 February 2023 and given an opportunity to respond by 3 March 2023. On 1 March 2023 he contacted the DPC seeking an extension of time. An extension was granted until 10 March 2023.

19. On 1 March 2023 the Complainant submitted documentation to the DPC in response to the Commencement Notice of 9 February 2023. This was followed up on 10 March 2023 by a further email from his lawyer to confirm that this was the submission in its entirety. The extra documentation from the Complainant was provided in the form of credit card statements that cover a 5-month time period and show monthly payments to Apple, and a document signed by a notary public which purported to confirm that the Complainant was in possession of the iPhone and MacBook associated with the Apple ID.

20. Based on the submission received from the Complainant, the DPC elected to ask some further questions of Apple to assist with the inquiry. On 24 April 2023, the DPC wrote to Apple with a series of questions. Apple provided its response to the additional questions to the DPC on 18 May 2023.

- [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Apple, at this point, stated it was open to attempting amicable resolution again with the Complainant due to information provided in the DPC's letter of 24 April 2023. Apple stated in its letter of 18 May 2023 that it would not contact the Complainant directly unless the DPC was amenable to it. The DPC informed Apple that it was in favour of Apple's proposal and the DPC informed Apple that it had contacted the Complainant to inform him that Apple would make contact directly.

21. On 19 May 2023, the DPC wrote to the Complainant and informed him that a Senior Apple Care Specialist would contact him directly in order to guide him through an alternative method to access his account. The DPC also wrote to Apple on 19 May 2023 requesting that it inform the DPC once this contact had taken place whether the process had resulted in the Complainant regaining access to his account.

22. On 1 June 2023, Apple wrote to the DPC with an update on the process it undertook with the Complainant to try to assist him to restore his account. Apple stated that [redacted] on 22 May 2023 and that, despite its best efforts, it was unable to restore access to the Complainant's account. Apple undertook the following steps with the Complainant.

- [redacted] When attempting this, the Complainant was faced with two warnings that prevented access. The first instruction was that two-factor authentication had to be set up; this was not possible as the password was not accepted. The second was the account was blocked, the password was not accepted and he was unable to reset it.

- Apple had also hoped that it could activate the iCloud account [redacted] associated with the AppleID, but this option was not available.

23. To conclude the letter of 1 June 2023, Apple stated that it returned to its conclusion of 18 May 2023: *"It is a user's responsibility to ensure they input the correct information when creating an account. The most likely explanation for the account lock out is* [the Complainant] *inputting his own date of birth incorrectly. He did not set up two factor authentication, a trusted number or a recovery key, all of which would have provided a path to enable him to regain access."* Apple also stated that it had exhausted all standard procedures to resolve the issue and that it hoped that the attempts it made were evidence of its commitment to attempt to find amicable resolution to issues such as this.

24. The Complainant was advised on 12 June 2023 that the DPC would proceed to prepare a Draft Decision, which would be provided to him in due course.

Notification of Preliminary Draft Decision to the Controller

25. The DPC provided Apple with a copy of the Preliminary Draft Decision on 29 November 2023 and requested that it provide by 15 December 2023 any final submissions which it wished the DPC to consider when completing its Draft Decision.

26. Apple provided a response on 11 December 2023 and advised the DPC that it had no substantive submissions to make in regard to the Preliminary Draft Decision. However, Apple requested that its responses to the DPC of 18 May 2023, outlined at paragraph 20 of this Decision, be redacted as the complainant had not demonstrated his right to access this confidential account information. Apple stated that it did not object to these responses being shared with the concerned supervisory authorities.

27. The DPC carefully considered Apple's response to the Preliminary Draft Decision and, in that regard, when issuing the Preliminary Draft Decision to the Complainant, the DPC acceded to Apple's request not to share with him certain information included at Paragraph 20 (above). Similarly, the DPC intends to equally accede to Apple's request to exclude this information when this Decision is provided to the Complainant.

Notification of Preliminary Draft Decision to the Complainant

28. The DPC provided the Complainant (via his lawyer) with the Preliminary Draft Decision on 19 December 2023, inviting the Complainant to make any final submissions by 5 January 2024. No acknowledgement of the DPC's correspondence and no submissions in relation to the Preliminary Draft Decision were received by the deadline. On 8 January 2024, the DPC issued further communication to the Complainant (via his lawyer), noting that the deadline for final

submissions had now passed and that no submissions had been received. The DPC stated that it would prepare a Draft Decision pursuant to Article 60 of the GDPR forthwith.

