Dear Mr...,
Dear Sir or Madam,

1 as a result of our investigation of the processing of the Worldcoin Foundation, we find that the Worldcoin Foundation has violated the General Data Protection Regulation (GDPR) as described in detail below. Consequently, the following orders are issued pursuant to Article 58(2)(b), (d), (f) and (g) of the GDPR.

Orders:

Orders regarding the Iris-Codes:

2 I. A reprimand is issued to the Worldcoin Foundation for the infringement of Article 32 of the GDPR lasting from 24 July 2023 to 14 May 2024 by storing the iris codes as plain text in a database.

3 II. It is ordered that the Worldcoin Foundation erases the iris codes collected in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR) from 24 July 2023 to 13 December 2024 within one week of this decision becoming definitive, insofar as it (still) processes them for the purpose of passive comparison, which includes the processing steps of storing the iris codes and comparing with them in the event of a new registration of a user.

4 III. It is ordered that the Worldcoin Foundation confirms the erasure pursuant to point II. in writing to the Bavarian Data Protection Authority for the Private Sector within one week after the erasure has been carried out and explains the measures taken in order to carry out the erasure.

5 IV. It is ordered that the Worldcoin Foundation shall, within two months of this decision becoming definitive, bring the processing of the iris codes carried out within the Worldcoin project for the purpose of passive comparison, which includes the processing steps of storing the iris codes and comparing with them in the event of a new registration of a user, insofar as this takes place in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR), into compliance with Articles 5(1)(a) first alternative, 9(1) GDPR and, insofar as this processing is essentially carried out as described under Section I. of the reasoning of this decision ("Findings"), into compliance with Articles 5(1)(a) first alternative, 6(1) GDPR by obtaining consent of the data subjects which is

a) in line with the requirements of Article 4(11) GDPR (Articles 9(2)(a), 6(1)(a) GDPR) and

b) explicit (Article 9(2)(a) GDPR).

6 V. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point IV. within one week after the implementation of those measures.

7 VI. It is ordered that the Worldcoin Foundation shall, within one month of this decision becoming definitive, bring the processing of the iris codes carried out within the Worldcoin project and in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR) into compliance with Article 17(1) GDPR by providing data subjects with a possibility of exercising their right to erasure.

8 VII. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point VI. within one week after the implementation of those measures.

9 VIII. It is ordered that the Worldcoin Foundation shall, within one week of this decision becoming definitive, cease the processing of the iris codes carried out within the Worldcoin project for the purpose of passive comparison, which includes the processing steps of storing the iris codes and comparing with them in the event of a new registration of a user, insofar as this takes place in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR), until it has complied with the obligations under

a) point IV. and

b) point VI.

10 IX. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point VIII. within one week after the implementation of those measures.

Orders regarding the SMPC-Shares:

11 X. It is ordered that the Worldcoin Foundation erases the SMPC-Shares collected/generated in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR) from 24 July 2023 to 13 December 2024 within one week of this decision becoming definitive.

12 XI. It is ordered that the Worldcoin Foundation confirms the erasure pursuant to point X. in writing to the Bavarian Data Protection Authority for the Private Sector within one week after the erasure has been carried out and explains the measures taken in order to carry out the erasure.

13 XII. It is ordered that the Worldcoin Foundation shall, within two months of this decision becoming definitive, bring the processing of the SMPC-Shares carried out within the Worldcoin project for the purpose of passive comparison, which includes the processing steps of storing the SMPC-Shares and comparing with them in the event of a new registration of a user, insofar as this takes place in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR), into compliance with Articles 5(1)(a) first alternative, 9(1) GDPR and, insofar as this processing is essentially carried out as described under Section I. of the reasoning of this decision ("Findings"), into compliance with Articles 5(1)(a) first alternative, 6(1) GDPR by obtaining consent of the data subjects which is

c) in line with the requirements of Article 4(11) GDPR (Articles 9(2)(a), 6(1)(a) GDPR) and

d) explicit (Article 9(2)(a) GDPR).

14 XIII. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point XII. within one week after the implementation of those measures.

15 XIV. It is ordered that the Worldcoin Foundation shall, within one month of this decision becoming definitive, bring the processing of the SMPC-Shares carried out within the Worldcoin project and in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR) into compliance with Article 17(1) GDPR by providing data subjects with a possibility of exercising their right to erasure.

16 XV. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point XIV. within one week after the implementation of those measures.

17 XVI. It is ordered that the Worldcoin Foundation shall, within one week of this decision becoming definitive, cease the processing of the SMPC-Shares carried out within the Worldcoin project for the purpose of passive comparison, which includes the processing steps of storing the SMPC-Shares and comparing with them in the event of a new registration of a user, insofar as this takes place in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR), until it has complied with the obligations under

c) point XII. and

d) point XIV.

18 XVII. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point XVI. within one week after the implementation of those measures.

Other further orders:

19 XVIII. If the Worldcoin Foundation fails to fulfil its obligation under point II., a penalty payment of EUR 50.000 is due for payment.

20 XIX. If the Worldcoin Foundation fails to fulfil its obligation under point III., a penalty payment of EUR 5000 is due for payment.

21 XX. If the Worldcoin Foundation fails to fulfil its obligation under point IV., a penalty payment of EUR 50.000 is due for payment.

22 XXI. If the Worldcoin Foundation fails to fulfil its obligation under point V., a penalty payment of EUR 5000 is due for payment.

23 XXII. If the Worldcoin Foundation fails to fulfil its obligation under point VI., a penalty payment of EUR 50.000 is due for payment.

24 XXIII. If the Worldcoin Foundation fails to fulfil its obligation under point VII., a penalty payment of EUR 5000 is due for payment.

25 XXIV. If the Worldcoin Foundation fails to fulfil its obligation under point VIII., a penalty payment of EUR 50.000 is due for payment.

26 XXV. If the Worldcoin Foundation fails to fulfil its obligation under point IX., a penalty payment of EUR 5000 is due for payment.

27 XXVI. If the Worldcoin Foundation fails to fulfil its obligation under point X., a penalty payment of EUR 50.000 is due for payment.

28 XXVII. If the Worldcoin Foundation fails to fulfil its obligation under point XI., a penalty payment of EUR 5000 is due for payment.

29 XXVIII. If the Worldcoin Foundation fails to fulfil its obligation under point XII., a penalty payment of EUR 50.000 is due for payment.

30 XXIX. If the Worldcoin Foundation fails to fulfil its obligation under point XIII., a penalty payment of EUR 5000 is due for payment.

31 XXX. If the Worldcoin Foundation fails to fulfil its obligation under point XIV., a penalty payment of EUR 50.000 is due for payment.

32 XXXI. If the Worldcoin Foundation fails to fulfil its obligation under point XV., a penalty payment of EUR 5000 is due for payment.

33 XXXII. If the Worldcoin Foundation fails to fulfil its obligation under point XVI., a penalty payment of EUR 50.000 is due for payment.

34 XXXIII. If the Worldcoin Foundation fails to fulfil its obligation under point XVII., a penalty payment of EUR 5000 is due for payment.

35 XXXIV. The Worldcoin Foundation is ordered to pay the costs of the proceedings.

36 XXXV. The proceedings fee is set at __ EUR.

37 XXXVI. The expenses are based on the enclosed bill.

38 **Reservation regarding the power to impose a fine:**

39 These orders do not affect the power of the Bavarian Data Protection Authority for the Private Sector (BayLDA), in its capacity as authority competent for imposing fines, to impose administrative fines in addition to these orders for the underlying violations in accordance with Articles 58(2)(i), 83 of the GDPR and to impose fines in accordance with Article 83(5)(e),(6) of the GDPR in addition to the penalty payments referred to in points XVIII. to XXXIII.

40 **Reservation regarding individual complaints:**

41 These orders are issued in the context of an ex-officio investigation in accordance with Article 57(1)(h) of the GDPR, independently of any individual complaints under Article 77 of the GDPR, and are without prejudice to the power to issue further orders in the context of any complaints already lodged or to be submitted in the future.

Reasoning:

I.

Findings

42 In April 2023, the Bavarian Data Protection Authority for the Private Sector (Bayerisches Landesamt für Datenschutzaufsicht; "BayLDA") launched an investigation into the processing of personal data carried out in the context of the Worldcoin project in response to an information request from the French data protection supervisory authority.

A. Parties to the Proceedings

43 Relevant actors in the context of the Worldcoin Project are the Worldcoin Foundation, Worldcoin Europe GmbH, Tools for Humanity GmbH and Tools for Humanity Corp.

44 While with regard to the latter two actors (Tools for Humanity GmbH and the Tools for Humanity Corp), reference should be made to the findings of the BayLDA's preliminary investigation report set out below, the following will examine the findings concerning the roles of the Worldcoin Foundation and the Worldcoin Europe GmbH as regards the processing at hand.

45 Worldcoin Europe GmbH, located at Mies-van-der-Rohe-Str. 6, 80807 Munich, Germany, registered in Commercial Register B of the District Court of Munich under the number HRB 295283, formerly operated under the name "ZipCode GmbH". ZipCode GmbH was registered in Commercial Register B of the District Court of Fürth under HRB 20351 and had its registered office at Henkestraße 91, 91052 Erlangen. On 27 June 2024, the change of the company's name was registered with the Fürth District Court. On 25 July 2024, the shareholders' meeting of "Worldcoin Europe GmbH" decided to move the company's registered office from Erlangen to Munich. Following the corresponding registration of this change, Worldcoin Europe GmbH was entered in the Commercial Register B of the District Court of Munich under the number HRB 295283 on 9 August 2024.

46 In response to a request from the BayLDA of 12 March 2024, the four actors last explained, by letter of 22 March 2024, their roles in the context of the Worldcoin project:

47 That letter clarified that, since 24 July 2023, the Worldcoin Foundation has been acting as controller for the data processing operations carried out in connection with the Worldcoin project.

48 As regards Worldcoin Europe GmbH (in the letter "ZipCode GmbH" yet), said actors clarified that it is a subsidiary and the only establishment of the Worldcoin Foundation in the European Economic Area (EEA). In addition, Worldcoin Europe GmbH has been given a central role in the design of the Worldcoin Foundation's strategy on the capabilities of the World ID (see details below) and in its technical implementation. According to the actors' statement, Worldcoin Europe GmbH made a

significant contribution to the Orb verification process. At a strategic level, the actors stated, the management level of Worldcoin Europe GmbH is an integral part of all relevant processing decisions in the context of the Orb verification process.

49 According to the actors' statement, Worldcoin Europe GmbH is also involved, in particular, with regard to the design of the new SMPC set-up, for which Worldcoin Europe GmbH participated in and actively contributed to specific research, design and planning meetings. The new system design would not have been adopted without the confirmation of Worldcoin Europe GmbH, as it is an effective means of achieving the project's objectives.

50 Overall, Worldcoin Europe GmbH provided 134 code contributions on Github to the Open Source World ID Protocol and the World ID Orb verification mechanism by April 2024 alone.

51 In addition, according to the actors' statement, the management level of Worldcoin Europe GmbH participates in recurrent meetings concerning the specification of the Orb verification process.

52 The actors also explained that the system would be fundamentally different if Worldcoin Europe GmbH had not participated in its design. Finally, the Worldcoin Europe GmbH is now also actively involved in the processing of data by the Worldcoin Foundation as a party to the SMPC setup. According to the actors' statement, in that context, Worldcoin Europe GmbH acts as a processor on behalf of the Worldcoin Foundation.

53 In this respect, a processing agreement between Worldcoin Foundation and Worldcoin Europe GmbH was concluded on 21 March 2024 (for its content see F. and G.).

B. Cooperation Procedure and Hearing of the Worldcoin Foundation

54 On 30 April 2024, the BayLDA provided the other European supervisory authorities with a first preliminary draft decision via IMI ("Internal Market Information System") as part of the cooperation procedure pursuant to Article 60 GDPR.

55 This preliminary draft decision and the feedback from the supervisory authorities of Spain and Portugal were subsequently provided to the Worldcoin Foundation by letter of 30 April 2024 and email of 15 May 2024. The Worldcoin Foundation responded to the preliminary draft decision as well as the feedback from the Spanish and Portuguese authorities by letter of 14 May 2024 and letter of 17 May 2024, respectively.

56 In its replies the Worldcoin Foundation stated the following:

57 With the introduction of the SMPC system on 15 May 2024, the iris codes were erased. This erasure was purely carried out on a voluntary basis, without any legal obligation to do so.

58 Furthermore, the Worldcoin Foundation argued that the iris codes are not personal data, as they are not linked to the World-ID, the name or other identifiers. This is true even more since the introduction of the SMPC system, as the iris codes are split and the Worldcoin Foundation is no longer able to recombine the shares and identify a user.

59 The Worldcoin Foundation further argued that it is not possible to create an iris code from "simple images or video recordings", as the lower the resolution and the greater the deviation from the ideal light spectrum, the less information there is in an iris image and the less suitable it is for comparison. The Worldcoin Foundation therefore uses the specially self-developed Orb which is equipped with particularly high-resolution cameras, which also capture light in the infrared spectrum. The algorithm used to generate the iris codes is a proprietary, non-public algorithm. Neither the means for capturing suitable images nor the algorithm for converting them into an iris code are available to third parties; therefore, the iris codes are not reproducible. The Worldcoin Foundation therefore only treats the iris codes as personal data as a precautionary measure. The iris codes are also not biometric data or special categories of personal data within the meaning of Art. 9(1) GDPR, as they are not processed for the purpose of uniquely identifying data subjects. The Worldcoin Foundation does not use the iris codes to verify or find a specific person but to verify one's humaneness and uniqueness, in other words to verify "person" (generic).

60 Moreover, the Worldcoin Foundation stated that Article 6(1)(1)(f) GDPR serves as the legal basis for the processing of the iris codes. The Worldcoin project is a voluntary offer. However, the decision does not address the aspect of voluntariness. Furthermore, there is a legitimate interest in effectively protecting the integrity of internet services and platforms and, as a result, the general public from attempted fraud in connection with the use of the World-ID. This goal of protecting digital spaces can best be compared to the use of biometric data to control access to certain secure facilities such as buildings. It can only be sensibly achieved by storing iris codes for a longer period of time. The consent-based solution assumed in the draft would fatally defeat the purpose of the World-ID system and further reduce its usefulness beyond the significant costs already incurred by allowing users to request the cancellation of their World ID (including the erasure of their iris codes). Going any further would risk negating the potential benefits of the system in protecting the integrity of online spaces and the enhancement of the privacy of their users.

61 Lastly, Worldcoin objected against the finding of a violation of Article 32 GDR. The preliminary draft decision incorrectly assumes very high risks for data subjects. The scenario of large-scale unlawful retrieval of iris codes assumed in the draft is not realistic in light of the security mechanisms used. The technical and organisational security measures implemented (such as encryption mechanisms and access restrictions) are not only appropriate, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the the rights and freedoms of natural persons, but also go far

beyond the relevant IT and data security standards for industry and public bodies in the field of "biometric template encryption" (a term used by the Worldcoin Foundation). However, even if hackers were to gain unauthorised access, they would not be able to attribute an iris code to a specific person due to the lack of the iris codes being personal data.

62 In consideration of the feedback of the other European supervisory authorities and the two statements from the Worldcoin Foundation, the BayLDA prepared a second preliminary draft decision. On 6 June 2024, it sent the second preliminary draft decision to the legal representative of the Worldcoin Foundation via the Special Electronic Mailbox for Public Authorities (Besonderes elektronisches Behördenpostfach – BePo) together with a notice, which provided for a deadline to comment until 12 June 2024. By email dated 7 June 2024, the BayLDA granted the Worldcoin Foundation's request to extend the deadline to 26 June 2024.

63 In its letter dated 26 June 2024, received via BePo on the same day, the Worldcoin Foundation commented on the BayLDA's second preliminary draft decision.

64 The content of the statement was largely limited to a repetition of the arguments already put forward in the letters dated 14 May 2024 and 17 May 2024.

65 With the exception of the reference to the contractual penalty clause regarding the merging of SMPC shares in the data processing agreements with Worldcoin Europe GmbH (at the time of conclusion of the data processing agreement "ZIPCode GmbH") and Tools for Humanity Corp, the statement did not contain any new factual evidence to support the arguments already brought forward. The content of the data processing agreements is now included in the draft decision (see F. and G.).

66 In addition, the Worldcoin Foundation argued that the implementation deadlines set out in points II, IV, VIII and X, XII, XVI of the decision were too short. It is not possible for the Worldcoin Foundation to follow the orders within these deadlines. Fulfilment requires a substantial effort personnel-, organisational- and financial-wise, which, however, the Worldcoin Foundation did not specify further in its statement. It would therefore only be possible for it to fulfil the orders if it were to initiate relevant measures before the decision becomes final. However, this would unreasonably restrict its right to an effective defence. Consequently, the deadlines were disproportionate and outside of the limits of discretion of the authority.

C. Subject-matter of the Proceedings

67 The present orders are limited to the processing activities which can be finally assessed at the time of its adoption and set out in detail below, while some individual downstream examination sections (e.g. compliance with data security requirements for mobile ORBs) and announced but not yet

finalised changes to the processing activity are excluded as much as numerous voluntary improvements already carried out by the controller during the investigation process.

68 The following facts are covered by this decision:

69 1. The processing of iris codes for the purpose of passive comparison since the start of the Worldcoin project (24 July 2023) until the introduction of the SMPC system (15 May 2024). As the introduction of the SMPC system and the associated claim by the Worldcoin Foundation that iris codes are no longer processed for the purpose of passive comparison could not yet be verified, the examination includes not only the SMPC shares but also the iris codes. It will be explained that the iris codes have so far been processed unlawfully for the purpose of passive comparison and must therefore be erased by the Worldcoin Foundation. Accordingly, in the event that the Worldcoin Foundation's claims cannot be confirmed, orders with regard to the iris codes have been issued (as a precautionary or clarifying measure) as well.

70 2. The processing of the SMPC shares for the purpose of passive comparison following the introduction of the SMPC system. However, this does not include a detailed technical examination of the system and the question of a possible – persisting – violation of Article 32 GDPR (cf. Section I. of the decision and below E. for more detail on the SMPC system).

71 3. The lack of the option for data subjects to request erasure of the iris code and SMPC-Shares.

72 The following aspects, which were presented to the BayLDA but have not yet been submitted in a verifiable form, are reserved for a separate assessment within another official proceeding:

73 1. A detailed technical examination of the SMPC system and the question of whether this system is sufficient to assume that the iris codes and SMPC shares are now processed in accordance with Art. 32 GDPR.

74 2. The possibility for a data subjects to request the erasure of their iris code. A short time before the introduction of the SMPC system, the controller informed the BayLDA that it had now created (on a voluntary basis) a possibility for data subjects to request and obtain erasure of their iris code. The BayLDA has not yet been able to conclusively verify the introduction and operativeness of this voluntarily established means to request erasure of the iris code ("World ID unverify option"). The same is the case for the SMPC shares. By letter dated 13 August 2024, the BayLDA requested (among other things) further information from the companies involved in the Worldcoin project on this option offered to users, in particular with regard to its availability after the introduction of the SMPC system. In its response dated 23 October 2024 (received on the same day), the Worldcoin Foundation informed the BayLDA that the 'World ID un-verify option' had been available to users between 2 April 2024 and 8 May 2024. However, with the introduction of the SMPC system on 8 May 2024, all iris codes had been deleted; there was no (legal) obligation

to delete the SMPC shares, as these (in the view of the Worldcoin Foundation) did not constitute personal data pursuant to Art. 4(1) GDPR (see p. 3 et seq. of the response).

75 For further details regarding the facts of the case the preliminary investigation report up to the introduction of the SMPC system, but not including a (detailed) description of it, can be found directly below under D. The report is supplemented by the description of the SMPC system that follows hereto under E. and by the reproduction of the content of the data processing agreements between the Worldcoin Foundation and the processors involved in the SMPC system (in extracts) under F. and G.

D. Findings of the Investigation

1) Introduction

76 This audit report deals with the processing of personal data by the Worldcoin Foundation for the World ID service. In particular, the investigation focuses on biometric data a, as these can entail high risks for rights and freedoms of natural persons. Biometric data in the form of a so-called iris code is generated by the biometric enrolment device called "Orb" when the artificial intelligence of the Orb has determined that a real human being is in front of it as part of a registration process and no attempt of manipulation is being made. The unique registration of a person is referred to by Worldcoin as "Proof of Personhood". This is also intended to ensure that each person can only register once.

77 The start of processing is the market launch of the cryptocurrency Worldcoin on 24 July 2023. The previous product development by Tools for Humanity GmbH/Erlangen, which was completed with the market launch of Worldcoin on 24 July 2023, is not the subject of this investigation.

2) Investigation documents

78 The present investigation and assessment of the processing of personal data using the "Worldcoin" technology is carried out, among other things, on the basis of the following documents, which were requested in accordance with Article 58(1)(a), (b), and (e) GDPR: or were collected as part of a data protection inspection via the World App itself:

- 'Data Protection Impact Assessment' as of 21 March 2023, hereinafter designated as 'WorldID-DSFA' (worldid-dsfa_02_08_2023.pdf). The document is used in particular for technical background information on WorldID and the biometric iris codes
- Excerpt from a letter from Worldcoin on the role of ZipCode GmbH (today "Worldcoin Europe GmbH") (role-zipcode-2024-03-22.pdf)

- consent template used by Worldcoin Foundation regarding biometric data (biometric-data-consent-form-1-4-de.pdf). Document in version 1.4 in German, relevant excerpts translated into English

3) Timeline of the data protection investigation

79 BayLDA first looked into the Worldcoin technology at the end of 2022 due to press coverage.

80 After resolving questions of competence and queries from other data protection supervisory authorities that had arisen in the meantime, BayLDA initiated a basic investigation by requesting a data protection impact assessment in April 2023. At this time, Worldcoin was not yet operational on the German market and there were no data protection complaints (including from other European member states). The data protection impact assessment for the field testing phase (as of 21.03.2023) submitted at the time was updated several times in the course of the investigation by the controller and adapted to the different developments in processing activities and protective measures (most recently with separate data protection impact assessments on the ""*Orb processing*" *in the context of the verification of a Proof of Personhood*" and on the "*SMPC protocol (version 1) in the context of the iris uniqueness check*", each as of 17.09.2024). A final evaluation of this assessment of the consequences of the planned processing operations for the protection of personal data and whether an infringement of Article 35 GDPR occurred at the time the processing operations were initiated (started) is reserved for a separate decision.

81 In July 2023, the development phase of the Worldcoin technology ended with the launch of the cryptocurrency with the same name, "Worldcoin", on 24 July 2023 and the associated restructuring of the companies involved in the Worldcoin technology.

82 At this time, the Bavarian Data Protection Authority for the Private Sector (BayLDA), decided to initiate more detailed data protection investigation in accordance with Article 58 GDPR. At that time, still no data protection complaints had yet been received, neither from Germany nor from other EU/EEA member states.

83 The following investigation report covers the processing of personal data by the Worldcoin technology since 24 July 2023. In detail:

84 **Timeline 1** of the audit, covering the period from **24 July 2023 to March 2024**, includes a detailed examination of the technology used by Worldcoin (more precisely under section 4 "Status description of Worldcoin") including an on-site inspection at ZipCode GmbH/Erlangen (today "Worldcoin Europe GmbH/München") as well as at Tools for Humanity GmbH/Erlangen in September 2023 with the aim of evaluating the fundamental data protection issues associated with

Worldcoin: 1) legal basis of the processing, 2) deletion of the biometric iris codes and 3) protection of the biometric iris codes in accordance with Article 32 GDPR.