Relevant and Reasoned Objections and Comments from "supervisory authorities concerned"

29. Having transmitted the Draft Decision on 16 January 2024 to the "supervisory authorities concerned" in accordance with Article 60(3) of the GDPR, the DPC did not subsequently receive any relevant or reasoned objections. Comments were received from two supervisory authorities (Berlin and Hungary). Both questioned the necessity for the DPC's examination in the Draft Decision of Apple's Privacy Policy under Articles 15(1) and (2) of the GDPR. The DPC responded to the comments with clarification on why the examination of the Privacy Policy took place, including clarifying that in this specific case the Complainant had explicitly requested that Apple provide him with all elements of the information requirements in Article 15. No further comments were received.

Applicable Law

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

    - Article 12
    - Article 15

Analysis and Findings of Inquiry

31. **When the DPC issued a Commencement Notice to Apple on 9 February 2023, Apple was informed that there were two issues to be examined. For the purposes of this Decision, the issues are so closely linked, that the DPC proposes to analyse them below together.**

Issue 1: An examination of whether Apple's handling of the Complainant's access request was compliant with Article 12 and Article 15 of the GDPR.

32. In accordance with Article 15 GDPR, a data subject has the right to obtain from the data controller a copy of the personal data undergoing processing, and certain additional information concerning the processing and the data subject's rights as prescribed by Articles 15(1)(a) to (h), and Article 15(2) of the GDPR. The scope of the personal data to be provided under Article 15(1) GDPR comprises full and complete information on all data relating to the data subject undergoing processing in order for the data subject to be aware of, and to verify the lawfulness of the processing.

33. Article 12 of the GDPR sets out the requirements for transparent information, communication and modalities for the exercise of the rights of the data subject. This information should be in clear and plain language and be easy to access. Action taken on requests under Articles 15 to

22 shall be provided without undue delay within one month of the receipt of the request. Under Article 12(6), if a controller has reasonable doubts concerning the identity of the data subject the controller may request the provision of additional information necessary to confirm the identity of the data subject.

34. The Complainant submitted an access request under Article 15 of the GDPR through his lawyer on 8 July 2021 via registered post and email. In his email of 23 August 2021 to the DPC, he stated that Apple had not complied with the request, and he felt that it had ignored it. The copy of the Complainant's request to Apple was provided in German, but a translated copy was provided on 25 August 2021 after the DPC made a request for an English language version.

    In the course of the inquiry, the DPC wrote to Apple on 9 February 2023 and asked it to confirm the date it received the access request and the date it responded to the request. Apple provided copies of emails to the DPC showing the initial communication and an email exchange with the Complainant's lawyer.

35. The correspondence shows that the Complainant's solicitor made an access request on his behalf on 8 July 2021 to which Apple replied on 19 July 2021, with a further response on 21 July 2021.

    The DPC notes that Apple has not provided a copy of any data, including any personal data, associated with the Complainant's AppleID to the Complainant or his lawyer due to the fact the Complainant has not been able to progress through the security steps it has in place to confirm his entitlement to access the relevant Apple ID account. Apple, however, provided the Complainant with information on the informational aspects of the access request of 8 July 2021, such as how it uses personal data, and links to Apple's Privacy Policy and its Data and Privacy page.

36. The DPC also notes that Apple outlined the following to the Complainant in its email of 19 July 2021: *"Logging in to that service is a key step in ensuring our customers account security. I would highlight our web page at https:// iforgot.apple.com should your client need to recover access to his account.*

    You will appreciate that under the GDPR (Regulation 2016/679), Apple has a legal obligation to protect customer personal data and thus to take reasonable steps to verify the identity of an account holder before deletion of or access to an account. It is a matter for each data controller, in the first instance, to put in place the security measures that it considers appropriate. Without having verified that an individual is actually the account owner, we cannot proceed with such a request (or other data protection rights). We would note that having a consistent, established and secure means to verify identity of our users is at the core of how we meet our GDPR security obligations in this respect. A situation where an account holder indicates that they cannot access their account and appears unable or unwilling to take the easy steps that we have provided to retrieve access to their account is precisely the

situation where we are required to adopt an even more cautious approach to ensure it does not lead to wrongful access to or wrongful deletion of an account."