85 **Timeline 2** of the audit began in **March 2024 and continues as of the date of this audit report**, after Worldcoin changed the way in which the biometric iris codes are stored, after the BayLDA had determined in a letter to Worldcoin dated 23 December 2023 that the previous protective measures did not achieve an adequate level of security in accordance with Article 32 GDPR. In this timeline, the possibility of deleting the iris codes implemented by Worldcoin since March 2024 was also included in the data protection investigation (status at the time of this investigation report with date 30 April 2024 as a review of the rough concept).

86 **Timeline 3**, which follows **the conclusion of the audit of the fundamental issues** mentioned in the previous paragraph, includes the need for improvements to these fundamental issues, which have not yet been assessed as sufficient in timeline 2, in particular to ensure a sufficiently adequate level of protection in accordance with Article 32 GDPR.

87 This investigation report is based on the data protection assessment of Worldcoin in timeline 1. Where this report addresses any of the significant amendments that have occurred after the end of timeline 1, such as regarding the deletion of iris codes, explicit reference is made to timeline 2.

4) Description of the concept "Worldcoin"

88 The term **"Worldcoin"** refers to both a **cryptocurrency** and a **company** that operates an infrastructure called World ID in addition to this cryptocurrency.

89 The **World ID** is used to provide proof in digital services that an actor is human and has registered at most once - this process is referred to by the company Worldcoin as **"Proof of Personhood"**.

90 The "Proof of Personhood" feature at Worldcoin comprises a system that is also referred to as a **"deduplication scenario"**. This is intended to ensure that a person may only be registered once within a registration system.

91 To carry out this verification, a registration process is initiated using an app called **"World App"**, in which a user's head is scanned in a mobile registration device called "Orb".

92 **Artificial intelligence** in the Orb is used to check whether or not a real person is standing in front of the device and whether or not possibly a contact lens with a manipulated iris pattern is being worn.

93 If a real person is standing in front of the Orb, iris images of the eyes are captured and converted into a 0/1-bit representation (**iris code**) within the Orb.

94 The iris code is stored in the company's **IT backend**.

95 Various cryptographic keys are generated as part of the registration process; a central key pair, consisting of a **public key** and **private key**, plays a central role in the World ID infrastructure.

96 The public key/private key pair is generated inside the app on the smartphone at the first start of the World App.

97 In the World ID infrastructure, the private key remains exclusively on the smartphone of a World ID user.

98 The private key is stored exclusively on a data subject's World App smartphone app and is understood to be a securely stored secret key. The public key is entered into a blockchain via the registration process after successful verification that a user is a human being and has not yet registered previously. The public key is identical to the World ID.

99 The public key in the blockchain and the private key on a user's smartphone can be used to prove membership of a defined group (e.g. "registered in the World ID infrastructure") by means of a cryptographic zero-knowledge protocol without disclosing further identification features or the private key.

100 Proof of membership of a defined group ("Proof of Personhood") represents the primary business model of the Worldcoin company at the time of this evaluation.

101 In the context of this assessment, the World ID infrastructure refers to the generation and storage of iris codes in the IT backend, the entry of Orb users' public keys in the blockchain during the registration process, and the implementation of zero-knowledge protocols. The World App is also understood as a component of the World ID infrastructure.

102 The cryptocurrency "Worldcoin" is not categorised as part of the World ID infrastructure in the context of this investigation, as it has no technical connection to the processing of iris codes, the blockchain and the zero-knowledge protocols and does not itself contain any personal data[1].

103 Registration with the "World ID" is also associated with the payment of a certain amount of the cryptocurrency Worldcoin.

104 The cryptocurrency "Worldcoin" has no connection to the World ID infrastructure with regard to the processing of personal data. In particular, no personal data of a unit ("coin") of the cryptocurrency is stored, especially no iris code.

105 Due to the technically complex processing of personal data, the audit was split into individual sub-areas, which are based on the sketch in Figure A.

[1] The fact that transactions, as with other cryptocurrencies, may lead to conclusions about natural persons is not the focus of this data protection audit.

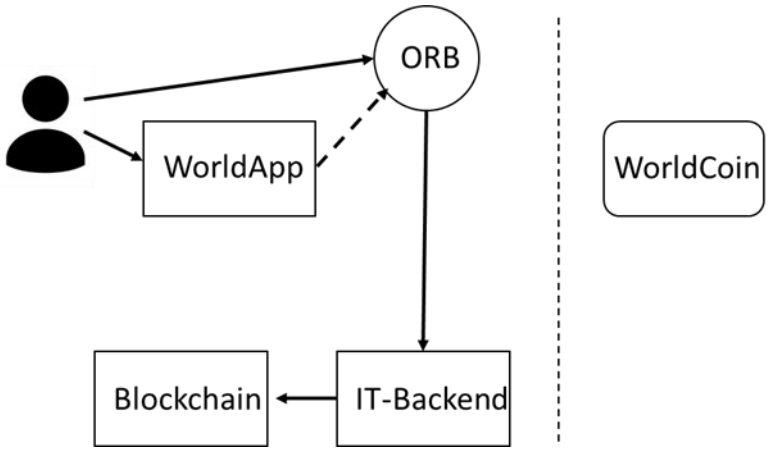


Figure A: Technical elements of Worldcoin

Now in more detail:

1. Smartphone app "World App"

106 The "World App" can be downloaded from the Android and Apple app stores and is also marketed there as a wallet for the cryptocurrency Worldcoin.

107 Apart from the wallet, the World App can be used to initiate registration with the World ID infrastructure. To do this, the user is guided through a consent process in which they are also informed about the processing of personal data by the Worldcoin company.

108 At the end of the consent process, which consists of a "basic consent" and an "extended consent", in which image recordings in raw format are to be used for product development purposes, a QR code is displayed in the World App, with which the capture of image recordings on the Orb can be started.

2. Mobile recording device "Orb"

109 The Orb mobile capture device is a hardware component developed by Worldcoin itself, on which a high-resolution image sensor is mounted and which is connected to the Internet.

Figure B: https://worldcoin.org/blog/worldcoin/how-the-launch-works

110 The Orb should be able to be used largely without the support of Worldcoin by so-called Orb operators, who at most guide users interested in registering with regard to the standing position in relation to the Orb.

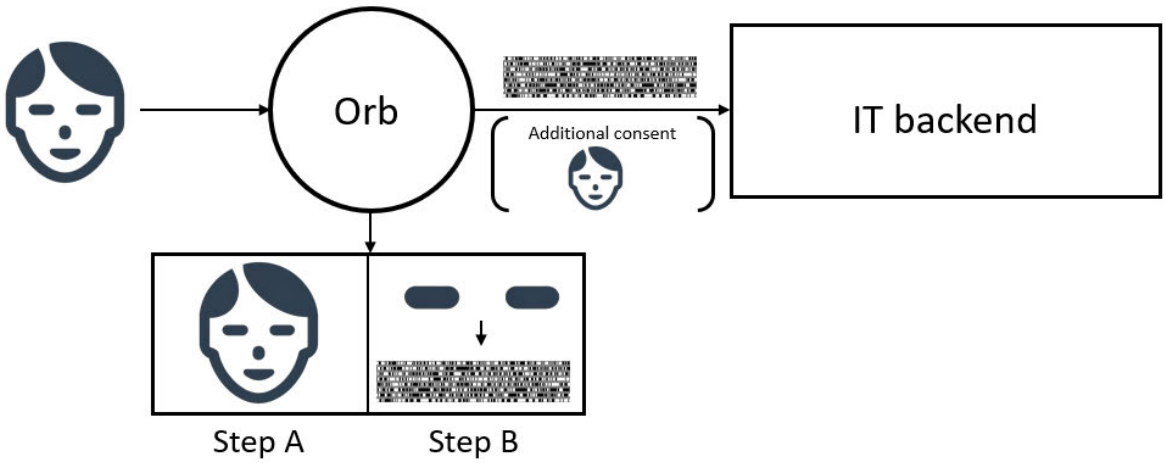


Figure C: Illustration of the checking if there is a real person (step A), the iris code calculation (step B) and the transmission of this data (depending on the type of consent) to the IT backend

111 The Orb is said to be realised with a high degree of resistance to manipulation attempts such as a secure boot, cryptographic signing of software components and encrypted (temporary) storage.

112 As part of the consent process, consent to the processing of biometric data is mandatory for registration. This is referred to as "iris code consent" (Figure D) in this investigation report.

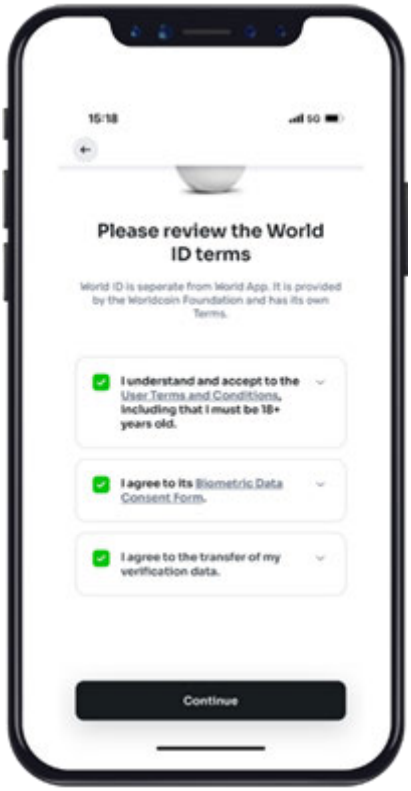


Figure D: Consent to the processing of biometric data ('Iris code consent')

113 A user must also agree to the 'User Terms and Conditions' for Orb registration. At the first level of the consent dialogue, the user must also confirm that they are at least 18 years old (Figure E).

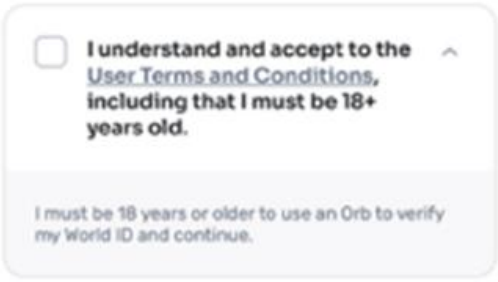


Figure E: The minimum age for using an Orb is 18 years

[redacted] A detailed investigation to determine whether an infringement of Article 25 of the GDPR occurred at the time the processing operations were carried out and a final assessment of these measures for the protection of minors are reserved for a separate decision.

114 In the consent text 'Biometric Data Consent Form' of the consent dialogue (Figure F), the processing of iris codes is described as follows:

> **Derivatives of the above data.** We use complex state of the art algorithms and our own neural networks to create numerical representations ("**Derivatives**") of the above images to enable machine comparisons and interactions between them. These derivatives are strings of numbers (*e.g.*, "10111011100…") that entail the most important features of the images. It is not possible to fully reverse the Derivatives to the original image. Most importantly, we use our custom version of the Daugman Algorithm to calculate such a string of numbers from the iris image ("**Iris Code**"). This Iris Code is used to ensure that users can only sign-up once.

Figure F: Description of the iris code in the 'Biometric Data Consent Form' consent dialogue

115 Furthermore, the scope of the consent to the processing of iris codes is defined in the consent text 'Biometric Data Consent Form':

> The data we collect (described above) may or may not be considered biometric data depending on the applicable laws where you live. However, we treat them as biometric data and handle them with extra security and care. The legal basis to collect the Image Data is your explicit consent. The legal basis to calculate derivatives of the Image Data (like the Iris Code) and actively compare it against our database is your explicit consent. The legal basis to store the Iris Code and passively compare your Iris Code is our legitimate interest – namely, our interest to defend ourselves against fraudulent users that illegally try to sign-up more than once.

Figure G: division of the legal bases for processing an iris code into two processing domains

116 In timeline 2, the registration process was redesigned in such a way that users interested in registering must book a registration appointment. When booking an appointment, both the consent text "Biometric Data Consent Form" and an age of at least 18 years must be confirmed (Figure H).

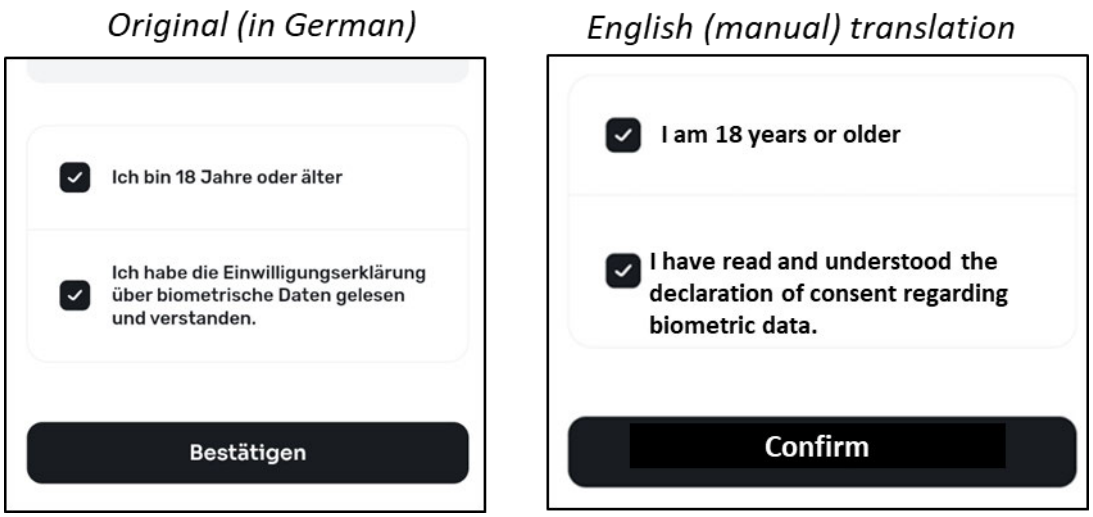


Figure H: Age confirmation and confirmation of knowledge of the declaration of consent for biometric data are a prerequisite for appointment registration

117 Approximately 2 hours before the appointment, the data protection consent for the processing of biometric data can then be given as before, but with a different menu navigation (Figure I). [redacted]

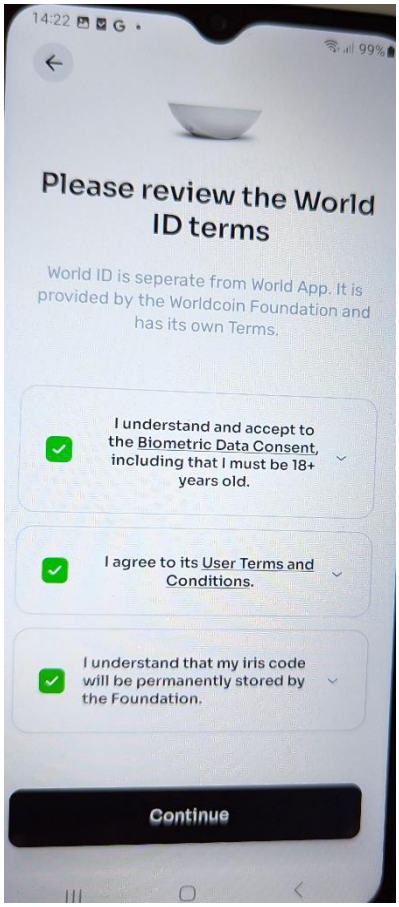


Figure I: Consent dialog in timeline 2 (photo, as the screenshot function is disabled for the dialog in the WorldApp)

118 In the consent text "Biometric Data Consent Form" of the consent dialog (Figure F) in timeline 2, the processing of iris codes is presented as follows:

- Derivatives of the above data. We use complex state of the art algorithms and our own neural networks to create numerical representations ("Derivatives") of the above images to enable machine comparisons and interactions between them. These derivatives are strings of numbers (e.g., "10111011100…") that entail the most important features of the images. It is not possible to fully reverse the Derivatives to the original image. Most importantly, we use our custom version of the Daugman Algorithm to calculate such a string of numbers from the iris image ("Iris Code"). This Iris Code is used to ensure that users can only sign-up once.

119 The scope of consent in the consent text "Biometric Data Consent Form" with regard to the processing of iris codes remains essentially the same in timeline 2 (in the German version the term "Derivate" is used by now instead of "Ableitungen"):

> The data we collect (described above) may or may not be considered personal data or biometric data depending on the applicable laws where you live. However, when it comes to security, we treat them as biometric data and handle them with extra security and care. The legal basis to collect the Image Data is your explicit consent. The legal basis to calculate derivatives of the Image Data (like the Iris Code) and actively compare it against our database is your explicit consent. The legal basis to store the Iris Code and passively compare your Iris Code is our legitimate interest — namely, our interest to defend ourselves against fraudulent users that illegally try to sign-up more than once.

120 Accordingly, the processing of the iris code at Worldcoin is divided into two "processing domains":

1. The collection of the iris code in the Orb by calculating it from the pixel images of a user who wants to register, and the comparison of the iris code of such user with the iris codes of already registered users ("active comparison"), which are already stored in the iris code database, constitutes processing domain 1.

2. The storage of the iris code of a registering user, insofar as the iris code was not already existing in the iris code database and therefore the comparison carried out in processing domain 1 was successful in the sense of the deduplication scenario (= successful registration), as well as its future use for comparisons in the context of registration processes, in particular of other Worldcoin users ("passive comparison"), constitutes processing domain 2.

121 The purpose of processing domain 1 is to carry out the registration of a user (not yet included in the iris code database).

122 The purpose of processing domain 2 is the comparison of already registered users with a new user according to processing domain 1 and the detection/prevention of attempts by a user to register more than once.

123 For processing domain 1, consent is used as the legal basis by means of the consent text 'Biometric Data Consent Form' from Worldcoin.

124 For processing domain 2, on the other hand, the above text refers to “legitimate interest” as a legal basis.

125 The legal basis for the processing of a data subject's iris code is therefore consent for the purpose of their registration (“active comparison”). Whereas, the use of their iris code to ensure a one-time registration (“passive comparison”) is not based on consent, but on a legitimate interest (probably within the meaning of Article 6(1)(f) GDPR).

126 In addition to the processing of iris codes, consent can be given to the forwarding of pixel images for research and product improvement purposes ("data custody"). This is referred to as "custody consent" in this investigation report.

127 According to Worldcoin, the custody consent is intended to relieve users of the requirement of re-registering with an Orb in the event of a future change in the algorithms used for generating the iris code.

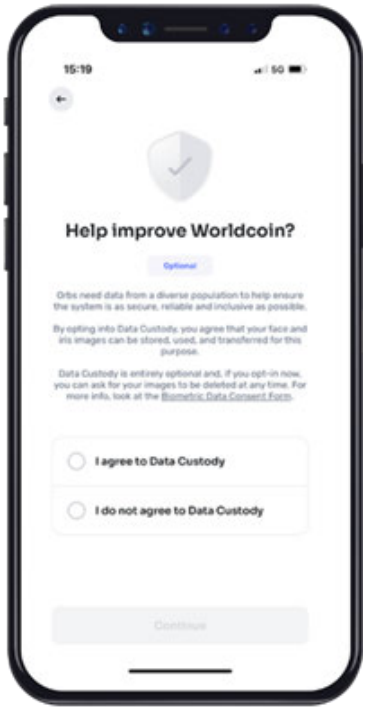


Figure J: Consent to the transfer of pixel data ("custody consent")

128 If an interested user wants to register with the World ID infrastructure after installing the World App and completing the consent process there, which is indicated by the display of a QR code in the World App, the QR code is held in front of the sensor of the Orb.

Figure K: QR code of the World App after consent of the person concerned

129 The QR code does not contain the user's Public Key, but a User ID. This is used to transfer the public key to the IT backend as part of the registration process. For this reason, Wordcoin also receives the user's IP address together with the Public Key and could also link it to the iris code.

130 The validity of the QR code is reported back by means of visual/audible signalling and the recording of the image data of the interested user is started.

131 Several high-resolution photos of the interested user are now taken, in which the user's face should be visible.

132 These high-resolution photos of the face and the sections of the eye with the iris are referred to as "pixel images" in this investigation report.

133 In addition, high-resolution photos of both eyes of the interested user are taken by the sensor.

134 The Orb includes an artificial intelligence component (AI component) that uses the images to decide whether a real person and not, for example, a photo was held in front of the Orb. Furthermore, this AI component should also be able to decide whether there are any attempts to manipulate the eye images, e.g. in the form of prepared contact lenses.

135 If the AI component concludes that there is a sufficient probability that a person without manipulated eye images is standing in front of the Orb, then further processing is initiated. Otherwise, the detection process is cancelled, which is reported back to the interested Orb user by means of visual/acoustic signalling.

136 During further processing, a biometric datum, the so-called iris code, consisting of a 0/1 character string, is calculated within the Orb from the eye images[2]. For this purpose, a standard procedure is used to calculate the iris code, which has been optimised by an in-house development.

137 This involves calculating the unique features of a human iris that should be as position-independent as possible (in relation to the angle at which the pixel image is captured by the camera sensor).

138 The Gabor filter used here transforms a pixel image into a so-called complex mathematical space consisting of four (complex) areas. By categorising each pixel of the pixel image into one of these four areas, a value (either 0 or 1) of the iris code sequence is calculated.

139 The complete sequence of the individually calculated values then results in the iris code.

140 By assigning the complex mathematical numbers to one of the four areas, there is a loss of information (which is quite intentional with the aim of enabling position-independent recognition). However, the iris code generated in this way should still be so unique to a specific person that any further iris codes of this person calculated using the same procedure have a greater similarity[3] than to all other persons for whom an iris code is calculated using the identical generation algorithm.

141 The iris code is then digitally signed and transmitted to the IT backend of Worldcoin via an encrypted transport connection.

142 In the case where a user has provided "extended consent", the raw face and eye data is encrypted using end-to-end encryption within the Orb and then also transferred to the Worldcoin IT backend.

143 According to Worldcoin's concept description, the iris codes are not stored persistently on the Orb.

144 Nor is there any persistent storage of raw data collected after extended consent has been granted, which is temporarily stored on the Orb in encrypted form in such a way that decryption is only possible in the IT backend.

3. IT backend

145 The iris code and the user's public key are transmitted to the IT backend via an encrypted TLS connection.

The following processing takes place there:

146 The user's iris code is compared with all iris codes already stored (1:n comparison with all iris codes in the iris code database). To this aim, a Hamming distance is calculated on the bit values of the iris

[2] Using a Daugman algorithm modified by Worldcoin, which is the standard procedure for generating iris codes from pixel images of the eye area.

[3] Using a suitable similarity metric, e.g. a Hamming distance, which calculates the number of deviations between the 0/1 values in a standardised way.

codes as a similarity metric. Above a defined delta threshold, a newly entered iris code is categorised as already existing or not:

147 If the iris code is assessed as already existing, it is not stored in the iris code database. Instead, a message is sent to the user's smartphone. The Orb at which the specific registration was carried out also receives an error message, which is communicated by the Orb to the registering Orb user by means of a visual and acoustic cancellation signal.

148 If the Hamming distance results in a value less than delta, this means that the iris code has not yet been registered with Worldcoin. In this case, the iris code is entered in the iris code database. The successful registration is also communicated to the Orb where the specific registration was carried out and to the World App of the registering Orb user.

4. Blockchain entry

149 After successful initial registration, the user's public key is entered into a blockchain (https://etherscan.io/address/0xf7134CE138832c1456F2a91D64621eE90c2bddEa).

150 The iris code or further other user data are not stored in the blockchain.

151 After entry in the blockchain, the user is informed of the successful registration via the World App.

152 For this purpose, the World App generates a zero-knowledge protocol that proves that the user has a private key that matches an existing public key on the blockchain.

153 Zero-knowledge protocols are a cryptographic procedure in which one party can convince another party that a certain assertion is true without revealing any information beyond that.

154 In the present case, the World App learns that the user has successfully registered, but not which iris code belongs to the user.

155 Worldcoin uses the open-source semaphore programme library, which is part of the Privacy & Scaling Explorations group supported by the Ethereum Foundation, as the basic building block for this.

156 After successful registration, a fixed amount of Worldcoin cryptocurrency is paid out to the user.

5. World ID infrastructure

157 The Word ID infrastructure can be used following successful registration by entering the public key into the blockchain.

158 The same technology of zero-knowledge protocols is offered for this purpose, which was already used for the feedback of a registration to the World App

159 With the World ID infrastructure, it is possible to prove that someone is a human being and not a software bot when using any Internet service without revealing the identity of the private key that remains on a user's smartphone.

160 However, when using the World ID infrastructure, the user's IP address is always transmitted to Worldcoin.

161 [redacted] If the user is blocked by an internet service, for example due to a breach of the latter's terms of use, the real person, who is not known to the internet service, can no longer "identify" themselves there using the World ID infrastructure. In this case, the World ID not only functions as an instrument of proof of being human, but the uniqueness of the registration also plays a key role. If the user has their iris code deleted from the iris code database at Worldcoin, they would be able to re-register with Worldcoin and the Internet service at which they are blocked. This way of using the World ID was mentioned by Worldcoin during a video conference held with the BayLDA in March. In this use case World ID is applied as a kind of biometric access provider for any Internet service.

162 The World ID and iris code are closely connected. The processing of the iris codes is aimed at ensuring that a person can only receive on World ID. If the comparison carried out during registration shows that the iris code of the registering user does not match any iris code previously stored in the database, i.e. if the iris code does not yet exist in the database, the user is considered not yet registered and his/her iris code is stored in the database in order to be able to detect in the future whether the user attempts to register a second time (contrary to the terms of use). Once the public key generated within the World App (see paragraph 95 et seq. above) has been entered in the blockchain (see paragraphs 146-149 above), registration is complete and the user is in possession of a (validated) World ID (see paragraphs 157 and 98 above).
However, if the comparison results in a match with an already stored iris code, a new or further registration is rejected, i.e. the public key is not entered in the blockchain and the user does not come into possession of a (validated) World ID (see paragraphs 146-149 above).
According to the concept of the World ID infrastructure, each person should only be able to have one (validated) world ID, because the World ID is supposed to not only serve the user's interest in being able to confirm to services in a simple way that they are a human and not a bot programme ('Proof of Personhood', e.g. as a replacement for having to solve so-called 'captchas' in order to access a service), but also the interests of third parties (service providers) connected to the World ID infrastructure concerning the protection of their services and their services' integrity.

If a user could register multiple times, malicious actors could create a large number of World IDs or obtain them from third parties and thus circumvent the protection against bot programmes intended by the World ID infrastructure.

6. Cryptocurrency Worldcoin

163 The cryptocurrency Worldcoin (WLD for short) is based on the open-source decentralised blockchain Ethereum. Ethereum enables the storage of smart contracts on the blockchain, the content of which is public and written in a programming language.

164 The "ERC-20" smart contract standard is used for the cryptocurrency Worldcoin in this regard - a standard procedure that enables compatibility with the existing Ethereum ecosystem. Since the number of possible transactions on Ethereum is limited, Worldcoin uses the "Layer 2" solution "Optimism" for better scalability; the transactions are first collected independently of Ethereum and then bundled and written to the Ethereum blockchain ("Layer 1") as a single transaction.

165 The cryptocurrency Worldcoin is therefore not based on any new technology in terms of its technical construction.

166 The smart contract stipulates that in the first 15 years after its launch, the number of available WLDs is limited to 10 billion, [redacted] The other 75 % - managed by the Worldcoin Foundation - will mainly be allocated to users, e.g. in the form of a "grant" after successful verification on an Orb.

167 The cryptographic keys for the WLD "wallet" are independent of the keys used for World ID. In direct connection with the cryptocurrency, therefore, no (personal) data from the registration/usage process is stored at Worldcoin (in particular no biometric data such as iris codes).

168 For this reason, the examination of the Worldcoin cryptocurrency in the context of this investigation is limited to the fact that it is paid out upon initial registration and in the form of regularly recurring "grants" and, accordingly, the interests of the Worldcoin company in protecting against multiple registrations would have to be considered in a legal assessment.

5) Focus of the Investigation Pursuant to Article 58 GDPR at Worldcoin

169 BayLDA initiated its investigation pursuant to Article 58 GDPR at its discretion ex officio, considering the significant risks of processing and the potentially large number of data subjects, as there were no complaints at the time the review began.

170 For this reason, an investigation focus was selected that particularly addresses the risks to data subjects when using World ID. Due to the high technical complexity, this was divided into two audit areas based on a conceptual evaluation of the received data protection impact assessment (Annex A):

<u>Audit area 1: Focus on the protection of biometric data</u>

171 Audit area 1 focuses on the question of the legal basis of the processing, compliance with data subjects' rights, and the security of the processing in accordance with Article 32 GDPR.

In more detail:

(a) Legal basis of the processing

172 The use of the World ID infrastructure requires the installation and use of the "World App" app, as described above.

173 The World App is used to implement the information obligations under Article 12 et seqq. GDPR.

174 As users' biometric data is also processed, a central point to be examined is whether this processing of biometric data falls under Article 9 GDPR and, accordingly, whether consent must be obtained in accordance with Article 9(2)(a) GDPR or whether - at least for some processing steps – a balancing of interests in accordance with Article 6(1)(f) GDPR could be used as a legal basis.

175 It must also be assessed whether, in the event that the processing does not fall under Article 9 GDPR, the consent of the data subject would still be required and whether this would apply to all processing steps - in particular to the storage of iris codes.

(b) Deletion of the iris codes

176 In addition to the question of whether the information obligations under Article 12 et seqq. GDPR are complied with sufficiently, the investigation of the World ID infrastructure focuses in particular on the right to erasure, as the iris code cannot be deleted from the World ID infrastructure (screenshots of the app in Appendix B).

177 Worldcoin justifies this with the prevention of multiple registrations.

178 The impossibility of deleting an Iris Code is also shown in the World App in the deletion dialogue (Figure L).

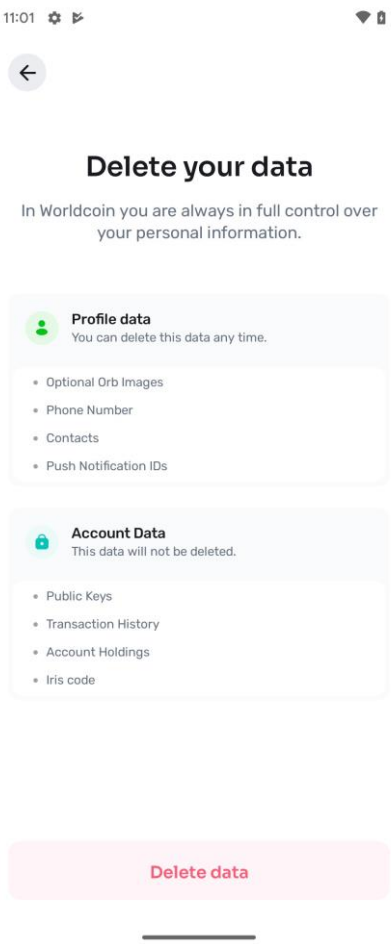


Figure L: The Iris Code is included in the deletion dialogue under 'Account Data' and displayed as non-deletable

179 The question of the deletion obligation is closely linked to the question of whether a processing of biometric data in the meaning of Article 9 GDPR takes place, as the iris code would then have to be categorically deleted.

180 If the processing were not subject to Article 9 GDPR, it would have to be examined on the basis of Article 17(1)(c) GDPR whether the right to object under Article 21(1) GDPR is interpreted in such a way that the iris code must nevertheless be erased and how the objection process would have to be structured in relation to a withdrawal of consent (in case Article 9 would not apply).

(C) Security of processing in accordance with Article 32 GDPR

181 Worldcoin's aim is to ensure that as many users as possible worldwide use its World ID infrastructure and that the iris codes of as many people as possible are processed.

182 Since all iris codes are stored centrally in the iris code database, one focus of the investigation is whether the level of security designed by Worldcoin by means of technical and organisational measures in accordance with Article 32 GDPR is sufficient to mitigate the risks to the rights and freedoms of data subjects.

Audit area 2: Focus on Orb, World App and TOM of the IT infrastructure

183 The second audit area, which is to take place after the completion of audit area 1, covers the implementation of the security mechanisms of the mobile enrolment device "Orb", the World App and the technical and organisational measures of the IT infrastructure that do not directly relate to the biometric data.

184 According to a concept review carried out by BayLDA to date, high risks for the overall application are indeed seen in these areas, should the implementation of the basic concept and security safeguards show deficiencies.

185 At the same time, it cannot be ruled out that a level of security required under Article 32 GDPR can be achieved in this area in particular by using cryptographic procedures, including a careful process for managing the cryptographic keys used, for example, for end-to-end encryption of raw data, for signing the integrity of an iris code during transport to the IT backend or for the tamper resistance of the Orb operating system.

186 As a review of, in particular, the implementation of the concepts requires a large amount of time, it was decided during the audit planning to separate this audit area from the fundamental issues contained in audit area 1 (this would be a timeline 4, see section 3 Timeline of the data protection audit).

6) Actors and responsibilities

187 Various actors other than the data subject are involved in the data processing associated with the Worldcoin project in different (data protection) roles (Figure M).

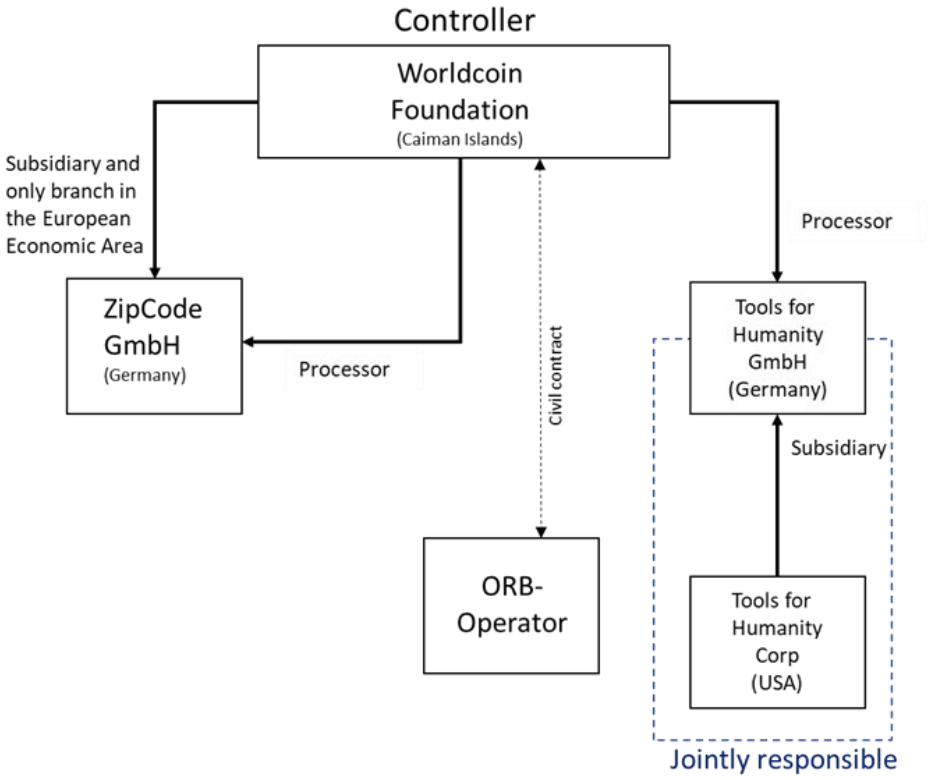


Figure M: Actors involved in Worldcoin

(a) Tools for HumanityGmbH

188 Tools for Humanity GmbH is a (wholly owned) subsidiary of Tools for Humanity Corp and is based in Erlangen, Germany.

189 As a hardware and software service provider, Tools for Humanity GmbH develops hardware and software applications for Tools for Humanity Corp, also with regard to the so-called Proof of Personhood technology of the World ID infrastructure.

190 The processing activities carried out in connection with the development and product testing of the Proof of Personhood technology (before timeline 1, not in the investigation focus) were carried out by Tools for Humanity Corp and Tools for Humanity GmbH (according to their own assessment as provided by them to BayLDA) as joint controllers pursuant to Article 26 GDPR.

191 Tools for Humanity GmbH is moreover the only establishment of Tools for Humanity Corp in the European Economic Area.

(b) Tools for Humanity Corp

192 Tools for Humanity Corp, based in the USA, is the parent company of Tools for Humanity GmbH and, together with Tools for Humanity GmbH, is a joint controller for the processing operations carried out in the context of product testing and development of the so-called Proof of Personhood technology (see above).

(c) Worldcoin Foundation

193 The Worldcoin Foundation, based in the Cayman Islands, assumed responsibility for the data processing carried out in this context with the launch of the so-called Worldcoin project on 24 July 2023 and has thus been the controller for this data processing operations since this date.

194 Since this date, Tools for Humanity has only been the controller for operating the World App. Moreover, it has also acted as a processor for the Worldcoin Foundation since this date.

(d) Worldcoin Europe GmbH (prior "ZipCode GmbH")

195 Worldcoin Europe GmbH, based in Munich/Germany, is a (100% owned) subsidiary of the Worldcoin Foundation and its only establishment in the European Economic Area.

196 Besides being a subsidiary and thus an establishment of the Worldcoin Foundation, it also acts as a processor on behalf of the Worldcoin Foundation.

(e) Orb Operators

197 Orb operators are independent companies that enable data subjects to register with World ID via the Orb on the basis of civil law contracts.

198 To this end, they should provide information about the World ID technology and guide and support registration using the Orb.

199 According to the Worldcoin website, Orb operators are paid in the cryptocurrency Worldcoin.

200 According to information on the Worldcoin website, locations, operating hours and other details are selected in consultation with Worldcoin project staff to ensure compliance with local laws and regulations (Appendix 1).

E. SMPC System

201 On 15 May 2024, the controller made significant changes to the design of its processing with the introduction of the SMPC system.

202 SMPC stands for 'Secure Multiparty Computation' and is a modern and mathematically complex cryptographic protocol with which - generally speaking - a function can be computed by several involved parties without each of them having full knowledge of the input data for this function. Worldcoin's SMPC system - according to the sketch outlining the system - is designed in such a way that a Hamming distance of a new iris code can be calculated, but no more plain text iris codes are required in the Worldcoin database. Instead, so-called 'shares' are used.

203 SMPC shares are - if conceptually correctly implemented and generated - random sequences of numbers that do not contain any information about the original plain text when looked at individually. The generation of SMPC shares takes into account the number of actors, which are also referred to as 'parties'. If, for example, an SMPC system consists of three actors, a plaintext is split using a specific share generation algorithm so that three shares are generated from it, each of which is transmitted individually to one of the actors.

204 If shares are merged, the original plaintext can be fully reconstructed. In the case of Worldcoin, this means that all plaintext iris codes can be reconstructed by merging the actors' databases. For this reason, when assessing whether shares constitute personal data and whether an SMPC system implemented like this meets the requirements of Art. 32 GDPR, special consideration must be given to the specific technical and organisational measures as well as the corporate structure of the actors involved.

205 The aim of the Worldcoin SMPC system is to create an appropriate level of protection in accordance with Art. 32 GDPR at data level by implementing a so-called 'Biometric Template Protection Scheme'.

206 The information available at this time is limited to rudimentary descriptions of the system in slides provided by Worldcoin dated 12 May 2024, which contain a sketch outlining the 'Wordcoin SMPC Version 1', and the data processing agreements with the processors Worldcoin Europe GmbH and Tools for Humanity participating in the SMPC system as 'parties'. A detailed examination of the SMPC system will be carried out from summer 2024 due to the high complexity of the system (both version 1, which according to Worldcoin is intended to be an interim implementation, and version 2, which is intended to be the final implementation, insofar as this will be implemented by that time).

207 The facts available from these sources of information are sufficient for assessing the SMPC shares' nature as personal data and the legal basis for the processing of the shares. They are as follows:

208 Within the Worldcoin SMPC system version 1 - according to the sketch outlining the system - the plain text iris codes are no longer stored persistently. However, these are still available in plain text

not only during processing in the ORB, but are also transmitted (using transport encryption) as plain text iris codes to the IT backend and then to the two parties involved in the Worldcoin SMPC system version 1 (Tools for Humanity GmbH and Worldcoin Europe GmbH), which process the plain text iris codes for the calculation of a preliminary result of the Hamming distance. After successful registration, the shares calculated from the plaintext iris code as part of this passive comparison are stored in the databases of Tools for Humanity GmbH and Worldcoin Europe GmbH.

209 The shares are random sequences of numbers calculated from the original plain text iris codes. The plaintext iris codes previously stored by Worldcoin were converted into shares as part of the migration process to the SMPC system. Furthermore, new plaintext iris codes added since the introduction of the system (i.e. in the event of successful registration by a user - see below) are also split into shares. The system is currently an SMPC system with two actors ('parties'). In the future, according to the controller's statements, there may be a split into three shares, which will require three actors.

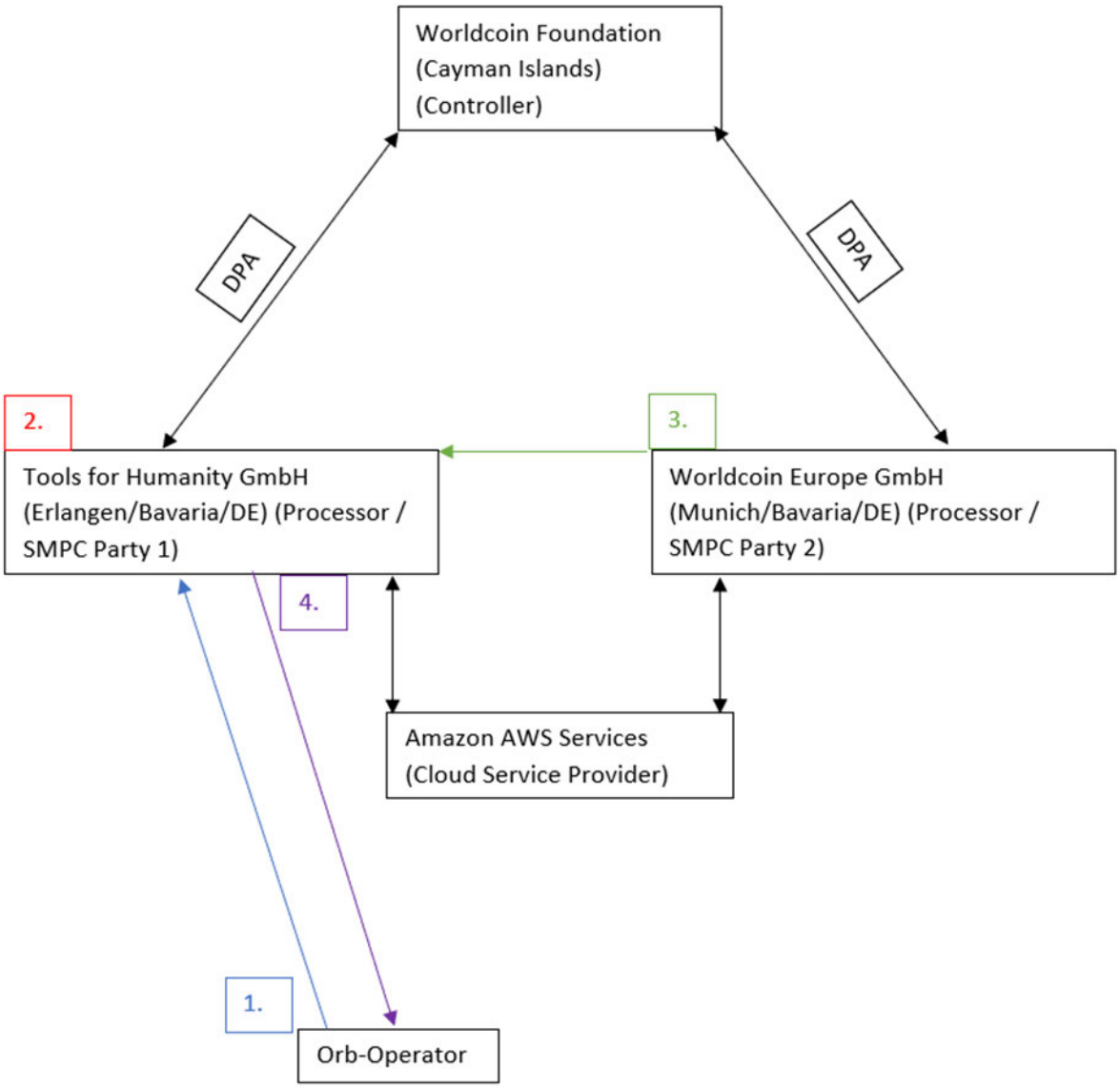
210 The two shares generated in the IT backend from the plaintext iris code are divided between the so-called 'SMPC parties', each of which stores one share permanently and processes it on behalf of the Worldcoin Foundation for the purpose of passive comparison.

211 Both SMPC parties currently use the same cloud service provider, Amazon AWS, for the computation-intensive operations

212 Although the original plain text iris code no longer exists in the database due to the splitting, it can be restored by merging the shares.

213 In the normal workflow of the system, merging the shares is neither necessary, as will be explained in a moment, nor is it intended by the Worldcoin Foundation. The extent to which this is effectively ensured in terms of algorithms and implementation will be a key focus of the further investigation of the Worldcoin system. The current assessment focuses on assessing the shares' nature as personal data and the legal basis for the processing of the shares, for which a detailed technical examination of the implementation is not necessary.

214 When a new user is registered, the following procedure takes place (Worldcoin SMPC Version 1):



215

216 1. A user visits an orb operator. The plain text iris code is generated within the orb and sent to the IT backend. The pixel images created when the iris code is generated are principally deleted (with the exception of 'extended consent').

217 2. Tools for Humanity GmbH ('TFH') (first SMPC party) calculates the distance between the plain text iris code and each share stored by it ('partial distance 1') and retains these 'partial distances 1'. TFH also sends the iris code to Worldcoin Europe GmbH (second SMPC party).

218 3. Worldcoin Europe GmbH calculates the distance between the iris code and each share stored by it ('partial distance 2') and sends these 'partial distances 2' to TFH.

219 4. TFH calculates the (total) hamming distances from the partial distances and thus determines whether a user is already registered in Worldcoin's infrastructure/database or not.

220 If this is not yet the case, the iris code is split and the parties involved in the Worldcoin SMPC system Version 1 (Tools for Humanity GmbH and Worldcoin Europe GmbH) each store a share in their databases for the purpose of passive comparison.