37. The Complainant's solicitor responded to Apple on 20 July 2021 outlining the reasons why, under both Articles 12(3) and 15 of the GDPR, his client's request to access his data should be processed and the information provided to him in writing. He suggested that, alternatively, that the Complainant be sent a link to reset his password, and that the link also be sent to the solicitor.

38. On 21 July 2021, Apple responded again to the Complainant's solicitor, referring back to its previous email and providing a link to an Apple support page containing further information regarding what data the Complainant could request a copy of by logging in to their account.

    The page provided clear information in relation to the data associated with an Apple ID and about what information was available to a data subject: *"Any data that isn't provided is either in a form that is not personally identifiable or linked to your Apple ID, is stored in an end-to-end encrypted format that Apple cannot decrypt, or is not stored by Apple at all. Additionally, some data may have been held only for a very short time and is no longer on our servers."*

    Apple's response also stated the following; *"The Irish Data Protection Commission deals with complaints from individuals who are unhappy with final responses which they have received from controllers in relation to formal data requests for access/rectification/deletion. You can find further information on this under: https://www.dataprotection.ie"* Apple also provided the following link: https://edpb.europa.eu/about-edpb/board/members_en, which lists the contact details for each national Supervisory Authority. Apple also noted that its processing of personal data was subject to the provisions of the Data Protection Act 2018 and the GDPR and provided a link to the Act, which includes the provisions outlining the right to a judicial remedy.

39. On 22 July 2021, the Complaint's lawyer responded to Apple outlining that his client's Apple ID was blocked and he could not access his data at https://privacy.apple.com and that unblocking the account via https://iforgot.apple.com was not possible. [redacted]

40. As already outlined, Apple provided documentation to the DPC in its response to the Commencement of Inquiry notice that showed that it responded to the access request of 8 July 2021 on 19 July 2021. Apple also further engaged with the Complainant's lawyer regarding the issues around the account being locked and unable to be accessed by the Complainant.

Based on the information provided to the DPC in this Inquiry, the DPC is therefore satisfied that Apple complied with Article 12(4) GDPR in its response to the Complainant's access request. It provided the Complainant with links to the Act, the DPC's website, and a list of

Supervisory Authorities in the EEA to assist him. It provided this information within one month of the Complainant's access request.

Article 15 information provided in Apple's Privacy Policy and related pages

41. As outlined at paragraph 17, Apple confirmed during this Inquiry that it did not provide a copy of any personal data to the complainant on foot of his access request, as he *"has been unable to progress through the security steps required to access an account"*. However, it stated that it did provide responses to the informational aspects of the Complainant's request in compliance with Articles 15(1) and 15(2) GDPR in its email of 19 July 2021. On that date, Apple provided the Complainant, through his lawyer, a link to its Data and Privacy page[1] and its Privacy Policy page[2] (which was in any case linked from the Data and Privacy page). These documents outline, amongst other matters, the purposes for which Apple processes personal data.

42. For the purposes of this Decision, the DPC has accessed archived versions of the documents on the Internet Archive to reflect the policy extant at the time of the complaint. The URL examined for the Privacy Policy was Legal - Apple Privacy Policy - Apple (archive.org)[3] and the URL examined for the Data and Privacy page was Data & Privacy (archive.org)[4].

43. The information provided at the links sent to the Complainant did not specifically refer to the GDPR. However, analysing the information provided against the requirements of Article 15, the following information was provided:

Article 15(1)(a)

i. ***"What are the purposes of processing your data?***

- *To keep you posted on Apple's latest product announcements, software updates, and upcoming events.*
- *To help us create, develop, operate, deliver, and improve our products, services, content and advertising, and for loss prevention and anti-fraud purposes.*
- *To verify identity, assist with identification of users, and to determine appropriate services. For example, we may use date of birth to determine the age of Apple ID account holders.*
- *To send important notices, such as communications about purchases and changes to our terms, conditions, and policies.*

[1] https://privacy.apple.com/data/privacyinfo

[2] https://www.apple.com/legal/privacy/en-ww/

[3] web.archive.org/web/20210719074933/https:/www.apple.com/legal/privacy/en-ww/

[4] http://web.archive.org/web/20210416150220/https:/privacy.apple.com/data/privacyinfo

- *For internal purposes such as auditing, data analysis, and research to improve Apple's products, services, and customer communications.*

- *To administer sweepstakes, contests or similar promotions if you enter into them."*

Apple's Privacy Policy, which was also linked from the Data & Privacy page and provided in a link sent to the Complainant, provided further details about Apple's processing of personal data. In a section headed 'Apple's Use of Personal Data', the policy stated: *"Apple uses personal data to power our services, to process your transactions, to communicate with you, for security and fraud prevention, and to comply with law. We may also use personal data for other purposes with your consent."*

The policy went on to outline the purposes in greater detail.