F. [redacted]

[redacted]

[redacted]

[redacted]

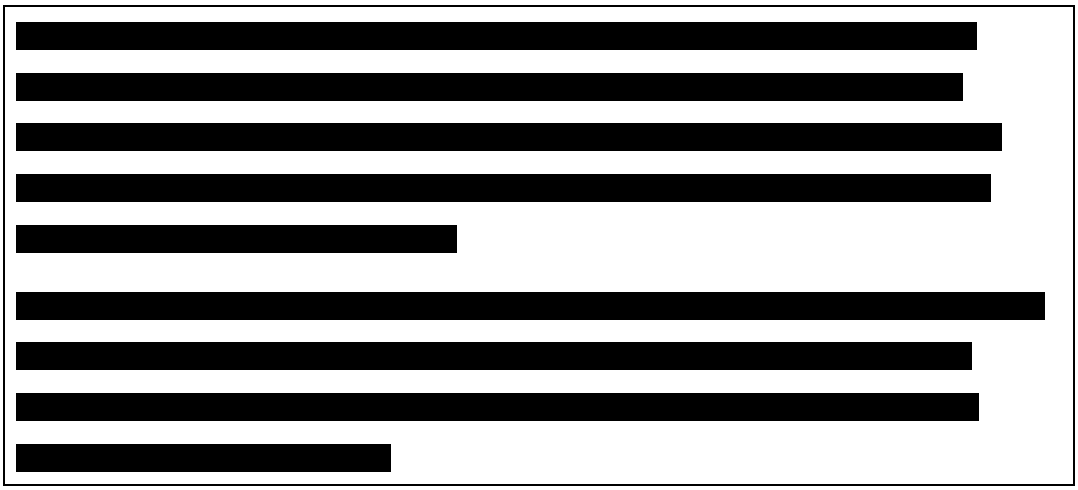
[redacted]

[redacted]

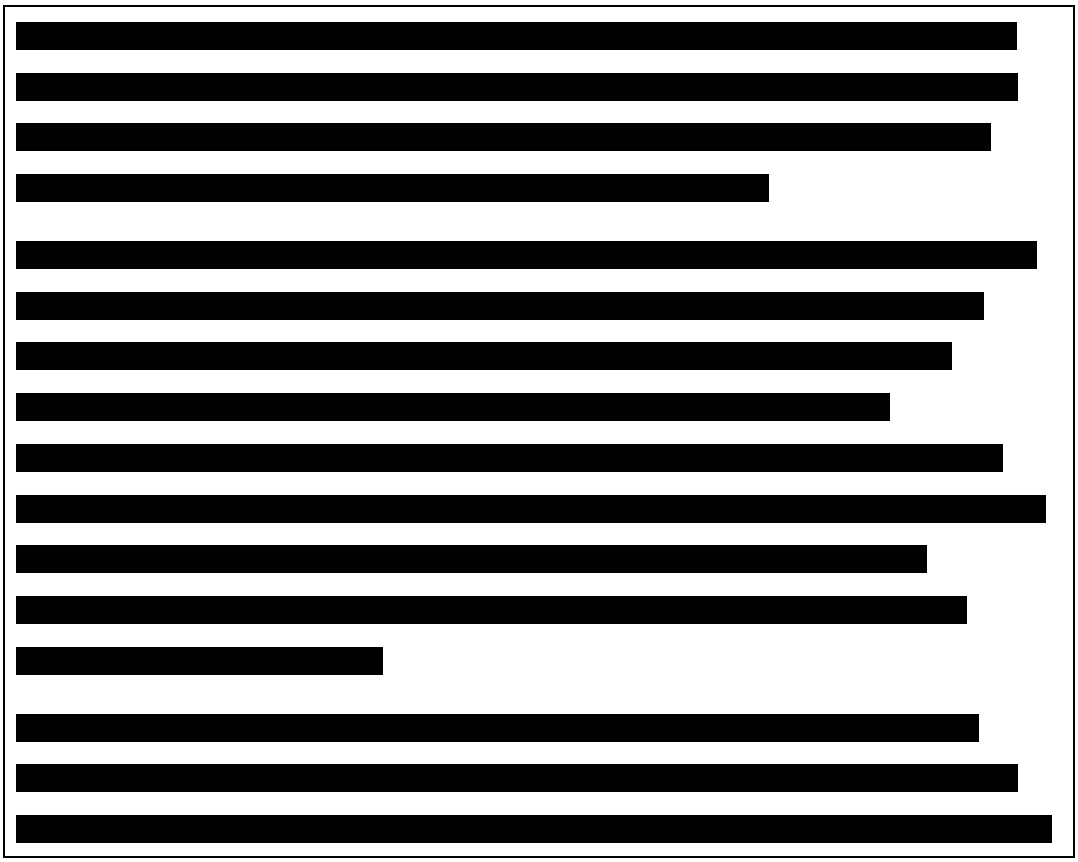
[redacted]

[redacted]

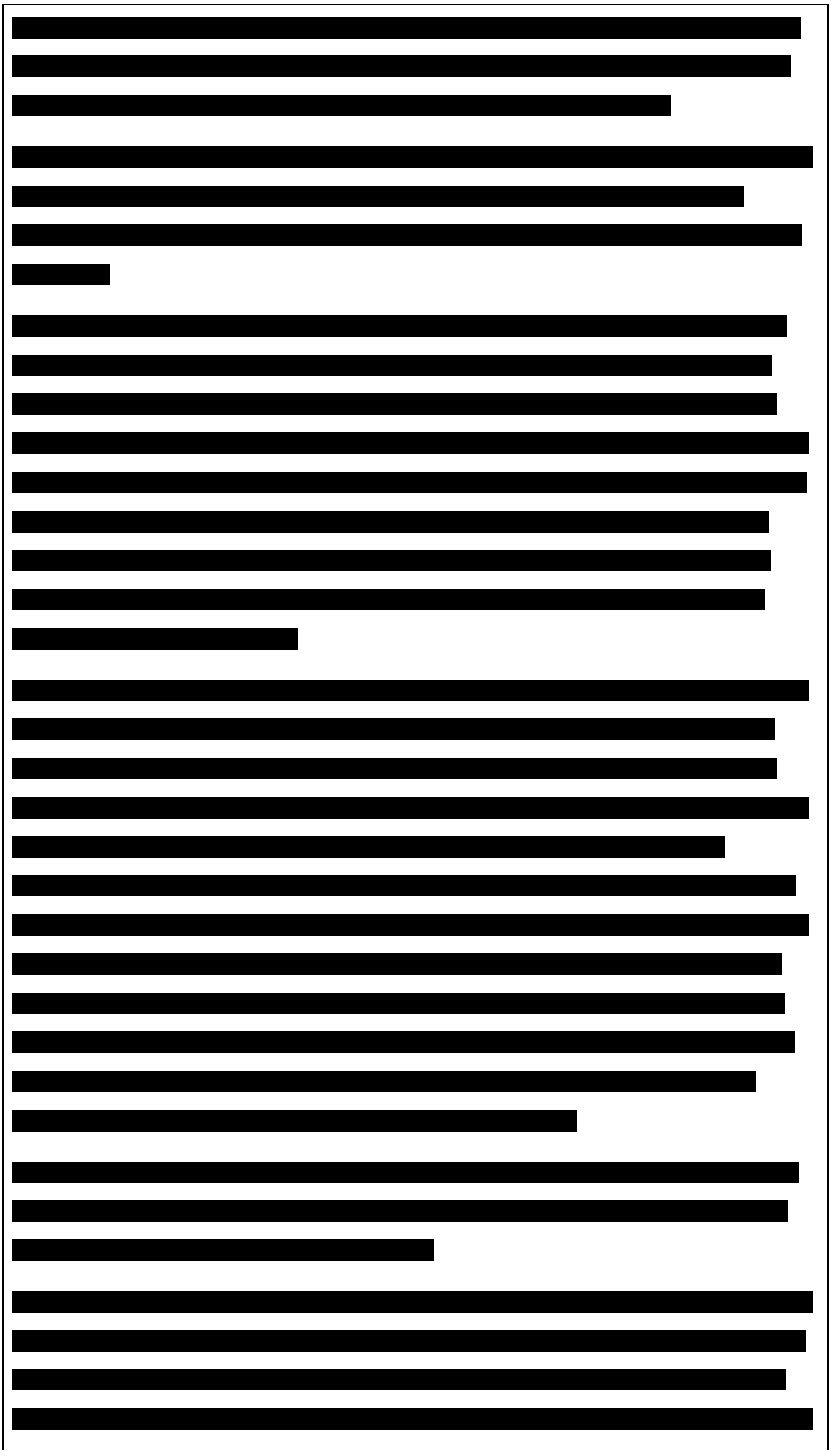
227 [redacted]



[redacted]



[redacted]



[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

233 [redacted]

[redacted]

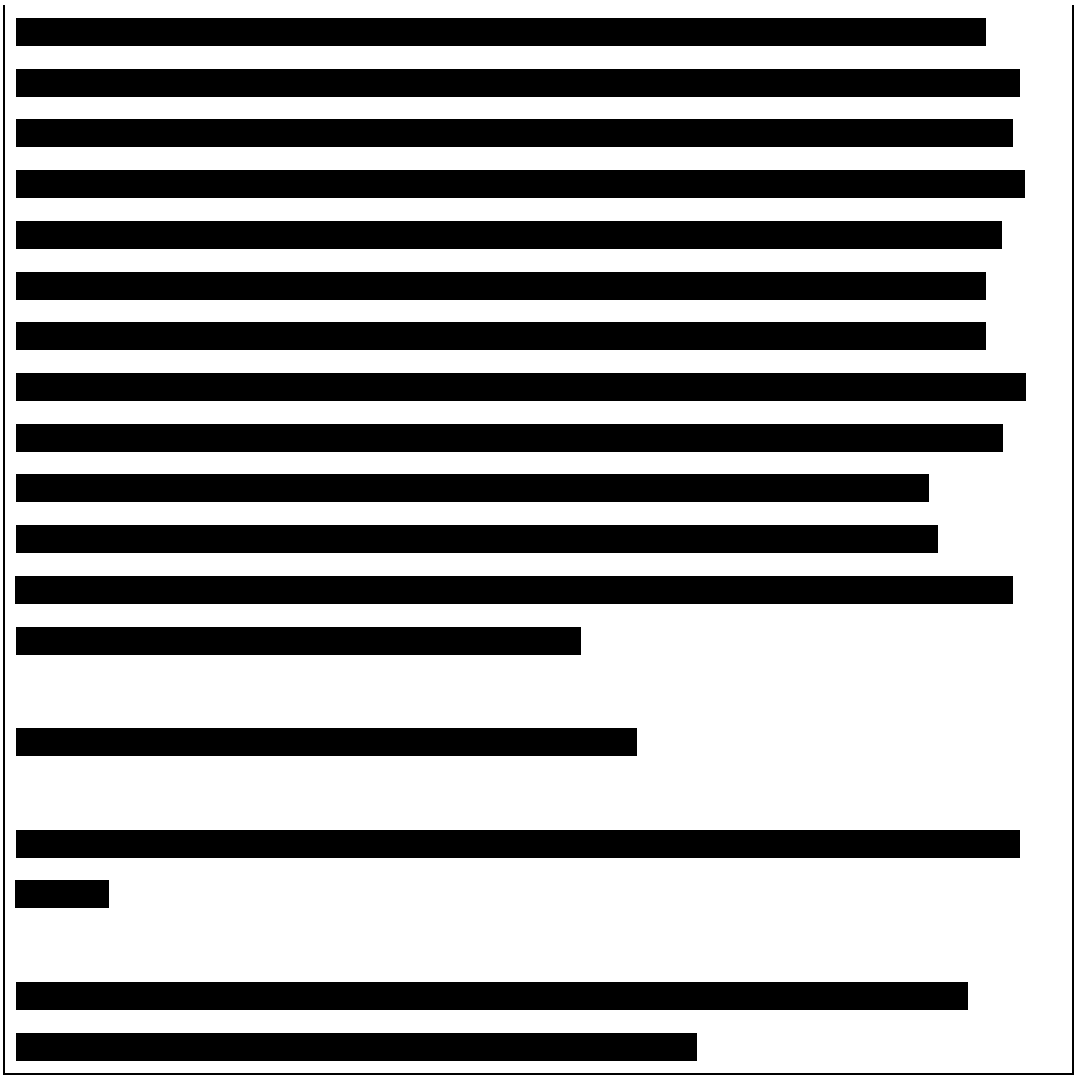
[redacted]

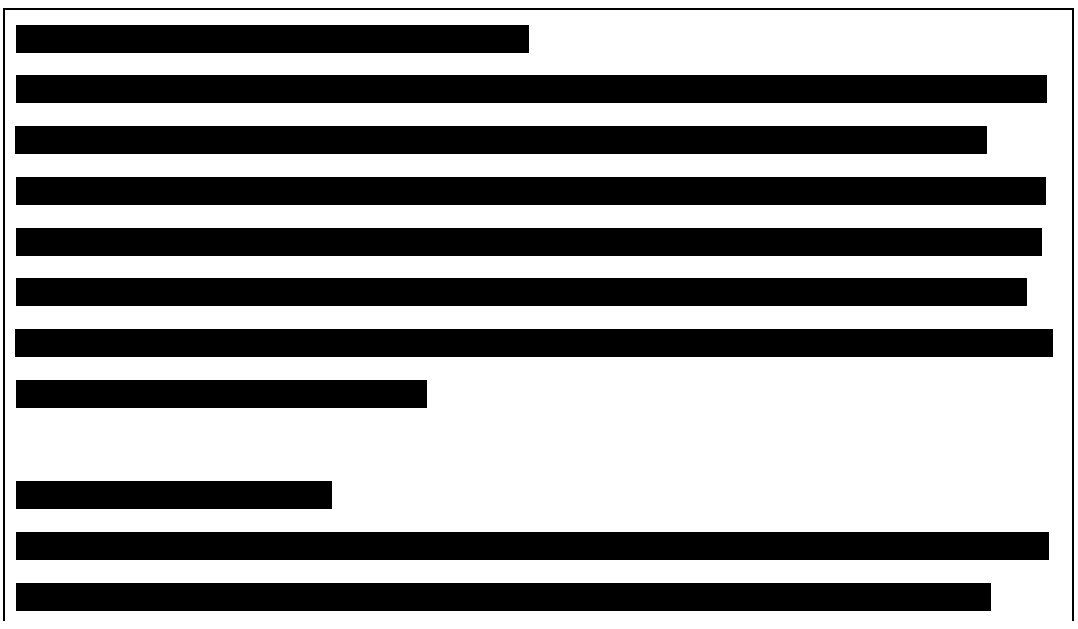
234 With letter dated 13 August 2024, the BayLDA requested further information from the companies involved in the Worldcoin project regarding, among other things, the data processing agreements and sub-processing agreements concluded in relation to the project.

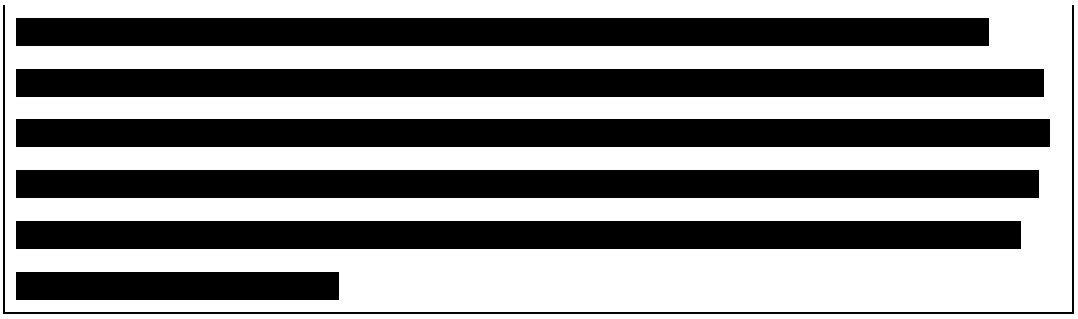
235 [redacted]

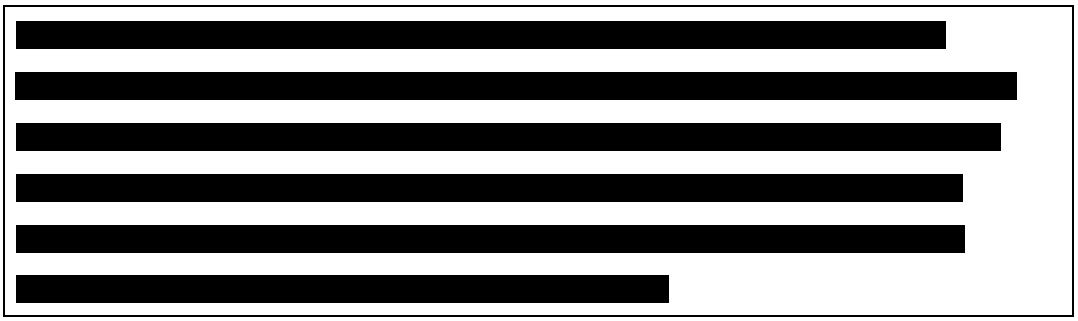
[redacted]

[redacted]









249 [redacted]

[redacted]

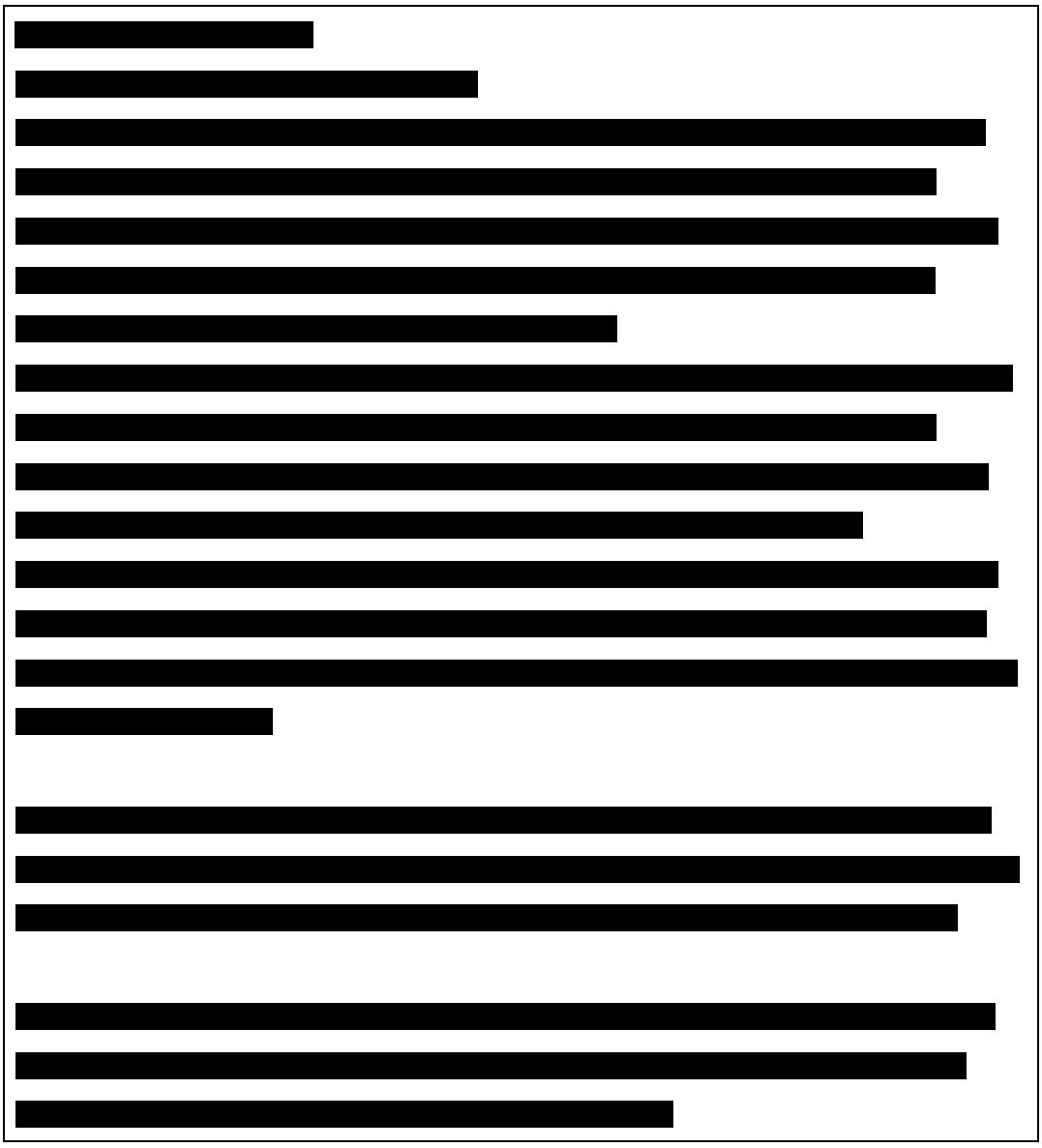
[redacted]

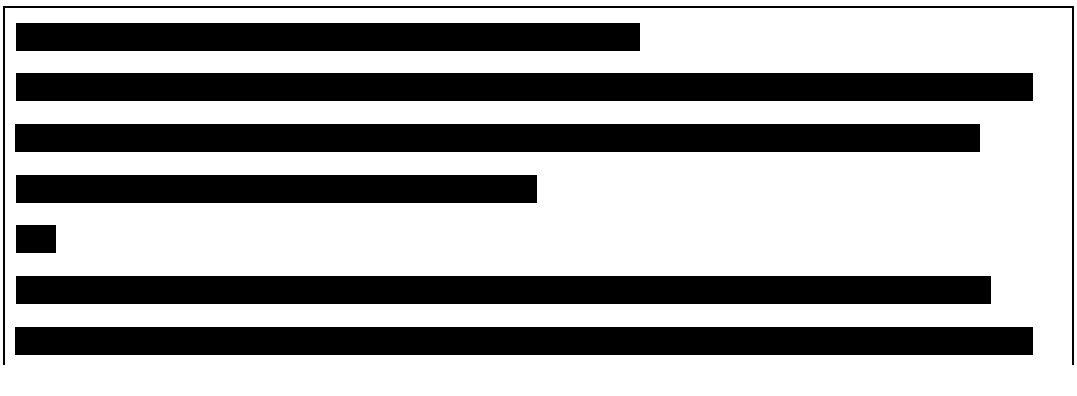
[redacted]

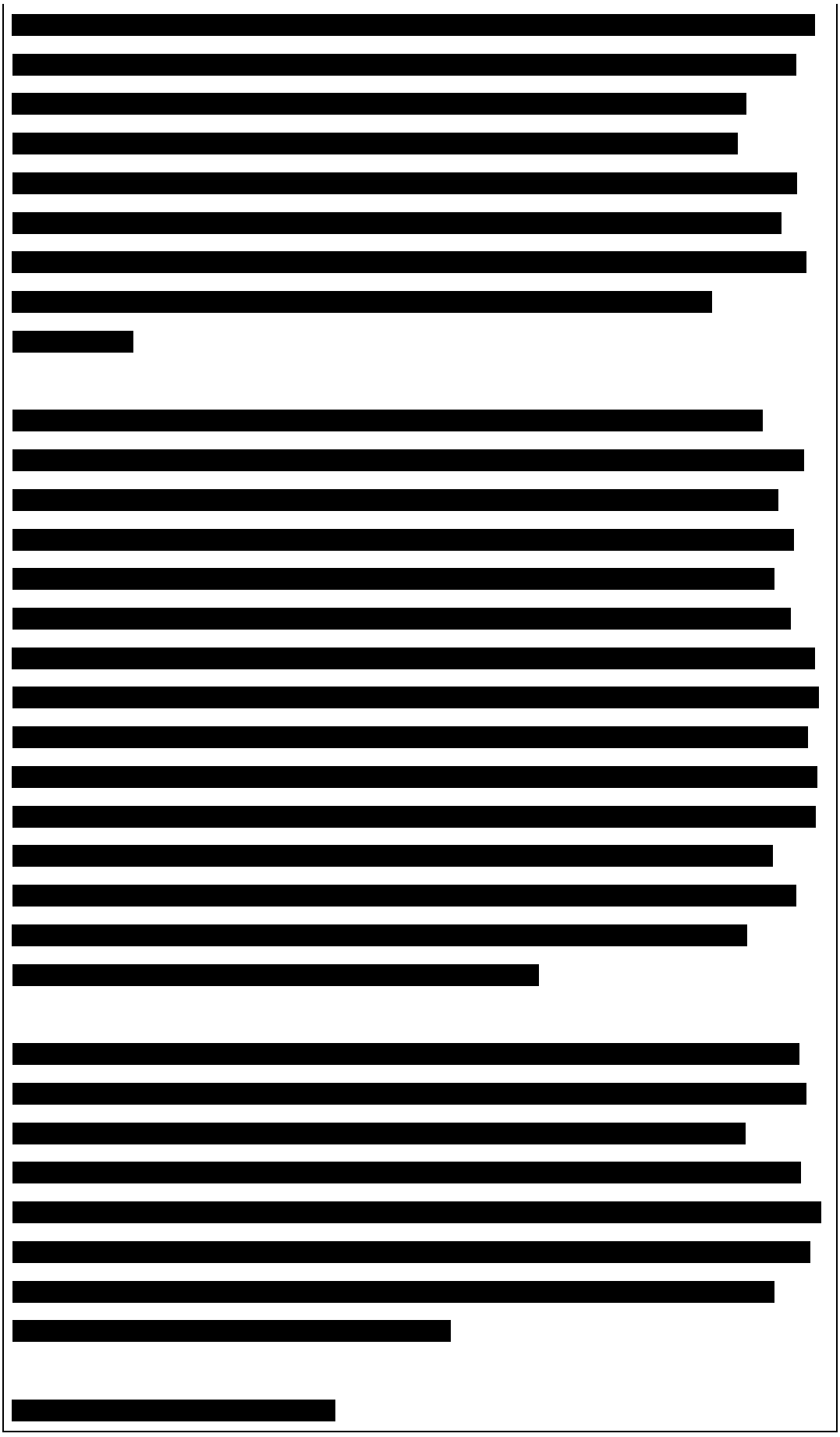
[redacted]

[redacted]

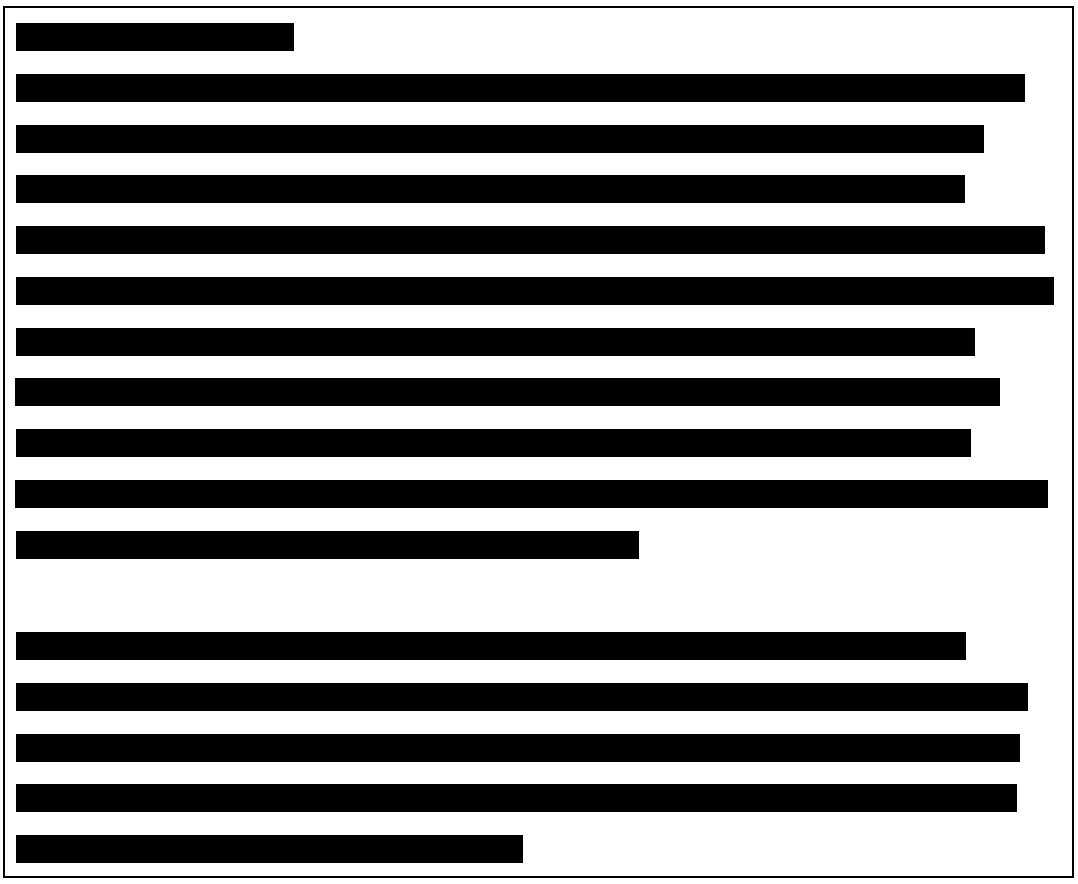
[redacted]





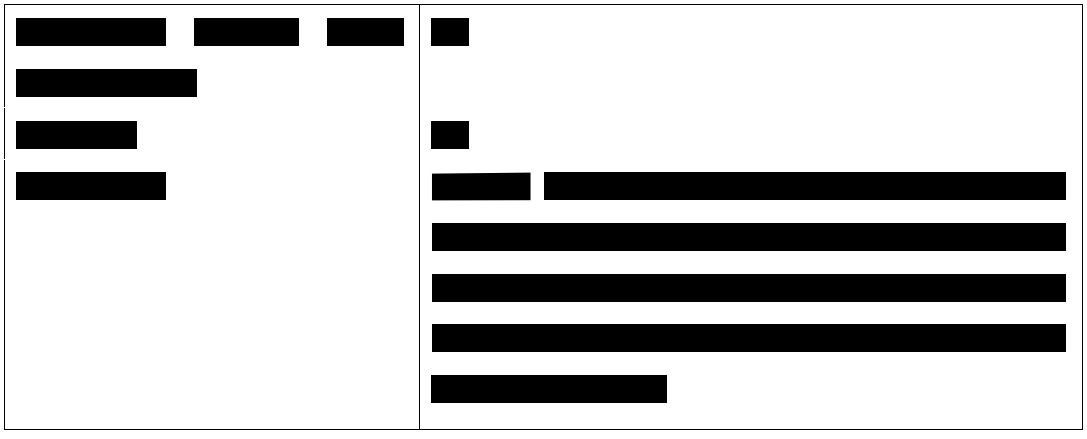


251 [redacted]

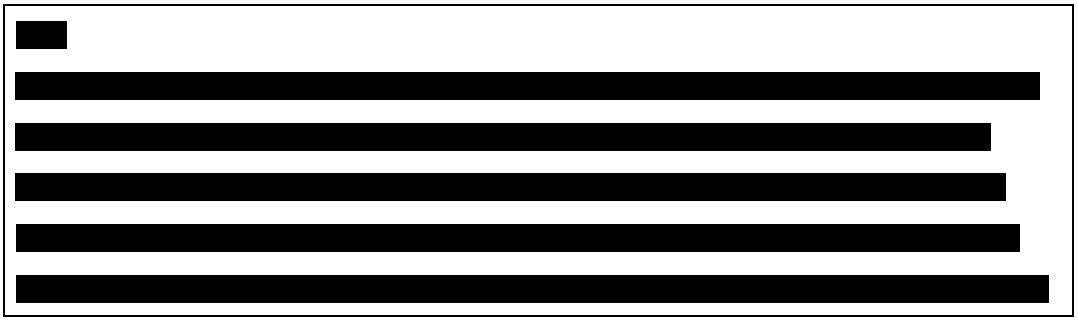


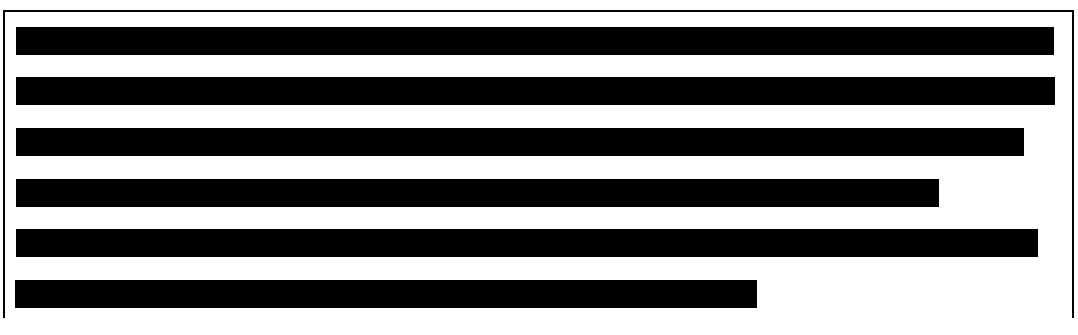
[redacted]

[redacted]



[redacted]





[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

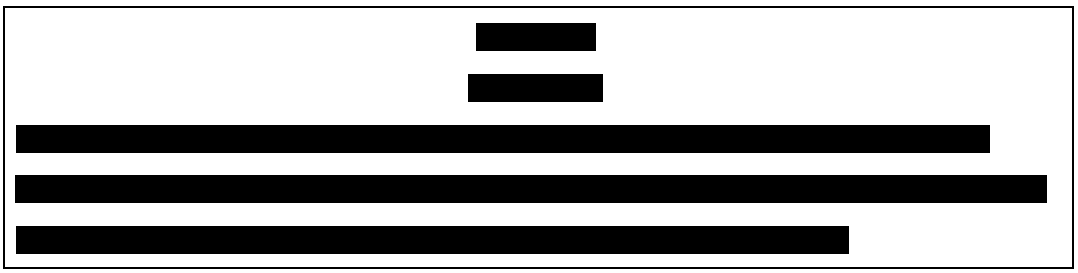
[redacted]

[redacted]

265 [redacted]

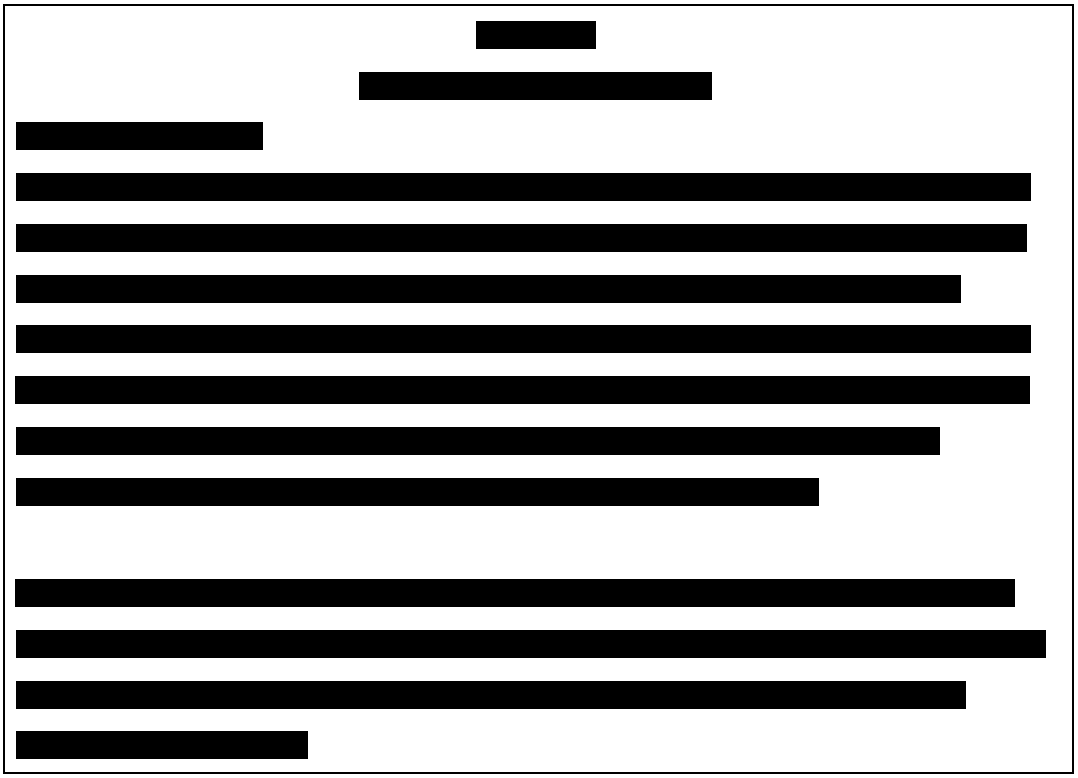
[redacted]

[redacted]

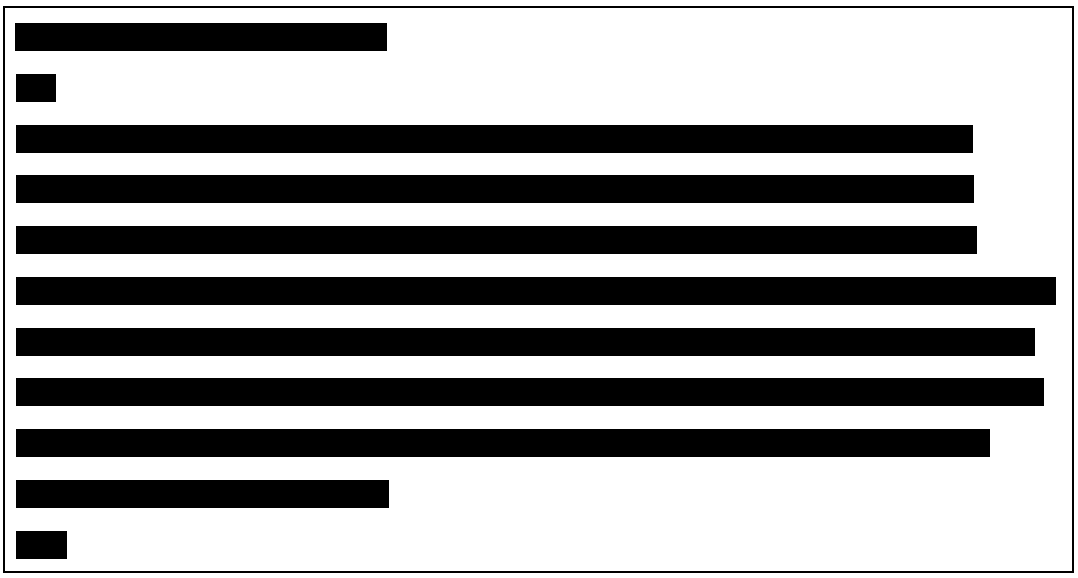


[redacted]

[redacted]



[redacted]



[redacted]

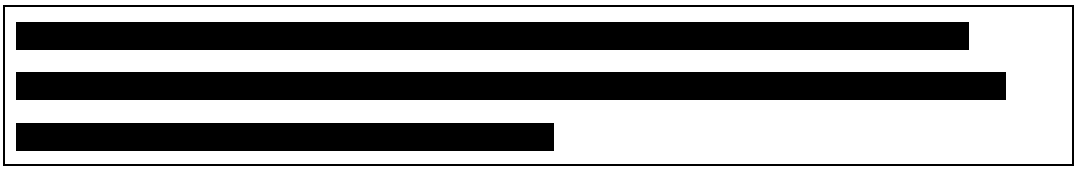
[redacted]

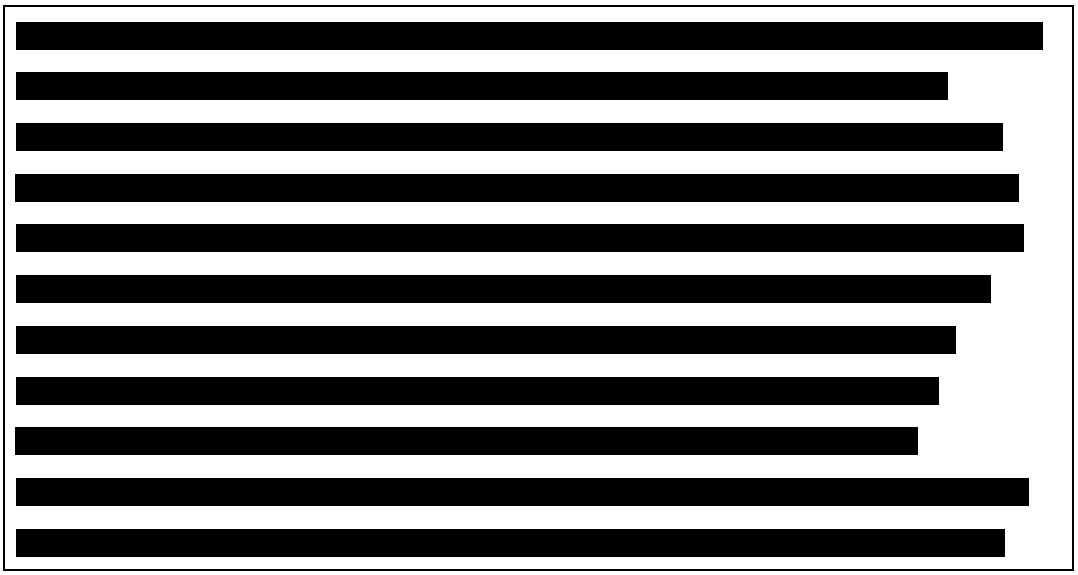
[redacted]

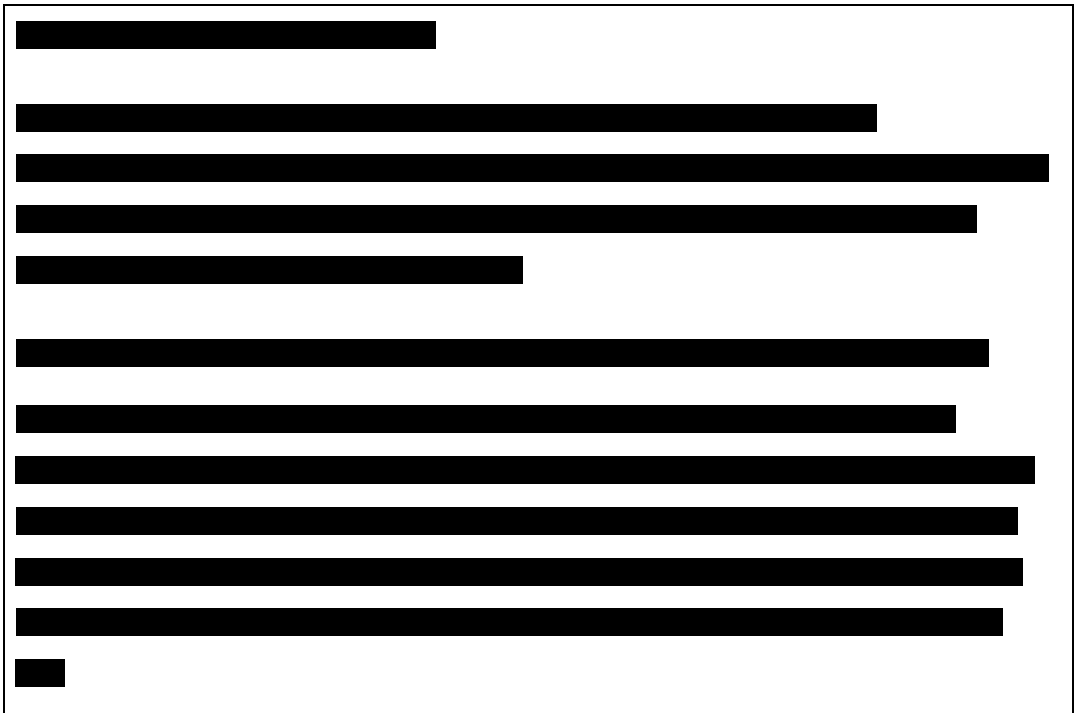
[redacted]

[redacted]

[redacted]







[redacted]

II.

Legal Analysis

276 The GDPR is materially and territorially applicable **(1.).**

277 The processing of the users' iris codes by the Worldcoin Foundation was in violation of Article 32 of the GDPR from 24 July 2023 to 14 May 2024 **(2.)**.

The legal assessment of Art. 32 GDPR is thus limited to the period specified above and does not preclude a future assessment of the period after 14 May 2024 (with regard to both the iris codes and the SMPC shares).

278 The processing of the iris codes and of the SMPC-Shares for the purpose of passive comparison, which includes the processing steps of storing the iris codes / SMPC shares and comparing with them in the event of a new registration of a user, is unlawful in its past and current form under the first alternative of Article 5(1)(a) GDPR and Article 9(1) GDPR as well as the first subparagraph of Article 6(1) GDPR, so that the collected iris codes and SMPC-Shares must be deleted immediately by the Worldcoin Foundation according to Article 17(1)(d) of the GDPR **(3.)**.

In that regard, in addition to the assessment of security under Article 32 of the GDPR, the legal assessment is limited to the processing of the iris codes and SMPC-Shares for the purposes of passive comparison. It is without prejudice to a future reassessment of the lawfulness of the processing, in particular due to changed circumstances related to the processing, other personal data and/or processing for the purpose of active comparison, which includes the processing steps of the collection of pixel images, calculation of the iris code from them and the comparison with the Iris codes already registered.

279 In addition, the Worldcoin Foundation infringed Article 17(1) of the GDPR by not providing data subjects with the means to request or obtain erasure of their iris code and SMPC-Shares **(4.).**

1. Applicability of the GDPR

280 The GDPR applies both materially (a.) and territorially (b.) to the processing of the iris codes and the SMPC-Shares by the Worldcoin Foundation.

a. Material scope of the GDPR, Article 2 of the GDPR

281 The GDPR is materially applicable.

282 The Iris codes and the SMPC-Shares processed by the Worldcoin Foundation constitute personal data pursuant to Article 4(1) of the GDPR (aa.). The processing is carried out in an automated manner (bb.) and there is no exception to the material scope under Article 2(2) of the GDPR (cc.)

aa. The Iris codes and the SMPC-Shares as personal data pursuant to Article 4(1) of the GDPR

283 Both the iris code and the SMPC shares constitute personal data within the meaning of Art. 4 No. 1 GDPR.

(1) The Iris code as personal data pursuant to Article 4(1) GDPR

284 According to Article 4(1) of the GDPR, personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

285 In order to determine whether a natural person is identifiable, the third sentence of recital 26 of the GDPR states that all means reasonably likely to be used by the controller or by another person to identify the natural person directly or indirectly, such as singling out, should be taken into account.

286 According to the fourth sentence of recital 26 of the GDPR, in order to determine whether means are reasonably likely to be used to identify a natural person, all objective factors, such as the cost of and the amount of time required for identification, should be considered, taking into consideration the available technology at the time of processing and technological developments.

287 In the light of these requirements, it is clear that the Iris Code is personal data within the meaning of Article 4(1) of the GDPR for the following reasons:

288 The iris code is a unique identifier of a natural person.

289 As the second part of Article 4(1) of the GDPR makes clear, a distinction can be made between identifiers and 'other personal data'. Other personal data are 'neutral' information, such as: "Account balance = EUR...", "favourite colour = red", "parent of...", etc.