The DPC is satisfied that the information provided fulfilled the requirements set out in Article 15(1)(a) of the GDPR.

Article 15(1)(b)

ii. On the Data & Privacy page, Apple provided a list of the categories of personal data that it processes, which are listed below:

"What types of personal information do we collect?

- *Name, address, phone number, email address, device identifiers, IP address, location information and credit/debit card information may be collected when you interact with us in one of many ways such as create an Apple ID, apply for commercial credit, purchase a product, connect to our services, download a software update, contact us or participate in an online survey.*

- *In certain jurisdictions, we may ask for a government issued ID in limited circumstances including for the purpose of extending commercial credit, managing reservations, or as required by law."*

Apple's Privacy Policy also provided additional information about the categories of personal data processed by Apple.

In a section headed 'Personal Data Apple Collects from You', Apple provided further extensive information about the categories of personal data it processes, including device information, payment information, usage data, health information, fitness information and other information provided by data subjects. Apple also described in detail the personal data it receives from other sources under a separate heading. This included information collected from Apple Partners.

The DPC is satisfied that the information provided satisfied the requirements set out in Article 15(1)b) of the GDPR.

Article 15(1)(c)

iii. A section on the Data and Privacy page specifically dealt with the sharing of information with third parties:

"Do we share your data with third parties?

- *Apple may share personal information with companies who provide services such as information processing, extending credit, fulfilling customer orders, delivering products to you, managing and enhancing customer data, providing customer service, assessing your interest in our products and services, and conducting customer research or satisfaction surveys.*
- *It may be necessary – by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence – for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.*
- *We may also disclose information about you if we determine that disclosure is reasonably necessary to enforce our terms and conditions or protect our operations or users. Additionally, in the event of a reorganization, merger, or sale we may transfer any and all personal information we collect to the relevant third party.*
- *These recipients, which include other Apple companies and its affiliates who are in all cases obligated to protect your personal data. They may be located outside the region in which you are a resident."*

Further information was provided in the full Privacy Policy document under the heading 'Apple's Sharing of Personal Data. This included information on Apple's sharing with Services Providers, Partners and Others, as a general description of the categories of third party with whom personal data was shared.

a. The DPC notes that, in a ruling on 9 June 2023, the Court of Justice of the European Union answered a question referred for a preliminary ruling by the Austrian Supreme Court regarding a controller's obligations under Article 15(1)(c) of the GDPR. The judgment stated as follows: "[Article 15(1)(c)] *must be interpreted as meaning that the data subject's right of access, provided for therein, must necessarily extend, where the data subject so requests, to the identification of the specific recipients to whom his or her personal data are disclosed. That right of access may be restricted to an indication of the categories of recipient where it is materially impossible to identify the specific recipients to whom the personal data of the data subject are disclosed or where the data controller demonstrates that the data subject's requests are*

manifestly unfounded or excessive, within the meaning of Article 12(5) of Regulation 2016/679."

While Apple's Privacy Policy on the date it was provided to the Complainant did not name the specific recipients to whom personal data had been, or would be, disclosed, the DPC makes no finding of an infringement in relation to Article 15(1)(c). While the specific recipients of personal data may have been known by Apple as of the date of the Complainant's access request, the requirement that the controller go beyond merely disclosing "categories" of recipient had not at that date been clarified by the CJEU. The DPC is therefore satisfied that the information provided to the Complainant was aligned with the requirements of Article 15(1)(c) as understood as of that date.

Article 15(1)(d)

iv. On 19 July 2021 in the Data and Privacy link provided by Apple to the Complainant there was information regarding the retention of personal data by Apple. The policy stated as follows:

"How long do we retain your personal information?