290 'Other personal data', unlike identifiers, do not have the inherent property of identifying or singling out the person to whom they refer to as one among many or all ("indirect" in Article 4(1) GDPR, see CJEU judgment of 7 March 2024 in case C-479/22 P (OC v Commission), paragraph 47). As long as 'other personal data' cannot be associated with an identifier by the controller (or another person), they do not relate to an identified or identifiable natural person within the meaning of the first part of Article 4(1) of the GDPR. However, in the moment in which they can be associated with an identifier, without an actual association taking place, they relate to an identifiable person (second alternative of the first part of Article 4(1) of the GDPR). At the time when they are actually associated

with an identifier, they refer to an identified person (first alternative of the first part of Article 4(1) of the GDPR).

291 Identifiers, on the other hand, are personal data per se because they represent the person him- or herself or – in other words– they represent the person's identity.

292 The Iris code is an identifier which identifies a natural person in a (infinite) crowd of persons, as the Iris code is different for each natural person and reflects the person's physical or physiological identity.

293 The very wording of the second part of Article 4(1) of the GDPR and of the third sentence of recital 26 'singling out' shows that there are, or may exist, other identifiers in addition to the 'classical' social identifier of the name.

294 This notion of the meaning of personal is also used in the context of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty 108), revised in parallel to the GDPR with Protocol 223 (link to the Convention: https://www.coe.int/de/web/conventions/full-list?module=treaty-detail&treatynum=108; Link to the minutes: https://www.coe.int/de/web/conventions/cets-number-/-abridged-title-known?module=treaty-detail&treatynum=223). It is a convention of the Council of Europe. The Convention and Protocol 223 have been ratified by many EU Member States, including Germany. The Protocol was drafted with utmost care to ensure consistency between the Convention and the GDPR (Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 3, available at https://rm.coe.int/16808ac91a). The Explanatory Report to the Protocol states in paragraph 18 that:

295 '18. The notion of 'identifiable' refers *not only to the individual's civil or legal identity* as such, but so to what may allow to *'individualise' or single out (and thus allow to treat differently)* one person from others. This "individualisation" could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, *biometric* or genetic *data*, location data, an IP address, *or other identifier*. The use of a pseudonym or of any digital identifier/digital identity does not lead to anonymisation of the data as the data subject can still be identifiable or individualised. Pseudonymous data is thus to be considered as personal data and is covered by the provisions of the Convention [italic are author's emphasis].'

296 In addition, the Article 29 Working Party (the predecessor of today's European Data Protection Board (EDPB)) has already under the Data Protection Directive (Directive 95/46/EC; the predecessor of the GDPR) stated that there are identifiers other than the name (WP-29, Opinion 4/2007 on the concept of personal data, English version, p. 14, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf).

297 In addition, the purpose of the processing is also a significant indicator as to whether or not an information constitutes personal data. If the processing of the data is aimed at identifying or singling out a person, the argument that it is not personal data constitutes a contradiction in itself (WP-29, Opinion 4/2007 on the concept of personal data, English version, para. 16 et seq.).

298 In the present case, the Iris code is specifically processed for the purpose of determining whether a particular person has already registered with the WorldID infrastructure, in order to take a decision on whether the person is to be registered and receives a certain amount of the crypto-currency Worldcoin or whether registration and payment of the crypto-currency is to be refused.

299 The purpose of processing the iris code is therefore precisely to distinguish one person from another in order to take the decision on registration and payment.

300 According to the settled case-law of the CJEU, information is personal data 'where, by reason of its content, purpose or effect, it is linked to an identifiable person' (CJEU judgment of 7 March 2024 in case C-604/22 (IAB Europe), paragraph 37; see WP-29, Opinion 4/2007 on the concept of personal data, English version, pages 10 et seqq.).

301 The Iris code is an information to which all three characteristics apply. It is undeniably linked to a particular person by its content (see WP-29, Opinion 4/2007 on the concept of personal data, English version, pages 8 and 10). It is also linked by its purpose to a specific person, as it is specifically intended to treat a particular person in a certain way (registration and payment of the cryptocurrency or not) (see WP-29, Opinion 4/2007 on the concept of personal data, English version, page 10). In addition, the processing of the iris code also has an impact on a particular person, at least when that person wishes to re-register for the WorldID infrastructure and the registration and payment of the cryptocurrency Worldcoin are refused (see WP-29, Opinion 4/2007 on the concept of personal data, English version, p. 11).

302 Even if, and contrary to the above consideration, one would argue that identification in a narrow sense must take place, that would be the case here.

303 On the one hand, the controller – the Worldcoin Foundation – has means at its disposal which it could reasonably use to associate the iris code to a particular person in a narrower sense. On the other hand, third parties (reasonably to be included into the considerations) have means available or may have means available within a foreseeable time-frame to carry out such an identification as well.

304 With regard to the first option, it should be noted that the person's iris code can also be obtained from simple images or video recordings if the person's face is in a sufficiently accurate position. Thus, the controller can associate the iris code with an individual on the basis of publicly available images or video recordings, e.g. on social media pages or job portals, if they are of a certain quality, i.e. high image resolution and adequate perspective.

305 As regards the second option, it should be noted that it is not necessary for the controller to hold all the information necessary to identify the data subject in its possession (CJEU judgment of 7 March 2024 in case C-604/22 (IAB Europe), paragraph 40). Accordingly, as the fourth sentence of recital 26 of the GDPR makes clear, it can be sufficient if a third party (reasonably to be included into the consideration) has the means to associate the information with a person. In this case, the information also constitutes personal data for the controller in question (see CJEU judgment of 7 March 2024 in case C-604/22 (IAB Europe), paragraph 47; CJEU judgment of 9 November 2023 in Case C-319/22 (Gesamtverband Autoteil-Handel), paragraph 49). In this regard, as the fourth sentence of recital 26 of the GDPR clarifies, account should not only be taken of the technological means available at the time of processing but also of (foreseeable) technical developments. These can be seen in particular in a possible future dissemination of biometric databases, which could then allow for concatenation of iris codes. In addition, such systems run the risk that iris codes generated by different generation algorithms may nevertheless be associated with one and another with sufficient probability and increasingly less effort. In addition, a central database managed under the responsibility of a single private company is an extremely attractive target for attackers, whether they are morally, financially or politically motivated (see also 2. below). Hence, these attackers and the means at their disposal must also be reasonably included in the assessment (cf. CJEU judgment of 7 March 2024 in case C-479/22 P (OC v Comission), paragraphs 43-66).

306 In its statement (para. 12 and 13) of 14 May 2024, the controller argues that the algorithm for creating the iris code is not available to third parties and that an orb is necessary to create the iris codes.

307 In this regard, it is firstly to be noted that a sufficiently capable third party could procure these means or produce them theirselves.

308 The controller uses the so-called Daughmann algorithm, which is the standard procedure for generating iris codes. The adjustments made to it do not represent a relevant additional level of protection with the efficiency of, for example, cryptographic procedures but at most an additional recoding in the sense of 'security through obscurity', which completely loses its (inadequate) level of protection by means of algorithmic analysis based on many iris code data or the passing on of an internal specification by a Worldcoin employee or an accidental disclosure or loss (e.g. through a hacker attack) of the source code.

309 Secondly, it is not necessary to possess the exact same means Worldcoin possesses in order to be able to establish a link. It is not necessary to be able to reproduce the iris code exactly. A sufficiently similar replica would also suffice in this respect.

310 Thirdly, it is sufficient that the Worldcoin Foundation has the necessary resources at its disposal, to establish a link between the iris code and a person, which has already been described in recital 305.

311 Finally, it should also be noted that the Iris codes do not constitute 'usual' personal data, but rather a special kind of personal data, namely biometric data within the meaning of Article 4(14) GDPR.

312 According to Article 4(14) of the GDPR biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

313 Sentence 3 of recital 51 of the GDPR clarifies that the processing of photographs should not systematically be considered to be processing of special categories of personal data as photographs are covered by the definition of 'biometric data' only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

314 The iris codes are calculated using a specific technical method, the Daughmann algorithm, which has been minimally adjusted by Worldcoin to the sensor developed by Worldcoin, and are to be categorised as biometric templates. Biometric templates represent, according to ISO 24745, a set of biometric features that can be directly compared with other biometric features, which is the case for the iris codes by calculating a distance metric using hamming distance. Thus, Iris codes allow for the unique identification of a natural person and inevitably meet the requirement for classification as a biometric date under Article 4(14) GDPR.

315 It is also clear from the definition of biometric data that a narrow interpretation of the concept of personal data is not appropriate. A fingerprint or, as in the present case, the binary code representing the unique features of a person's iris, must be classified as personal data even if it is not stored in conjunction with or cannot be (directly) linked to a person's name, address and date of birth, since it itself allows the identification or singling out of a specific person and allows the linking of further information to that person or allows taking decisions (in this case, the decision on the registration and payment of the cryptocurrency) concerning that person (see WP-29, Opinion 4/2007 on the concept of personal data, English version, page 8 et seq.).

316 At this point, it should again be highlighted that the question of the classification of a date as biometric data pursuant to Art. 4(14) GDPR and the question of the applicability of Art. 9(1) GDPR are related but separate issues. In paragraph 14 of its statement of 14 May 2024, the controller appears to mix these two issues by stating that "In particular, iris codes are precisely not biometric data and special categories of personal data within the meaning of Art. 9(1) GDPR. The purpose required for this, which would have to be aimed at identifying data subjects, is already lacking."
However, the purpose of uniquely identifying a person is only necessary for the applicability of Art. 9(1) GDPR and represents an additional requirement of Art. 9(1) GDPR compared to Art. 4(14) GDPR. A biometric date, on the other hand, already exists if it 'enables or confirms unique identification' without having to be processed specifically 'for uniquely identifying a natural person'.

317 In its statement of 26 June 2024, the controller expressed again that the iris codes are not to be considered personal data pursuant to Article 4(1) GDPR.

318 It argued that the iris code is no identifier, since it is in no position to calculate or in any other way reconstruct individual irises based on the iris codes (para. 8 of the statement).

319 Furthermore, the controller referred to paragraph 46of the CJEU's judgement of 19 October 2016 in the case *Breyer* (C-582/14) (para. 8, 9 of the statement), where it is stated:

320 "Thus, as the Advocate General stated essentially in point 68 of his Opinion, that would not be the case if the identification of the data subject was *prohibited by law* or *practically impossible* on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant (italic are author's emphasis)."

321 However, Worldcoin Foundation's reasoning is not convincing. The controller misjudges the legal criteria used to characterise an information as personal data.

322 Insofar as the Worldcoin Foundation argues that the iris code is no identifier because it is no position to reconstruct the original iris from it, the Worldcoin Foundation fails to understand that the possibility of reconstruction is neither decisive for classifying the iris code as an identifier / personal data nor for classifying it as biometric data.

323 Article 4(1) GDPR states that the identifier is "[…] *one or more factors specific* to the physical, physiological […] identity […]". The iris code is such a factor specific to the physical/physiological identity of a person. The iris code is unique for each and every person and represents that person. If and as long as an organisation has the means to create the iris code from the (photograph of the) iris of a person, as the Worldcoin Foundation has, the iris code is an identifier for this organisation; the person is 'marked' for this organisation and the organisation can distinguish him or her from other persons on the basis of the iris code.

324 Similarly, Article 4(14) GDPR does not require the reversibility of the technical procedure applied to the physical, physiological or behavioural characteristics.

325 The reversibility of the algorithm under which an identifier was created is therefore neither a requirement under Article 4(1) GDPR nor under Article 4(14) GDPR. It is rather sufficient that the algorithm produces a different result for each person (due to the uniqueness of the human iris), which identifies the respective person.

326 Likewise, the reference of the controller to the judgement of the CJEU in the case *Breyer* is not persuasive.

327 In the case of *Breyer*, the CJEU dealt with the question of whether a dynamic IP address constitutes personal data. A dynamic IP address is information that is volatile and changes over several connections for the internet user (see para. 36 of the judgement). It therefore constitutes 'other

information' which already lacks the permanence required for an identifier; when the IP address expires, the dynamic IP address loses its identifying effect. If a website operator stores the dynamic IP address beyond its expiry date, it is not processing an identifier, but 'other information', which only constitutes personal data for the website operator if it is possible to link it to further additional information, in particular an identifier (second part of Article 4(1) GDPR; see para. 288 et seqq. above). The CJEU had precisely dealt with this question (see para. 44 et seq. of the judgement) and found that the possibility of linking within the meaning of the second part of Article 4(1) GDPR does not exist if the linking is prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power (para. 46 of the judgment).

328 Since the iris code is no 'other information' which requires linking with further additional information but rather uniquely identifies the person by itself, the CJEU's finding in paragraph 46 of the judgement in the case *Breyer* is of no relevance to the case at hand.

329 To the extent as the controller also wishes to express with its submission that an identifier can only ever be the 'classic' civil identifier in the form of the name (in connection with the date of birth and/or place of residence), this claim is to be rejected, as already explained under paragraphs 293 et seqq. above.

330 Moreover, as shown under paragraphs 302 et seqq., also an identification in a narrower sense is feasible for the controller.

331 This identification is neither prohibited by law nor practically impossible.

332 An example for a legal prohibition may be the medical obligation to secrecy (§ 203 of the German Criminal Code (Strafgesetzbuch – StGB)). However, such a legal prohibition applying to the Worldcoin Foundation could not be identified in the present case.

333 Likewise, a disproportionate effort with regard to the (automatic) scanning of online available pictures is not ascertainable.

334 Contrary to the remarks of the controller in paragraph 9 of its statement, identification in a narrower sense is also neither legally prohibited nor practically impossible for third parties which obtain access to the iris codes (cf. para. 305-310 above).

335 In this respect, it should be noted that it is irrelevant whether the manner in which third parties gain access to the iris codes is prohibited by law. Otherwise, personal data would transform into non-personal data for an attacker who has gained access to the data in violation of criminal law. It is obvious that this cannot be the case.

336 Moreover, the GDPR does not constitute a prohibition by law within the meaning of the *Breyer* judgement (cf. Article 5(1)(e) GDPR). Such a finding would constitute a circular reasoning. The legal prohibition could only apply if the GDPR were applicable, but if the prohibition were to apply, the

GDPR would not be applicable. Consequently, the (possible) unlawfulness of linking information to a person under the GDPR does not qualify as a prohibition by law within the meaning of the *Breyer* judgement.

337 The Worldcoin Foundation on the other hand has not provided any explanation as to why the identification is legally prohibited or practically impossible for third parties, and neither is apparent on the basis of other known aspects or reasons. Therefore, the Worldcoin Foundation's submission cannot be followed.

(2) The SMPC-Shares as personal data pursuant to Article 4(1) GDPR

338 Just like an iris code, the SMPC shares represent personal data.

339 In paragraph 5 of its statement of 14 May 2024, the controller states that the iris codes were erased with the introduction of the SMPC system. It follows from this assumption and from paragraph 11 of the statement that the controller does not consider the SMPC shares to be personal data within the meaning of Art. 4(1) GDPR (this also corresponds to the opinion of the controller on the iris codes, see above), but considers the splitting of the iris code into two parts/shares to be an anonymisation measure.

340 However, this assumption cannot be followed for the following reasons:

341 Firstly, the splitting of the iris code into the two shares is under no circumstances an anonymisation measure (for the high requirements for actual anonymisation, see WP-29, Opinion 05/2014 on Anonymisation Techniques), but at most a pseudonymisation measure.

342 According to Article 4(5) GDPR, pseudonymisation means 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

343 The concept of pseudonymisation is closely linked to the concepts of 'indirect' and 'identifiable' in Article 4(1) GDPR (for these concepts, see CJEU judgment of 7 March 2024 in Case C-479/22 P (OC v Commission), paragraphs 47-49). Personal data that has been subjected to pseudonymisation does not, in itself, allow the data subject to be directly identified. However, pseudonymised data can be assigned to a specific person by adding further information.

344 Pseudonymised data constitutes personal data pursuant to Art. 4 (1) GDPR (sentence 2 of recital 26; CJEU judgment of 5 December 2023 in Case C-683/21, para. 58; WP-29, Opinion 4/2007 on the concept of personal data, English version, p. 18).

345 The splitting of the iris code into two shares represents at most a pseudonymisation measure in the current design of the SMPC system, because it is possible for the Worldcoin Foundation to restore the original iris code without major effort by simply merging the two shares.

346 This conclusion is not impeded by the fact that the shares are processed separately by two different companies with their own legal personality - Worldcoin Europe GmbH and Tools for Humanity GmbH - because these two companies, irrespective of any corporate or economic influence (see in a moment, para. 262 below), are already in terms of data protection law as processors of the Worldcoin Foundation within the meaning of Art. 4(8) GDPR bound by instructions of the Worldcoin Foundation, and are therefore not third parties (Art. 4 No. 10 GDPR) with sufficient independence for a fiduciary arrangement. The Worldcoin Foundation is the sole controller within the meaning of Art. 4(7) GDPR and thus alone determines the modalities of the processing. As processors, Worldcoin Europe GmbH and Tools for Humanity GmbH are subject to the instructions of the Worldcoin Foundation (Art. 28 (3) (a) GDPR); they are fully bound by the instructions of the Worldcoin Foundation.

347 The situation is therefore identical to, or at least not significantly different from, a situation in which the Worldcoin Foundation processes the shares in two separate databases operated by itself and managed by two different employees (cf. Art. 29 GDPR).

348 In addition, the three relevant actors - Worldcoin Foundation, Worldcoin Europe GmbH and Tools for Humanity GmbH - are closely intertwined companies whose primary business activities are centred on the Worldcoin project. [redacted] The close corporate, economic and personal ties between these companies must also be taken into account.

349 Secondly, it should be remembered that both processors - Worldcoin Europe GmbH and Tools for Humanity GmbH - use the same cloud infrastructure and the same cloud service provider, namely Amazon AWS. This means that there is only a virtual or logical separation (access rights etc.) of the databases. [redacted]

350 The means of other actors must also be taken into consideration. As already mentioned in paragraph 305 above, a centralised database of biometric data is an extremely attractive target for all kinds of attackers. Splitting the iris codes into shares has not eliminated this aspect. Although two shares per person are now processed instead of one iris code per person, both shares are processed in the same cloud infrastructure. This makes the cloud service provider an extremely attractive target and a 'single point of failure'.

351 Thirdly, the shares are processed for the purpose of identifying or singling out a person in order to determine whether the person is already registered and, accordingly, to make a decision regarding registration and payment of the cryptocurrency (cf. paragraphs 297-301 above). They are therefore linked to a specific identifiable person due to their purpose and effects. Rejecting the nature of the shares' as personal data would constitute a contradiction in itself (cf. paragraph 297 above).

352 Finally, it should be clarified that the shares are also biometric data within the meaning of Art. 4(14) GDPR.

353 Although the iris codes may have been pseudonymised by splitting them into shares, as Articles 6(4)(e), 25(1), 32(1)(a), sentence 2 and 3 of 89(1) GDPR and recitals 28, sentence 1 of 29, sentence 2 and 3 of 78, sentence 2 and 3 of 156 GDPR illustrate, pseudonymisation is an organisational and technical measure that particularly may have positive effects with regard to the principle of data minimisation pursuant to Article 5(1)(c) GDPR and the security of data processing, but which does not eliminate an information's nature as personal data (see paragraphs 341 et seqq. above).

354 Similarly, pseudonymisation does not remove an information's nature as 'biometric date'. Although the algorithm used for splitting the shares - which is subject to detailed future examination - may only produce random numbers that no longer have any visible connection to the original iris code from which they were generated, however, the effects and risks inherent to the iris codes are preserved in the shares. For example, the person who has access to both shares – as the Worldcoin Foundation - can not only restore the original iris code by merging the shares, but can also clearly identify a person based on one of their physical or physiological characteristics, namely the appearance of their iris, even without merging the shares. The Worldcoin Foundation itself demonstrates this on a daily basis. Instead of calculating the similarity of an iris code to an already stored or registered iris code, two 'partial similarities' are now calculated, the result of which is combined at the end and thus provides information as to whether a person is already registered or not. Only the number of calculations has increased, the result, however, remains the same: a person can be distinguished from all other people by the Worldcoin Foundation based on the appearance of their iris. In this respect, splitting the iris code may improve security, since - which is subject to a more in-depth examination - an unauthorised person needs access to both shares in order to be able to uniquely identify a person based on the appearance of his or her iris, but for the Worldcoin Foundation the shares are nevertheless biometric data within the meaning of Article 4(14) GDPR, albeit possibly pseudonymised.

355 In in its statement of 26 June 2024 (para. 10-13) the Worldcoin Foundation rejects the classification of the SMPC-Shares as personal data, especially the findings under paragraphs 345-347 and paragraphs 349-350. It argues that the finding that it is able to merge the SMPC shares without major effort (para. 345) is based on incorrect assumptions. The assumption that the Worldcoin Foundation could instruct the processors involved in the process to merge the SMPC shares on the

basis of its authority to issue instructions (para. 346) is incorrect. The opposite is the case: merging the SMPC shares is not permitted and practically impossible for the Worldcoin Foundation or at least involves a disproportionate effort. [redacted] The nature of an data processing agreement does not contradict this approach. Consequently, the present constellation differs significantly from the situation described in paragraph 347. Furthermore, the fact that the entities involved in the SMPC process use the same cloud service provider - in this case AWS - is not relevant. According to common sense, it is impossible or at least completely implausible that an attacker could succeed in hacking the databases of several participating entities (para. 350) despite AWS's extensive security systems. Equally remote is the assumption that AWS could merge the SMPC shares on its own initiative (para. 349).

356 Worldcoin Foundation’s arguments cannot be followed.

357 Whether the SMPC shares can or cannot be merged is irrelevant for the characterisation of the SMPC shares as personal data under Article 4(1) GDPR. As already explained in paragraphs 351 and 354, the SMPC shares are processed by the controller for the purpose of identifying / singling out / recognising a person. The aim of the controller is to be able to determine for each and every person whether the person is already registered or not. For this purpose, the controller utilises the inherent individuality of each person's iris. If data is processed for the purpose of identifying a person, the argument that it is not personal data constitutes a contradiction in itself (see para. 351 and para. 297). Furthermore, it is not just a mere wishful thinking of the Worldcoin Foundation to be able to determine on the basis of the SMPC-Shares whether each individual person is already registered or not, but it rather proves it on a daily basis (see para. 354).

358 Notwithstanding this and despite the Worldcoin Foundation's submission, there are also not sufficient indications that it is legally or practically impossible for the Worldcoin Foundation to merge the SMPC shares or that it requires a disproportionate effort from the Worldcoin Foundation.

359 [redacted]

[redacted]

360 However, the Worldcoin Foundation fails to realise that the aforementioned contractual provisions in no way turn the SMPC shares into anonymised data. Rather, the SMPC shares are in any case pseudonymised data, even when taking these provisions into account, as the definition of 'pseudonymisation' in Article 4(5) GDPR shows. [redacted]

361 [redacted] Only the Worldcoin Foundation has the authority to determine the means of the processing; something else may be true if an from the Worldcoin Foundation independent third party would process a part of the SMPC shares on its own authority (cf. para. 346 above).

362 [redacted] However, these are unilaterally amendable by the Worldcoin Foundation at any time by means of 'individual instructions' (point 2. under the heading 'The Instructions (Duration and Subject Matter of Processing)'), which cannot be derogated from as expressed in letter a) of the first subparagraph of Article 28 GDPR and in Article 29 GDPR. [redacted] Even if the instruction is unlawful or if the 'individual instruction' violates the instructions provided for in the original data processing agreement, the processor is in principle bound by these instructions (see the second subparagraph of Article 28(3) GDPR and EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 146 et seq.). According to the concept of the GDPR, the processor is merely an 'extended arm' of the controller or a 'tool' used by the controller. The controller is always the person who exercises control over the processing (cf. Art. 4(7) and (8) GDPR). This aspect is also reflected in the data processing agreements. [redacted]

[redacted]

363 [redacted] Insofar as one may use the 'test' of the CJEU's judgement in the case *Breyer* for assessing this aspect (cf. para. 319 et seqq. above), which the controller appears to do, the conditions laid down there are not met in the present case (due to the above and the following reasons). The controller has neither provided (sufficient) evidence nor is it apparent from other aspects that the Worldcoin Foundation is prohibited by law(!) from merging the SMPC shares or that the merging is practically(!) impossible for the Worldcoin Foundation on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of merging appears in reality to be insignificant.

364 The Worldcoin Foundation has not named a specific law(!) that prohibits the Worldcoin Foundation from merging the SMPC shares, nor is such a norm apparent by itself (see already para. 332 above).

[redacted]

365 Likewise, it is not apparent that merging the SMPC shares would practically(!) be impossible for the Worldcoin Foundation.

366 [redacted]

367 But also, irrespective of this, it is not apparent as to how the merging of the SMPC shares would not only require a great but a disproportionate effort. Technically the merging of the SMPC shares should be not difficult to realise and would only require some few human and financial resources, if any.

[redacted]

[redacted]

374 The third reason is that the Worldcoin Foundation could, as the creditor, release the respective processor from its payment obligation by way of a release agreement or a negative acknowledgement of debt (§ 397 of the German Civil Code (Bürgerliches Gesetzbuch – BGB), see also *Dennhardt*, in BeckOK BGB, § 397 BGB, para. 16).

375 The forth reason is that the close interlacing between the parties involved in the SMPC system must be taken into account in all these considerations (see para. 348 above). Diametrical conflicts of interest between the parties involved are not identifiable, so that contractual arrangements between these parties cannot constitute a sufficient factor which makes the risk of merger of the SMPC shares insignificant. This is indisputably the case in the relationship between the Worldcoin Foundation and Worldcoin Europe GmbH. [redacted] Worldcoin Europe GmbH is therefore a company that does not determine its conduct (on the market) autonomously, but carries out the instructions given to it by its parent company, the Worldcoin Foundation. The same bodies that determine the conduct of the Worldcoin Foundation also determine the conduct of the Worldcoin Europe GmbH (see CJEU judgment of 25 October 1983 in Case 107/82 (AEG v Commission), para. 49 et seq.; see also *Bayer/Schmidt*, in BeckOGK, § 37 GmbHG, para. 44 et seqq., 46). [redacted]

376 [redacted] Prior Termination of the data processing agreements is also not necessary for financial reasons (double payment). [redacted]

[redacted]

377 The statements of the Worldcoin Foundation regarding any third parties which are to be included into the assesement of the SMPC shares' character as personal data must also be rejected.

378 First, attackers being able to gain access to both SMPC databases (despite AWS's extensive security systems) is neither impossible nor entirely remote. This is demonstrated by various hacks of large service providers, such as the Microsoft hack in which attackers were able to steal a Master key for the Azure cloud (https://www.heise.de/news/Klatsche-fuer-Microsoft-US-Behoerde-wirft-MS-Sicherheitsversagen-vor-9674431.html - German newspaper article). This is not to say that (experienced) attackers should always be included as third parties in the assessment of whether information is personal data in accordance with the third sentence of Recital 26 GDPR. However, the processing carried out by the Worldcoin Foundation is not "everyday" processing. The Worldcoin Foundation processes biometric data of several million people from various countries. In addition, the Worldcoin Foundation ultimately wants to extend its activities to (almost) every country on earth. Its goal is to create the world's largest identity and financial network (see para. 582). With such extensive and intensive processing of particularly sensitive data, the databases maintained by the Worldcoin Foundation are not only a target for attackers with 'ordinary' skills, but also for particularly skilled attackers, be they criminals who generally pursue financial interests, morally motivated attackers ('hacktivists') or state attackers. In view of these special circumstances, (experienced) attackers as third parties and their means of identifying a person should also be reasonably included in the assessment of whether the (iris codes and) SMPC shares are personal data.

379 Second, the assumption that AWS could merge the SMPC shares on its own authority is also not so remote that this possibility is to be excluded from consideration. As already stated above, the merger does not involve a practical disproportionate effort, regardless of contractual limitations. Besides, no contractual limitations exist in relation to AWS (contrary to Article 28(4) GDPR), in particular no contractual penalty clause, analogous to those of the main data processing agreements. According to paragraph 10 of the Worldcoin Foundation's response dated 18 September 2024, only the 'standard' data processing agreement ('AWS Data Processing Addendum'), which AWS provides to all its customers, was agreed.

380 Third, a government agency can gain access to the SMCP shares by means of a request for disclosure. This is not affected by Point 17.4 of the data processing agreements, which stipulates that the request must always be challenged unless the Worldcoin Foundation, after careful assessment, concludes that the request is lawful. [redacted] In accordance with the reasons set out in paragraph 378, the possibility of state access to the SMPC shares must be included in the assessment. It should be noted that the assessment only concerns the categorisation of the SMPC shares as personal data within the meaning of Article 4(1) GDPR and does not entail any judgement on the permissibility of the disclosure. Particularly in case of such sensitive personal data as the ones in question and the expected increased interest in them, including by government agencies, effective protection must be ensured, especially concerning the lawfulness of the processing in accordance with Art. 6, 9 GDPR and the transfer to any third countries in accordance with Chapter V of the GDPR. Consequently, the possibility of access by state authorities is, in the present case, not to be regarded as so marginal that this aspect can be disregarded in the assessment of the SMPC shares as personal data pursuant to Article 4(1) GDPR (cf. paragraph 378).

bb. Processing of the iris codes and SMPC shares by automated means

381 The iris codes and SMPC shares are processed by automated means.

382 Processing is defined in Article 4(2) GDPR as any operation or set of operations which is performed on personal data, whether or not by automated means. As the list of examples in Article 4(2) GDPR shows, the concept of processing must be understood broadly.

383 Moreover, the processing of the iris codes and SMPC-Shares is undoubtedly carried out by automated means, since it is in digital form (see only CJEU judgment of 14 February 2019 in Case C-345/17 (Buivids), paragraphs 29 et seqq.).

cc. No exception to the material scope under Article 2(2) of the GDPR

384 There is obviously no exception to the material scope under Article 2(2) GDPR applicable in the present case.

dd. Interim result

385 Since the Iris Code and the SMPC-Shares constitute personal data within the meaning of Article 4(1) GDPR which is processed by automated means and no exception under Article 2(2) GDPR is applicable, the GDPR is materially applicable.

b. Territorial scope of the GDPR, Article 3(1) of the GDPR

386 The GDPR is also territorially applicable.

387 Under Article 3(1) GDPR, the GDPR applies to the processing of personal data in so far as it is carried out in the context of the activities of an establishment of a controller or processor in the Union, irrespective of whether the processing takes place in the European Union.

388 The Iris Codes and SMPC-Shares are processed by the Worldcoin Foundation in its capacity as controller within the meaning of Article 4(7) GDPR (aa.) in the context of the activities (cc.) of the Bavarian establishment of the Worldcoin Foundation, namely the Worldcoin Europe GmbH, which is established in Munich (bb.).

389 The applicability of the GDPR under Article 3(1) GDPR with regard to the Worldcoin Foundation is also not precluded by the fact that Worldcoin Europe GmbH has its own data protection role as a processor under Article 4(8) GDPR (dd.).

aa. The Worldcoin Foundation as controller pursuant to Article 4(7) GDPR

390 According to the findings, the Worldcoin Foundation determines the purposes and means of the processing of the iris codes and the SMPC-Shares and is therefore the controller under Article 4(7) GDPR with regard to that processing.

bb. Worldcoin Europe GmbH as an establishment of the Worldcoin Foundation

391 An establishment implies the effective and real exercise of activity through stable arrangements (second sentence of recital 22 of the GDPR). The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect (third sentence of recital 22 of the GDPR). According to the case law of the CJEU, the concept of 'establishment' is to be understood broadly (see also, on the concept of establishment, EDPB,

Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.0, page 6 et seq.). Any real and effective activity exercised through stable arrangements, even if it is minimal (CJEU judgment of 1 October 2015 in Case C-230/14 (Weltimmo), paragraph 31) is sufficient.

392 The Worldcoin Europe GmbH, which has its registered office in Munich, forms a subsidiary of the Worldcoin Foundation. Since the design phase, the Worldcoin Europe GmbH has been significantly involved in the continuous technological development of the Worldcoin project.

393 Consequently, the Worldcoin Europe GmbH exercises effective and real activity in a stable manner and constitutes an establishment of the Worldcoin Foundation within the meaning of Article 3(1) GDPR.

cc. The processing of the iris codes in the context of the activities of Worldcoin Europe GmbH

394 The further condition laid down in Article 3(1) of the GDPR, according to which the processing must take place 'in the context of the activities' of an EU establishment, is also fulfilled, since in the present case the processing takes place in the context of the activities of Worldcoin Europe GmbH.

395 In the so-called 'Google Spain decision' (Case C-131/12), the Court of Justice of the European Union required that the activity of the EU establishment be 'inextricably linked' to the data processing of the controller. However, such an 'inextricable link' does not require the European establishment to carry out the processing itself or play any role in it at all (see paragraph 52 et seqq. of the judgment and EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.0, page 8).

396 In the 'Google Spain decision', the CJEU considered it sufficient that the Spanish establishment (Google Spain) promoted the sale of advertising space on the search engine operated by the US parent company (Google Inc.) and thus to make the operation of the search engine profitable (paragraph 55 et seqq. of the judgment).

397 In the present case, the link between the processing of the Iris codes by the Worldcoin Foundation and the activities of Worldcoin Europe GmbH is even closer than in the 'Google Spain decision'.

398 The contribution of the Worldcoin Europe GmbH to the processing in question is beyond mere economic support. The Worldcoin Europe GmbH is involved in the processing of the iris codes as a processor pursuant to Articles 4(8), 28 of the GDPR since 21 March 2024 and is therefore an integral part of the processing.

399 Furthermore, as pointed out by the Worldcoin Europe GmbH (at that time "ZipCode GmbH") and the Worldcoin Foundation in their comments of 22 March 2024, the Worldcoin Europe GmbH was also an indispensable protagonist in the development and design of the system used, which would be fundamentally different without Worldcoin Europe GmbH's contributions. To this day Worldcoin Europe GmbH significantly contributes to the further development of the system, e.g. in the form of

code contributions and participation in both technical and leadership meetings regarding the specification of the Orb verification process.

400 It must therefore be assumed that there is an 'inextricable link' within the meaning of the case-law of the Court of Justice between the processing of the iris codes / SMPC-Shares and the activities of the Worldcoin Europe GmbH. Timewise, the 'inextricable link' exists since the design phase and lasts until today.

dd. Applicability of Article 3(1) of the GDPR with regard to the Worldcoin Foundation despite Worldcoin Europe GmbH's role as processor

401 The territorial applicability of the GDPR in relation to the Worldcoin Foundation cannot be refuted on the basis of the argument that the Worldcoin Europe GmbH is now playing a role in the processing taking place within the Worldcoin project, namely as a processor of the Worldcoin Foundation. It is true that, on pages 10 et seqq. of Guidelines 3/2018, the EDPB makes clear that processing in the context of the establishment of a processor does not automatically result in the territorial applicability of the GDPR in relation to the controller located in a third country. However, the EDPB in its remarks clearly assessed the situation of processor and controller not being economically intertwined and not having a relationship under company law, but as being two completely independent bodies. In the present case, however, Worldcoin Europe GmbH is a subsidiary of the Worldcoin Foundation, with the result that it not only acts as a processor for the processing carried out by the Worldcoin Foundation, but it also constitutes an establishment of its parent company within the meaning of Article 3(1) of the GDPR.

402 The concept of establishment within the meaning of Article 3(1) of the GDPR and the concept of controller and processor under Article 4(7)(8) of the GDPR are concepts which have a systematically different purpose and which have a completely different direction of impact.

403 The concept of establishment is related to the local applicability of the GDPR under Article 3(1) of the GDPR (and the competence for cross-border processing under Article 56 GDPR). Whereas, the terms 'controller' and 'processor' are used to describe the individuals or bodies being subjects to the regime of the GDPR.

404 Ultimately, a different interpretation of Article 3(1) of the GDPR would run counter to the objective of the GDPR, which is to ensure a high level of protection of natural persons with regard to the processing of their personal data (Recital 10, 11 GDPR). Article 3(1) of the GDPR is therefore not to be interpreted restrictively (see CJEU judgment of 15 June 2021 in Case C-645/19 (Facebook Ireland and Others), paragraph 91; CJEU judgment of 1 October 2015 in Case C-230/14 (Weltimmo), para. 25; CJEU judgment of 13 May 2014 in Case C-131/12 (Google Spain and Google), paragraph 53).

405 It would be paradoxical if the GDPR were to the applied to a controller from a third-country which only has a 'simple' establishment in the EU, which is not involved in the data processing, but were not to be applied to a controller from a third country whose EU establishment is directly involved in the processing even as a processor.

406 This would make it extremely easy for controllers from third countries with an establishment in the EU to prevent or limit the applicability of the GDPR (for a list of the few aspects/provisions that would be monitorable/applicable if the GDPR were only to be applied with regard to the processor, see EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.0, pages 12 et seq.).

407 The third-country controller could significantly limit the applicability of the GDPR to its processing by means of a simple contract.

ee. Interim result

408 In accordance with Article 3(1) of the GDPR, the GDPR applies to the processing of the iris codes and SMPC-Shares by the Worldcoin Foundation in its capacity as controller, as the processing is carried out in the context of the activities of the Worldcoin Europe GmbH. The fact that the Worldcoin Europe GmbH acts as a processor is irrelevant to the applicability of the GDPR with regard to the Worldcoin Foundation, but rather establishes a close link between the activities of the Worldcoin Europe GmbH as the EU-establishment of the Worldcoin Foundation and the processing carried out by the Worldcoin Foundation.

c. Interim result

409 The GDPR applies materially and territorially to the processing of the iris codes and the SMPC-Shares by the Worldcoin Foundation.

2. Infringement of Article 32 of the GDPR

410 Under Article 32 of the GDPR, a level of protection appropriate to the risk must be ensured, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Appropriate technical and organisational measures shall be implemented to effectively mitigate this risk. Under Article 32(1)(a) of the GDPR, measures of pseudonymisation and encryption are appropriate.

411 At Worldcoin, the iris codes, which are in principle to be classified as biometric personal data with a high risk to the rights and freedoms of natural persons, were at least from 24 July 2023 until 14 May 2024 stored in plain text.

412 This form of storage enables a range of misuse possibilities should unauthorised persons access this data (e.g. by means of a cyberattack) or should Worldcoin unintentionally disclose it (e.g. due to a misconfiguration of the access options to the database via the Internet).

413 In such cases, it would be possible in individual cases to use the plain text iris codes to calculate back image fragments of the iris of Worldcoin users, from which conclusions can also be drawn about the health situation of natural persons in individual cases (e.g. eye melanomas). Despite the loss of information when transferring iris images to the plain text iris code, this is due to the fact that eye diseases such as ocular melanomas can (sometimes) be characterised in the iris images by strong colour differentiation from the otherwise healthy iris and these clear differences are not only found as characteristic features in the plain text iris codes, but could also be statistically significant in a reconstructed iris image, which does not necessarily have to have an obvious similarity to the original iris image, due to a distribution of light and dark pixels.

414 Furthermore, it is possible under certain circumstances that these back-calculated image fragments, although they sometimes no longer match the original pixel image of an iris, can still be used as the basis for calculating a unique iris code of a data subject - e.g. for registration with other biometric systems by means of an eye scan outside the World ID infrastructure.

415 It is also possible for plain text iris codes to be compared with other plain text iris codes from other biometric systems by calculating a similarity value, which can lead to the ability to interlink different biometric systems.

416 In the case of Worldcoin, this is also not prevented by their individual adjustments to the algorithm used for generating the iris code, as the basic information content of a human iris remains sufficiently accurate and the adjustments to the generation algorithm do not have any protective function with the strength of a cryptographic process, for example, but at most implement a re-coding of bit patterns that can also be sufficiently traced back using artificial intelligence, for example.

417 It is also possible that a plain text iris code from the Worldcoin system could be stolen without authorisation and entered into another biometric system as a supposedly valid iris code, e.g. in a search system that may also be used in a third country in which no legal avenue may be available for challenging such classification as a wanted criminal.

418 When assessing the risk of misuse of biometric data, a significantly longer period of time must be assumed for the protection of biometric data compared to commonly used IT systems without biometric data, e.g. an online shop with access by means of a password.

419 In view of today's assumed life expectancy and the earliest possible registration age of 18 years, a period of approx. 80 years is therefore assumed in this review. This means that risks must also be considered that could extend into the year 2100.

420 Although it is hardly possible to reliably look into such a distant future, it is by no means the case that assessments with a view to future time spans would otherwise not be carried out.

421 In the field of encryption, for example, it is common to estimate time spans for specific encryption methods for which it can be assumed that they are sufficiently secure (or not) according to the current state of the art, e.g. in the technical guideline "BSI TR-02102 Cryptographic methods: Recommendations and key lengths" of the German Federal Office for Information Security.

422 As things currently stand the World ID infrastructure could become the largest biometric database in the world operated by a private company, as this infrastructure, according to its technical design and business model is intended to collect data of billions of data subjects as World ID users. For the reasons laid out in the previous paragraph, when assessing a level of security in accordance with Article 32 GDPR for the storage of plain text iris codes, it is assumed that the legal environment that allows for access to the Word ID infrastructure could change within the long protection period of 80 years in such a way that government agencies could gain access to the iris code database.

423 The service provider Amazon AWS, which operates Worldcoin's plain text iris code database, must also be considered in the specific technical implementation.

424 It must also be assumed that a very large, possibly even the largest biometric database in the world, could be an attractive target for cybercriminals with the aim of data extraction and blackmail (ransomware), for political actors who want to spread their own political message (hacktivism) or even for state-directed cyberattackers who carry out such attacks as part of a covert operation.

425 It is a generally recognised basic assumption in the discipline of computer science that biometric data, be it iris codes, templates of facial images or fingerprints, must never be stored in plain text, as the risk of misuse is too high and, unlike passwords, for example, which can be changed after an attack, there is no possibility of mitigation if such misuse has taken place due to the immutability of biometric data.

426 With biometric data, for example, it is not possible for a data subject to “grow” a new eye.

427 The protection of biometric data is the subject of a separate discipline in computer science, which aims to achieve biometric security using technical methods in such a way that, for example, it is possible to compare different iris codes, but the risks described above can occur with a significantly reduced probability - these methods are also called "biometric template protection schemes".

428 The protection of biometric data is now also defined in relevant ISO standards (ISO/IEC 24745), which, even if the use of biometric data is not currently widespread in companies, makes it clear that biometric data requires a special protection framework.

429 [redacted]

430 [redacted]

431 These protective measures represent the state of the art in the protection of personal data that is processed, for example, in online retail, such as names, addresses, payment methods or order histories.

432 However, it is now also common practice in online retail that personal data that is assumed to be at high risk of attack, such as credit card data including the security code, is generally no longer stored by online retailers themselves, but instead there are requirements from credit card companies that credit card data may only be stored by companies that have undergone PCI DSS certification - this sets highest standards for information security management, which, for example, go beyond purely technical protection constructs as described above.

433 Due to the high risk of a (future) attack or access by state authorities (possibly from third countries that do not provide for an adequate level of data protection), the BayLDA comes to the conclusion that IT protection measures as described above cannot be sufficient for the protection of biometric data, as these cannot be effective in the case of governmental orders to surrender (as Worldcoin itself has access to the plain text iris codes and could therefore - from a technical point of view - also surrender them) and, secondly, they would not be sufficient to implement an appropriate level of security with regard to cybercriminals or state attackers, assuming they have the appropriate motivation.

434 It would be conceivable, for example, that the firewall protection could be circumvented in such a way that an attacker gains access to a Worldcoin computer that is not blocked by the firewall, obtains administration rights at Worldcoin by means of rights escalation, or gains access to a Worldcoin computer that is not blocked by the firewall (although this requires a high level of technical expertise, this is a common procedure in the case of ransomware attacks, for example, and these techniques lead to a successful attack on a company almost every day in Bavaria) and thus also creates opportunities to bypass two-factor authentication (using man-in-the-middle techniques) and can also remove possible role rights restrictions.

435 Even encrypted storage (at database level) does not provide sufficient protection here, as it continues to contain iris codes in plain text when the database is running (which should generally be the case 24/7 for Worldcoin, unless the database system is temporarily shut down completely for maintenance purposes). Encrypted storage (at database level) creates a protective framework, especially when replacing hardware (hard drives) or when creating backups, which is a sensible and sometimes necessary basic measure in accordance with Article 32 GDPR when processing personal data, but does not ensure specific protection against access to the biometric plain text iris codes, as these are available in plain text (at least temporarily, but usually permanently) in the main memory

of Amazon's cloud server, at the latest when the distance is calculated using the Hamming code comparison algorithm.

436 The BayLDA therefore comes to the conclusion that the protection of biometric data, as described, cannot be ensured at IT system level, but must take place at data level. This means that even if an attack successfully overcomes access protection measures, the risks to the rights and freedoms of data subjects must be mitigated to the extent that iris codes are not stored in plain text. Instead, methods from the group of "biometric template protection schemes" would be suitable for ensuring such protection in accordance with Article 32 GDPR.

437 Worldcoin asserts in its statement of 14 May 2024 in para 18 – without describing any possible and specific attack scenarios – that the security measures taken are not only appropriate, but also go far beyond the relevant IT and data security standards, including with regard to the protection of biometric data. As already explained here, it must be assumed that measures to protect biometric data at IT system level cannot be sufficient when biometric data is stored centrally, especially not with standard IT and data security measures such as firewalls, two-factor authentication and role/rights concepts, which are now commonly implemented even by those controllers which process less critical data than biometric templates, e.g. smaller online shops or SMEs when using cloud services.

438 Instead, protective measures at data level must be implemented that fall into the category of 'Biometric Template Protection Schemes'. These would be, for example, protection measures from the group of 'homomorphic encryption methods', in which biometric data is transferred into a cryptographic space with protection at the level of strong encryption, or so-called Bloom filters, in which a loss of information is implemented in such a way that a statistical similarity determination can be carried out, but a reconstruction of plain text iris codes is very unlikely. However, secure multi-party computation schemes (SMPC schemes) are also possible, provided that their algorithmic design and specific implementation are suitable for achieving an adequate level of protection in accordance with Art. 32 GDPR. As the specific implementation of these schemes is crucial to achieving an adequate level of protection, the Worldcoin SMPC system, for which only a sketch outlining the system is currently available, will be examined in detail in the future.

439 Since Worldcoin **stored iris codes in plain text** and only implemented security measures at IT system level in timeline 1 (see above), this constitutes an **infringement of Article 32 GDPR, as no measures** were implemented **at data level** ("biometric template protection schemes").