We only retain personal data for the period necessary to fulfill the purposes outlined above and detailed in our service specific privacy summaries. When assessing this period we carefully examine our need to collect personal data in the first instance and if we establish such a need we then ensure that we only retain it for the shortest possible permit unless a longer retention period is required by law, such as for example retaining records of financial transactions."

The information in the full Privacy Policy contained additional information regarding the retention of personal data as follows:

"Apple retains personal data only for so long as necessary to fulfill the purposes for which it was collected, including as described in this Privacy Policy or in our service-specific privacy notices, or as required by law. We will retain your personal data for the period necessary to fulfill the purposes outlined in this Privacy Policy and our service-specific privacy summaries. When assessing retention periods, we first carefully examine whether it is necessary to retain the personal data collected and, if retention is required, work to retain the personal data for the shortest possible period permissible under law."

The DPC is satisfied that the information provided satisfied the requirements set out in Article 15(1)(d) of the GDPR.

Article 15(1)(e)

v. Apple also provided in the link sent to the Complainant on 19 July 2021 information on the right to request from the controller rectification or erasure of personal data. The text is as follows:

"How do I correct or delete my personal information?

You can help ensure that your contact information and preferences are accurate, complete, and up to date by logging in to your account at https://appleid.apple.com/. For other personal information we hold, we will correct the data if it is inaccurate. Requests can be made through the regional Privacy Contact Form."

In relation to the right to restrict the processing of personal data, Apple's Privacy Policy as provided to the Complainant referred to the right of restriction in the first line under the heading 'Your Privacy Rights at Apple'.

The information stated: "*At Apple, we respect your ability to know, access, correct, transfer, restrict the processing of* [emphasis added], *and delete your personal data.*"

This page also provided a link to the privacy.apple.com portal for data subjects to sign in with their Apple ID to exercise their "privacy rights and choices".

The DPC is satisfied that the information provided satisfied the requirements set out under Article 15(1)(e) of the GDPR.

Article 15(1)(f)

vi. The Data and Privacy page provided information on data subjects' right to lodge a complaint with a supervisory authority. It stated as follows:

"How do I provide feedback or register a complaint?

If you are not satisfied with any aspect of our handling of personal information or how we have endeavored to provide you with your privacy rights as determined by applicable law, you may have depending on your jurisdiction of residence the right to lodge a complaint with the relevant supervisory authority. We are happy to further advise through our regional Privacy Contact Form."

The Privacy Policy also set out in detail how an individual could make a complaint to Apple, and how if they were not satisfied they may refer their complaint "*to the applicable regulator*". It added: "*If you ask us, we will endeavour to provide you with information about relevant complaint avenues which may be applicable to your circumstances.*"

In the email to the Complainant's lawyer dated 21 July 2021, Apple provided further information on how to lodge a complaint with a supervisory authority. It also provided a link to the Act and a link to a full list of supervisory authorities within the EEA.

The DPC is satisfied that the information provided met the requirements set out under Article 15(1)(f) of the GDPR.

Article 15(1)(g)

vii. In regards to Article 15(1)(g), the Data and Privacy page provided information regarding personal data that was not collected directly from a user. It read as follows:

"Is any of my personal data stored by Apple not collected directly from me?

We may have received your personal data from other persons if someone has shared their content with you using Apple products, sent gift certificates and products, or invited you to participate in Apple services or forums."

The Privacy Policy provided went into more depth regarding personal data that Apple receives from other sources. It states as follows:

"Personal Data Apple Receives from Other Sources

*Apple may receive personal data about you from other **individuals**, from businesses or third parties acting **at your** direction, from our **partners** who work with us to provide our products and services and assist us in security and fraud prevention, and from other lawful sources.*

• ***Individuals.** Apple may collect data about you from other individuals — for example, if that individual has sent you a product or gift card, invited you to participate in an Apple service or forum, or shared content with you.*

• ***At Your Direction.** You may direct other individuals or third parties to share data with Apple. For example, you may direct your mobile carrier to share data about your carrier account with Apple for account activation, or for your loyalty program to share information about your participation so that you can earn rewards for Apple purchases.*

• ***Apple Partners.** We may also validate the information you provide — for example, when creating an Apple ID, with a third party for security, and for fraud-prevention purposes.*

For research and development purposes, we may use datasets such as those that contain images, voices, or other data that could be associated with an identifiable person. When acquiring such datasets, we do so in accordance with applicable law, including law in the jurisdiction in which the dataset is hosted. When using such

datasets for research and development, we do not attempt to reidentify individuals who may appear therein".

The DPC is satisfied that the information provided satisfied the requirements set out under Article 15 (1)(g) of the GDPR.

Article 15(1)(h)

viii. In regards to automated decision-making, again, in the link provided by Apple on 19 July 2021 to the Data and Privacy page, information was provided regarding automated decision-making including profiling as follows:

"The existence of automated decision-making, including profiling:

Apple does not believe that it takes any decisions involving the use of algorithms or profiling that produces legal effects concerning you or similarly significantly affects you."

The Privacy Policy provided the following further information: *"Apple does not use algorithms or profiling to make any decision that would significantly affect you without the opportunity for human review."*

The DPC is satisfied that the information provided to the Complainant following his access request set out Apple's understanding as of that date that it met the requirements set out under Article 15 (1)(h) of the GDPR.

Article 15(2)

ix. Apple's Privacy Policy, which was updated on 1 June 2021 and provided to the Complainant following his access request, makes reference to the transfer of personal data between countries. Apple stated that it *"complies with laws on the transfer of personal data between countries to help ensure your data is protected, wherever it may be".* It further states: *"Personal data relating to individuals in the European Economic Area, the United Kingdom, and Switzerland is controlled by Apple Distribution International Limited in Ireland. Apple's international transfer of personal data collected in the European Economic Area, the United Kingdom, and Switzerland is governed by* Standard Contractual Clauses.[5]*"*

The DPC is satisfied that the information provided met the requirements set out under Article 15(2) of the GDPR.

[5] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

44. As outlined above, the information required under Article 15(1) and 15(2) was provided by Apple on 19 July 2021 and 21 July 2021 on foot of the Complainant's request. The information provided in the emails from Apple to the Complainant's solicitor, and the information set out on the relevant web pages, including the Privacy Policy and the Data and Privacy page, was, in the DPC's opinion, concise, transparent, intelligible and easily accessible, meeting the requirements of Article 12(1) of the GDPR.

Identification requirements: Article 12(6) and the right to obtain "a copy" under Article 15(3)

45. As already outlined, Apple did not provide the complainant with "a copy" of the personal data undergoing processing, in fulfilment of the requirements of Article 15(3) of the GDPR. This included the entirety of the data saved in the AppleID account bearing the handle [redacted]@mac.com. Apple's explanations for this refusal centred on the fact that the only criteria acceptable in order for the Complainant to satisfy the identification requirements were that he provide the correct authentication criteria when logging in. The Complainant was unable to do this.

46. From the communications provided by Apple, the DPC notes that Apple believes that the Complainant has not demonstrated a clear entitlement to access the account in question because:
    - The Apple account is in a locked out state due to security issues. Apple cannot confirm why the account is locked but it surmises that it is because the Complainant attempted to access using an incorrect password too many times, causing the account to lock and it requires a password reset to unlock it.
    - The Complainant has not been able to access the automated emails from https://iforgot.apple.com that would allow a password reset of the AppleID associated with the Complainant. Also, Apple stated that the Complainant had not set up a rescue email address.
    - The Complainant has not been able to provide the date of birth registered on the account in question and therefore cannot progress through the alternate methods for resetting a password.

47. Article 12(6) of the GDPR provides that, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

48. Recital 57 of the GDPR Act states : *"If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.*

However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights."

The Recital goes on to state: *"Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller."*

49. Returning to the provision of Article 12(6), Apple's responses in the course of the complaint-handling process and during this Inquiry clarified that it does not seek to verify a data subject's real identity when they set up an Apple ID. It only seeks to verify that they can provide the correct authentication, i.e. a password, a date of birth and/or the answer to security questions, in order to allow them to access their account on each occasion that they log in.

50. Apple customers set a password and provide a date of birth when registering an account and the correct input of the same credentials at each subsequent login verifies the right of access to an account.

As outlined to the DPC in the course of the inquiry[6], Apple does not capture any alternative credentials by collecting documents such as passports, photo IDs or any other material when an individual logs in with an Apple ID. It stated that there is *"no alternative system which is a source of truth"* that it can use to validate the Complainant's identity or his date of birth at this time. It further stated that it cannot do so in future without, from its perspective, requiring *"a disproportionate further collection of personal data from all users based on the possibility that they may in future forget the account details to access their account"*.

51. As regards the provision in Article 12(6) that the Controller may request the provision of additional information necessary to confirm the identity of the data subject, Apple did not in fact request, or accept, the additional material proffered by the Complainant in order to verify his identity. This included credit card statements and a signed affidavit from a notary public that he was in possession of two Apple devices. Apple did not accept this additional information because this information could not have provided the necessary assurance to Apple's systems that the Complainant was the person entitled to access the Apple ID account [redacted]@mac.com.

52. The DPC notes Apple's submissions regarding its established process for ensuring account security and for verifying entitlement to exercise access to the data associated with an AppleID[7]. Apple's position is that, without it being confident that a person is the account owner, it cannot proceed with an access request or other data protection rights [pursuant to Articles 15 to 22].

[6] Ibid.paragraph 17

[7] Ibid. paragraph 5, paragraph 10, paragraph 17

53. In asserting what he believed was his entitlement to access the data on the locked out AppleID account, the Complainant provided the DPC with credit card statements to show the fact that he pays certain sums to Apple. Apple stated in its communications to the DPC that a payment does not constitute confirmation of rightful access to an account.

54. Apple's position with regard to the credit card statements was as follows: "*[T]he current reset methods for accounts with security questions do not incorporate any means to verify credit card charges. It is also clearly the case that credit card payments do not in any way indicate that a person is the account holder and therefore data subject of any personal data in an account. Such statements only convey the making of payments.* [The Complainant] *could be doing so on behalf of any other person including, for example an estranged spouse*".

55. As outlined at paragraph 19, in the Complainant's response to the Commencement Notice, he also provided a document signed by a notary public with the IMEI of an iPhone and serial number of a MacBook Pro in his possession that he stated were linked to the AppleID in question. The DPC provided Apple with this information on 24 April 2023 and asked it some further questions.

56. Apple provided a response on 18 May 2023. Apple's responses are outlined in paragraph 20 (above). As outlined at paragraph 26 (above), Apple requested the redaction of these responses as it said the Complainant had not demonstrated his right to access this confidential account information. Accordingly, this information will be duly redacted when this Decision is provided to the Complainant and when it is published on the DPC's website.

57. Apple suggested it was willing to reach out to the Complainant in order to try and assist him with an alternative pathway to account recovery. Apple said that this may enable the Complainant to gain access to the account and, with that, Apple hoped, an amicable resolution to his complaint.

58. As outlined at paragraph 22, in the further engagement between Apple's Senior AppleCare Specialist, no solution was found to be possible and no resolution was found to the Complainant's concern.

59. Despite Apple's efforts to guide the Complainant through the process it has established for assisting data subjects who have forgotten their security credentials in order to access their AppleID account, the Complainant was unable to provide those credentials and remains unable to do so. Apple provided detailed explanations to both the Complainant and the DPC in relation to the verification requirements. Apple stated that it was not in a position to allow the Complainant to access the account in question without seriously undermining its legal obligations as a data controller. Apple also outlined that providing access to an account where it was concerned about the possibility that a request was malicious would breach its obligations under Articles 12 and 32 of GDPR. As outlined above, Apple stated that its security process would be extremely weakened if any person could access an account without access

to the email address associated with it and were also unable to answer basic questions such as date of birth.

60. It is therefore not disputed that the information not provided by Apple to the Complainant on foot of his access request included any data, including personal data, that was saved to the cloud and associated with the locked out AppleID. The DPC is satisfied that the only means by which Apple could have provided the Complainant with a copy of any personal data saved on his account, in fulfilment of the requirements of Article 15(3) of the GDPR, was for the Complainant to access it himself using the credentials he himself provided to Apple when he registered for an AppleID. [redacted]

61. While Apple did "refuse" to accept the additional information offered by the Complainant in order to support the exercise of his rights under Article 15(3), the DPC notes that the identification mechanisms a controller may rely on when fulfilling its obligations under the GDPR, include digital identification such as security credentials used to log in to an online service. Apple has demonstrated in the course of this Inquiry that the Complainant did not have access to this means of identification, those credentials being the only means possible to satisfy Apple's requirements.

62. Apple's explanations in support of its refusal to provide the Complainant with a copy of his data, including any personal data, that was processed in association with the Apple ID [redacted]@mac.com make clear that Apple's systems are agnostic as to whether [the Complainant's] name is the same as the name associated with the Apple ID [redacted]@mac.com], and as to whether he provided a correct date of birth when he registered for the AppleID.

63. The DPC notes again the following information provided in Apple's response of 3 November 2021 in the course of complaint handling: [redacted] *advised our Executive Relations team on 7 July 2021 that when attempting to answer security questions, he was prompted to confirm the date of birth set in the account, the expected date of birth was not accepted and that he was not able to proceed to complete verification. We note that* [redacted] *confirmed to the Executive Relations team on that same day that he might have set an incorrect date of birth for the account and he does not recall which one...Apple Support assisted the customer and confirmed to the customer that the birthday set on the account had never been edited, i.e. it is the date of birth that was entered when setting up the Apple ID* [emphasis added]."

64. The DPC also highlights the following information from Apple's response: *"It appears the issue lies with* [redacted] *being unable to input the password set on the account, not remembering his date of birth entered when the account was created, not having access to the emails sent to the address registered to the account and not having set up a recovery email. It is a*

customer's responsibility to ensure that their date of birth as entered is correct, or at least one they remember, and that they keep passwords secure [emphasis added]."

65. In that regard, the DPC also accepts that Apple's position that credit card statements or information about devices in the Complainant's possession were not sufficient to demonstrate the Complainant's entitlement to access data on the relevant locked-out AppleID account. The only information that would have satisfied Apple's normal requirements in relation to ascertaining the Complainant's entitlement to access information on the account [redacted]@mac.com were the security credentials which were unavailable to the Complainant.

66. Having regard to all of the information provided to the Inquiry, the DPC therefore accepts that Apple's position, in this specific case, it was not in a position to "identify" the Complainant in order to provide him with a copy of the data held in the relevant AppleID account, including any personal data saved therein.

67. The DPC therefore also accepts Apple's position that the Complainant has not demonstrated a clear entitlement to access the account in question, based on Apple's explanations in the course of complaint handling and this Inquiry.

68. The fact that he remains locked out of his Apple account is understandably frustrating for the Complainant. However, the DPC is satisfied that no information provided by the Complainant to Apple, other than the security credentials that are no longer available to him, would have alleviated any "reasonable doubts" concerning his identity. While the Complainant may have envisaged that his ID documents or other personal data would be treated as a proxy "permission" for Apple to access data on the locked account on his behalf and to provide him with a copy of it, or to unlock the account for him in the absence of the required security credentials, Apple has adequately explained in the course of this Inquiry why the provision of additional information was not of any assistance in helping to "identify" the Complainant to its satisfaction.

69. The DPC is satisfied based on the above analysis that Apple complied with the requirements of Article 15(1) and Article 15(2) of the GDPR, as requested by the Complainant on 8 July 2021. Having regard to the nature of the cloud service availed of by the Complainant, and the fact that his security credentials remained unavailable to him despite Apple's best efforts to assist him in recovering access to the account, the DPC accepts that it was not in this case possible for Apple to comply with Article 15(3) by providing him with "a copy" of any personal data undergoing processing in a locked-out AppleID account.

70. The DPC accepts Apple's argument in this case that its cautious approach was indeed to be expected under the requirements of the GDPR. The DPC also accepts Apple's contention that its security process would be *"extremely weakened if a person could access an account without*

access to the email address associated with it and were also unable to answer basic questions such as date of birth".

Based on the information provided to the Inquiry and the DPC's analysis, the DPC makes a finding that Apple's handling of the Complainant's access request was compliant with Article 12 and Article 15 of the GDPR and the Act.

Summary of Decision on infringements of the GDPR

71. The DPC finds that Apple did not infringe Article 12 or Article 15 of the GDPR in its handling of the Complainant's access request.

Remedial measures undertaken by Apple Distribution International Limited

72. No remedial measures were taken by Apple, nor were they required, in the case of this specific Complaint.

Exercise of Corrective Power by the DPC

73. As the Decision has not identified any infringements of the GDPR, the matter of exercising corrective powers does not arise in this case.

Judicial Remedies

74. 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 150(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 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 any imposition upon it of an administrative fine by the DPC.

Signed: Tony Delaney

Tony Delaney
Deputy Commissioner
On behalf of the Data Protection Commission