3. Unlawful processing of the Iris codes and the SMPC-Shares for the purpose of passive comparison and the obligation to erase the iris codes and SMPC-Shares without undue delay

440 The processing of the iris codes and the SMPC-Shares of the data subjects for the purpose of passive comparison, which includes the processing steps of storing the iris codes / SMPC-Shares as well as the comparison with them in the event of a new registration of a user, is unlawful under Article 9(1) of the GDPR (a.).

441 The unlawfulness of the processing results – beside from Article 9(1) GDPR – also from Article 6(1) GDPR (b.).

442 Due to the unlawfulness of the processing of the iris codes for passive comparison purposes, the Iris codes must be deleted immediately by the Worldcoin Foundation in accordance with Article 17(1)(d) of the GDPR, both in plain text and in the form derived from them ('SMPC shares').

a. Unlawfulness of the processing of the iris codes and of the SMPC-Shares for the purpose of passive comparison under Article 9(1) of the GDPR

443 The iris codes have been and, insofar as the SMPC system - contrary to the statements of the data controllers - is not yet (fully functional) in use (which remains to be examined separately), are still being processed for the purpose of passive comparison in violation of Art. 9 para. 1 GDPR (aa.).

444 The same is true for the SMPC-Shares (bb.).

aa. Unlawfulness of the processing of the iris codes for the purpose of passive comparison under Article 9(1) of the GDPR

445 Under Article 9(1) of the GDPR, the processing of the 'sensitive data' (cf. sentence 5 of recital 10) referred to therein is in principle prohibited. Processing of such data can only be considered if one of the conditions referred to in Article 9(2) GDPR is met (processing is only lawful if, additionally, one of the grounds for justification under the first subparagraph of Article 6(1) GDPR were to be fulfilled, see II. 3.a.).

446 In the present case, the Worldcoin Foundation processes the iris codes for the purpose of passive comparison in violation of Article 9(1) GDPR, as an iris code constitutes biometric data pursuant to Art. 4(14) GDPR (1), the Worldcoin Foundation processes it 'for the purpose of uniquely identifying a natural person' within the meaning of Article 9(1) GDPR (2) and no exception under Article 9(2) GDPR applies (3).

(1) The Iris-code as biometric data pursuant to Article 4(14) of the GDPR

447 The iris-code constitutes biometric data pursuant to Article 4(14) of the GDPR (see II. 1. a. aa. (1)).

(2) The processing of the Iris-codes "for the purpose of uniquely identifying a natural person" within the meaning of Article 9(1) of the GDPR

448 The processing of iris codes for the purpose of passive comparison by the Worldcoin Foundation constitutes the processing of biometric data 'for the purpose of uniquely identifying a natural person' within the meaning of Article 9(1) GDPR.

449 Worldcoin's assertion (statement of 14 May 2024, para. 14 and statements of 17 May 2024, para. 3-6/8) that the iris codes are not processed for the purpose of uniquely identifying natural persons cannot be followed.

450 The Worldcoin Foundation processes the iris codes to determine whether a person is already registered in the WorldID infrastructure. This is achieved by collecting a current template of the person wishing to register and comparing it with all templates in the database of already registered users (so-called '1:n comparison') to determine whether the current template is a duplicate with regard to a template already in the database (this is also referred to as 'deduplication' in information technology). If it is a duplicate, the user will be denied (re-)registration and payment of the Worldcoin cryptocurrency.

451 The Worldcoin Foundation does not see this as a situation of processing 'for the purpose of uniquely identifying a natural person', as the processing is not aimed at verifying or finding a specific person, but only at verifying whether the person who wishes to register is a 'person' in the generic sense. It does not know the identity of its users.

452 However, the Worldcoin Foundation fails to understand that processing 'for the purpose of uniquely identifying a natural person' does not require the biometric template to be linked to traditional identifiers such as name, address, date of birth or that these traditional identifiers appear as a result at the end of the process. As already explained in detail under II. 1. a. aa., 'identification' within the meaning of the GDPR does not require such a link. Rather, it is sufficient if the biometric template is processed in order to recognise or identify one person among many or all.

453 This is the case here. The Worldcoin Foundation uses the collected and permanently stored biometric template of a person's iris to distinguish this person from all other persons by means of a comparison and, based on this, decides whether a person who wishes to register may do so or not and whether an amount of the cryptocurrency Worldcoin will be paid out to him or her.

454 The conclusion that 'deduplication processes' are also covered by Art. 9 (1) GDPR can be inferred from the legislative history of the criterion 'for the purpose of uniquely identifying a natural person',

further EU legislation in the form of the Regulation laying down harmonised rules on artificial intelligence and relevant EDPB guidelines.

455 Neither the Commission's legislative proposal nor the (informal) position of the Council of the European Union, with which it started into the (informal) trilogue negotiations, referred to biometric date as a special category of personal data under Article 9(1). However, the European Parliament's first-reading legislative resolution, with which the Parliament started into the trilogue negotiations, listed biometric data in Article 9(1) (for this situation, see Council document 10391/15, page 266, available at https://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf).

456 During the trilogue procedure, biometric data was then included in the catalogue of Article 9(1) on a proposal from the Parliament. However, the Parliament and the Council agreed on the Council's proposal to include the addition 'for the purpose of uniquely identifying a natural person' in today's Article 9(1) GDPR. The reasons for this addition can be deduced from the Council document 14824/15 (available at https://data.consilium.europa.eu/doc/document/ST-14824-2015-INIT/en/pdf). Paragraph 7 on page 3 states:

457 '7. The European Parliament proposes to include in the list of sensitive data whose processing is in principle prohibited a reference to biometric data. The modernised Convention 108 of the Council of Europe defines biometric data *that uniquely identify* a person to qualify as sensitive data. In the Council's General Approach, the definition of biometric data is *based on specific technical processing*. In order to find an agreement with the European Parliament, the Presidency proposes *to further highlight this aspect* when including biometric data in Article 9: "biometric data specifically processed to uniquely identify an individual". *The Presidency indicates that this would not cover simple authentication via biometric data and allow for a more contextual approach*. An addition in recital (41) may be included to clarify that biometric data are to be considered as falling under special categories of personal data only if they are processed in order to uniquely identify an individual. *Such biometric data would only be covered by Article 9 if they take the form of templates*.'

458 This extract gives, in addition to reference to the already under II. 1. a. aa. (1) mentioned link between the GDPR and Convention 108 of the Council of Europe, various indications as to how to interpret the phrase 'for the purpose of uniquely identifying a natural person'.

459 On the one hand, it is based on Convention 108 where biometric data are classified as sensitive data when 'uniquely identifying a person' (for the exact text, see Protocol 223, page 4, available at https://rm.coe.int/16808ac918). On the other hand, the addition seeks to underline the fact that personal data only amounts to biometric data if they resulted from specific technical processing and if they are available as 'templates'.

460 In addition, the Council Presidency points out that this addition would allow for a more contextual approach and that simple authentication by means of biometric data would thus not be covered by Article 9 of the GDPR.

461 Further guidance on the interpretation of the element can be found in the adopted and by now in the Official Journal of the European Union published, but not yet in force, Regulation laying down harmonised rules on artificial intelligence (Regulation (EU) 2024/1689: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689; in the following called „AI Act").

462 According to the first sentence of recital 14 of the AI Act, the concept of 'biometric data' in Article 3(34) of the AI Act is to be interpreted in the light of Article 4(14) of the GDPR, Article 3(18) of Regulation 2018/1725 and Article 3(13) of Directive 2016/680.

463 The second sentence of recital 14 of the AI Act states that 'biometric data can allow for authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons. A distinction between those operational purposes is also made in recitals 15 to 18 and the corresponding definitions in Article 3(34) to (36) and (39) to (43).

464 The difference between authentication/verification and identification lies in the purpose and way in which the comparison is carried out.

465 The purpose of authentication/verification is to confirm a claim. Usually, this is the claim to be a certain person (and, if applicable, to have certain permissions because of that). In the context of authentication, a specific biometric template is stored for each person representing this person. If someone claims to be a specific person, a recent biometric template of this someone is created and compared with the template stored in the database for the person who this someone claims to be. Thus, authentication/verification involves a 1:1 comparison (see also the definition of 'biometric verification' in Article 3(36) of the AI Act). It should be noted that 'person' in the above does not necessarily mean the civil identity. It can also be an assertion such as 'owner of the device', 'employee number ...' etc. The focus of authentication or verification is usually on determining whether the subject/individual (not the civilian identity) who submits to the authentication or verification process is authorised to do something or have access to certain resources, such as being allowed to enter a certain room or use a certain device, by comparing a currently created biometric template of the subject with a previously created and permanently stored template of the same subject. Therefore, certain authorisations are usually linked to the permanently stored template (see also the second sentence of recital 15 of the AI Act).

466 The purpose of identification, on the other hand, is to identify a person under a multitude of persons by creating a recent biometric template of the person to be identified and comparing it with all or a majority of templates stored in the database. A 1:n comparison is made (see the definition of 'biometric identification' in Article 3(35) of the AI Act and recitals 15 and 17). What has already been

said about authentication or verification also applies here, namely that 'person' does not mean the civil identity, but refers to the subject/individual as such.

467 In addition, as Article 3(41) of the AI Act makes clear with its definition of 'remote biometric identification system' (see also recital 17 of the AI Act), a distinction can be made between biometric identification without and with the active involvement of the person as sub-forms of 'biometric identification'.

468 A vivid example of the use of biometric identification is the monitoring of a busy public square using real-time biometric analysis. A biometric template is created for people entering the square using biometric camera systems. As the person moves around the square, their movements and actions can be tracked by the camera systems. For this purpose, a biometric template of the person is repeatedly generated in real time or at extremely short intervals and compared with all other processed templates (see also the definition of 'real-time remote biometric identification system' in Article 3 No. 42 of the AI Act and Recital 17). If the person behaves incorrectly, e.g. by assaulting another person, stealing or damaging monuments, the real-time biometric monitoring prevents him or her from disappearing into the crowd and he or her may, for example, be apprehended by law enforcement authorities when leaving the square. This kind of system and the biometric data processed within such system are used 'to uniquely identify natural persons'. A link between person/subject and civilian identity does not take place in the context of biometric real-time surveillance and is also not necessary.

469 Biometric categorisation has the purpose of placing a person in a specific category on the basis of biometric data/information/characteristics. Categorisation may refer to sex, age, hair colour, eye colour, tattoos, behavioural characteristics, etc. (see the definition of 'biometric categorisation' in Article 3(40) of the AI Act and Recital 16).

470 Considering the legislative history of Art. 9(1) GDPR described above and the further EU legislation in the form of the AI Act, it becomes clear that the processing of iris codes carried out by the Worldcoin Foundation for the purpose of passive comparison constitutes processing 'for the purpose of uniquely identifying a natural person' within the meaning of Art. 9(1) GDPR.

471 When introducing the criterion 'for the purpose of uniquely identifying a natural person', the legislator made it clear that the processing of biometric templates falls under Art. 9(1) GDPR and that only procedures that could be categorised as 'simple authentication' should not be covered by it.

472 The AI Act supports this assumption and clarifies the various purposes and uses of biometric data.

473 As can be inferred from the definition of 'biometric identification' in Article 3(35) of the AI Act it is sufficient, in order to assume the criterion 'for the purpose of uniquely identifying a natural person' being fulfilled, that the person is identified or singled out on the basis of the comparison of the

biometric sample-template with the templates stored in the database. Establishing the civil identity is not necessary. Accordingly, a deduplication comparison is sufficient with regard to the criterion 'for the purpose of uniquely identifying a natural person', since the comparison uses the unique nature of the biometric date to 'mark' that person or – in other words – to make certain determinations concerning that person (here: registered vs not yet registered).

474 Worldcoin stores and processes an iris code for the purpose of passive comparison, i.e. to be able to recognise a person among a large number of people (global population). The iris code is not only processed to assign a person to a category, such as 'blue-eyed or brown-eyed', but is also used to identify, individualise and single out a person. This is not just a verification of 'person' in a generic sense, as Worldcoin claims, but rather an identification of 'person X' in a specific, individualised sense. With the processing, Worldcoin does not want to only determine whether the subject in front of the orb is 'a person' or 'a human being' (put simply: if it has a human head, two human arms, two humans legs, ten human fingers and ten human toes), but it rather presumes the humanness of the subject and wants to determine whether this person is already registered or not. The processing is linked to the individuality or – in other words – to the individual characteristic of a person's iris, which is exactly why biometric data is used.

475 The definition of "biometric identification" of Article 3(35) of the AI Act reads as follows:

476 '(35) 'biometric identification means' the automated *recognition of physical, physiological, behavioural, or psychological human features* for the purpose of establishing the identity of a natural person *by comparing biometric data of that individual to biometric data of individuals stored in a database*.'

477 This conclusion is also supported by the relevant publications of the EDPB.

478 Most recently, in connection with the legal framework for the use of facial recognition technology in law enforcement ('Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement' of 26 April 2023), the EDPB clarified with regard to the classification of identification and authentication procedures using biometric data in the context of Article 10 of Directive 2016/680, which is identical in content to Article 9 GDPR:

479 "Like any biometric process, facial recognition can fulfil two distinct functions:

• the authentication of a person, aimed at verifying that a person is who she or he claims to be. In this case, the system will compare a pre-recorded biometric template or sample (e.g. stored on a smartcard or biometric passport) with a single face, such as that of a person turning up at a checkpoint, in order to verify whether this is one and the same person. This functionality therefore relies on the comparison of two templates. This is also called 1-to-1 verification.

• the *identification of a person*, *aimed at finding a person among a group of individuals*, within a specific area, an image or a *database*. In this case, the system must process each face captured, to generate a biometric template and then check whether it matches with a person known to the system. This functionality thus relies on comparing one template with a database of templates or samples (baseline). This is also called *1-to-many identific*ation. For example, it can link a personal name record (surname, first name) to a face, if the comparison is made against a database of photographs associated with surnames and first names. It can also involve following a person through a crowd, *without necessarily making the link with the person's civil identity* [italic are author's emphasis]." (Guidelines 05/2022, para. 10).

"While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a *processing of special categories of personal data* [italic are author's emphasis]." (Guidelines 05/2022, para. 12).

480 That the processing of the iris codes by the Worldcoin Foundation for the purpose of passive comparison falls under Article 9(1) GDPR can also be inferred from the 'Guidelines 3/2019 on the processing of personal data by video devices'.

481 There, the EDPB (like the AI Act) distinguishes the processing of biometric data 'for uniquely identifying' from processing for the purpose of 'categorisation' (EDSA, Guidelines 3/2019 on the processing of personal data by video devices, Version 2.0, R. 80).

482 Furthermore, it is clear from the first example in paragraph 78 concerning check points at airports, the example in paragraph 83 concerning the shop owner and the first example in paragraph 85 concerning the hotel and the related statements in R. 79, 82 and 84 that the EDPB considers it sufficient for Article 9(1) of the GDPR that biometric data is processed for the purpose of comparison with a database of already existing biometric data. A link to a 'classical' identifier is not required.

483 This is particularly clear from the example in paragraph 83, where a shop owner uses a biometric facial recognition system in order to distinguish or individualise its customers, so as to be able to display tailor-made advertising to each customer while visiting the shop. The shop owner does not know the name of his or her customers, but can distinguish them from each other on the basis of the biometric characteristics of the face and thus identify them.

484 Moreover, this assumption follows from the fact that the collection of biometric templates from non-registered persons (i.e. not in the database) should also, in the view of the EDPB, fall under the regime of Article 9 GDPR. For non-registered users, there is not yet a biometric template in the database. It is obvious that the non-registrant cannot be associated with other identifiers, such as the name, by collecting an up-to-date template, at the moment the non-registered person enters the area covered by the video surveillance, and by the comparison against the database, because

there is no template in the database to compare the up-to-date template to and thus no link to or for additional information regarding the non-registrant.

485 The EDPB, therefore, considers that an exemption under Article 9(2) of the GDPR is necessary for all persons covered by a camera, regardless of whether they are already registered in the database or not (paragraph 84 et seq. of the Guidelines).

486 Furthermore, it is clear from the example in paragraph 78 of the Guidelines regarding the access management to a building and the examples in paragraph 85 of the Guidelines regarding the hotel and the concert hall that it is sufficient for the applicability of Article 9(1) GDPR if the comparison serves the primary objective of determining whether a specific person/individual is in the (comparison) database (cf. also para. 479). Being able to distinguish all persons from one another and thus to single out out the respective person is a necessary prerequisite for this determination. The identification of the person is therefore a necessary and thus intended transitional stage of this primary objective. The controller wants to or must be able to distinguish a person from all other persons, i.e. to be able to identify a person, in order to determine whether this person exists in the database and thus possess a certain attribute which is assigned to all persons in the database by the controller, e.g. being authorised to access the building (example in para. 78 of the Guidelines), being a VIP guest (example in para. 85 of the Guidelines), being a concert visitor (example in para. 85 of the Guidelines) or - as here - being (already) registered. The result of this determination is then (regularly) linked to measures regarding this person; he/she is allowed/denied entry, is given special treatment as a VIP guest/receives only the 'standard treatment' or, in the present case, is allowed to participate in the Worldcoin project (and thus apply for grants, trade the cryptocurrency Worldcoin or authenticate with his/her World ID with third-party services connected to the system) or participation is refused (and thus all of the above options/services are not available to him/her).

487 In summary, it can therefore be deduced from the legislative history of Article 9(1) of the GDPR, the provisions of the AI Act, which reflect as manifestations of the uniform understanding of the legislator, this legislative history and the relevant publications of the EDPB that the processing of iris codes for the purpose of passive comparison falls under Article 9(1) of the GDPR.

488 In its statement of 26 June 2024 (para. 15) the Worldcoin Foundation argued again that the iris codes are not being processed to identify a user but to categorise him or her. The processing's purpose is only to categorise users into "new human user" and "existing human user".

489 However, the Worldcoin Foundation misunderstands the term 'categorisation', as used by both the EU legislator in Art. 3 No. 40 of the AI Regulation and the EDPB in recital 80 of Guidelines 3/2019. It fails to understand that the processing it carries out is not for 'categorisation' within the meaning of EU law, but for '(unique) identification'.

490 Article 3(40) of the AI Act defines 'biometric categorisation system' as follows:

"'biometric categorisation system' means an AI system for the purpose of assigning natural persons to specific categories *on the basis of their biometric data*, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons;" (italic are author's emphasis)

491 [The original German draft decision explains in this paragraph and the following that the word "unless" ("sofern nicht" in German) is accidently missing in the German version of Article 3(40) of the AI Act]

492 [placeholder]

493 Recital 16 of the AI Act explains the term 'biometric categorisation' in more detail:

"The notion of 'biometric categorisation' referred to in this Regulation should be defined as assigning natural persons to specific categories *on the basis of their biometric data*. Such specific categories can relate to *aspects such as sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or political orientation*. This does not include biometric categorisation systems that are a purely ancillary feature intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of this Regulation. For example, *filters categorising facial or body features* used on online marketplaces could constitute such an ancillary feature as they can be used only in relation to the principal service which consists in selling a product by allowing the consumer to preview the display of the product on him or herself and help the consumer to make a purchase decision. *Filters* used on online social network services which *categorise facial or body features* to allow users to add or modify pictures or videos could also be considered to be ancillary feature as such filter cannot be used without the principal service of the social network services consisting in the sharing of content online."

(italic are author's emphasis)

494 Recital 30 of the AI Act, which relates to the prohibition of certain biometric categorisation systems under letter g) of the first subparagraph of Article 5 of the AI Act, has the following content:

"Biometric categorisation systems that are *based on natural persons' biometric data*, such as an individual person's face or fingerprint, *to deduce or infer* an individuals' political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation should be prohibited. That prohibition should not cover the lawful labelling, filtering or categorisation of biometric data sets acquired in line with Union or national law according to biometric data, such as the *sorting of images according to hair colour or eye colour*, which can for example be used in the area of law enforcement."

(italic are author's emphasis)

495 Point 1 of letter b) of the Annex III of the AI Act, which carries the headline "High-risk AI system referred to in Article 6(2)", reads:

> "AI systems intended to be used for *biometric categorisation, according to sensitive or protected attributes or characteristics* based on the *inference of those attributes or characteristics*;" (italic are author's emphasis)

496 Sentence 5 of Recital 54 of the AI Act especially explains what "sensitive or protected attributes" are:

> "In addition, AI systems intended to be used for biometric categorisation according to *sensitive attributes or characteristics protected under Article 9(1) of Regulation (EU) 2016/679 on the basis of biometric data*, in so far as these are not prohibited under this Regulation, and emotion recognition systems that are not prohibited under this Regulation, should be classified as high-risk." (italic are author's emphasis)

497 [At this paragraph the original German draft decision gives an additional translation of Sentence 5 of Recital 54 of the AI Act deviating from the original one cited in para 496 above, because the official German translation of Sentence 5 of Recital 54 of the AI Act is not very comprehensible]

498 In summary, this means that biometric categorisation, unlike biometric identification, is not used to recognise a person. Unlike in the case of biometric identification, there is no comparison of a person's biometric data with previously stored biometric data in the case of biometric categorisation (cf. Article 3(35) of the AI Act, see para. 476 above) in order to distinguish the person from other persons.

499 The differences between biometric categorisation and biometric identification (in the sense of Article 9(1) GDPR) essentially consist of the following key points:

- The main difference lies in the fact that, unlike with biometric identification and biometric verification/authentication, in the case of biometric categorisation no comparison or reference templates are (permanently) stored, with which a later momentarily created template is being compared (cf. also EDPB, Guidelines 3/2019 on the processing of personal data by video devices, Version 2.0, para. 80).
- In biometric categorisation, conclusions or findings are drawn or obtained directly from the characteristics of one or more physical, physiological or behavioural features. Categorisation therefore takes place directly on the basis of the characteristics. In contrast, in the case of biometric identification and biometric verification/authentication, the conclusion is not derived or obtained directly from the characteristics of one or more biometric features, but not until comparing the biometric feature (in the form of a biometric template) with one (verification/authentication) or more (identification) biometric feature(s) already stored.

- In this respect, it can also be said that biometric categorisation is linked to the "external properties/characteristics" of a biometric datum, while biometric identification and biometric verification/authentication are linked to the "inherent property" of individuality of a biometric datum (which results from the fact that the external properties/characteristics differ from person to person). Biometric categorisation is not interested in this property; however, it is a central and indispensable basis for biometric identification and biometric verification/authentication.

500 Regarding the processing of the iris codes, conclusions are not drawn directly from the (external) characteristics of a person's iris, but the individuality of the iris is utilised in order to be able to recognise a person by way of a comparison with already stored (binary/numerical representations of) irises and deny him or her (multiple) participation in the Worldcoin project.

501 Hence, the Worldcoin Foundation's statement of 26 June 2024 (para. 15) that the iris codes are only processed "for categorisation" is incorrect. The iris codes are rather processed "for the purpose of uniquely identifying a natural person" within the meaning of Art. 9(1) GDPR.

(3) No exception under Article 9(2) of the GDPR being applicable

502 Processing that is covered by Article 9(1) GDPR is generally prohibited. It can only be permitted if (at least) one of the exceptions set out in Article 9(2) GDPR is applicable (processing is only lawful if one of the justifications in Article 6(1)(1) GDPR is also fulfilled in addition to the exceptions of Article 9(2) GDPR, see b. below).

503 For the processing of iris codes for the purpose of passive comparison, however, none of the exceptions under Article 9(2) GDPR is applicable.

504 Only the exception of explicit consent under Article 9(2)(a) GDPR is even conceivable for the processing in question. However, there is no (valid) consent from the data subjects for the processing of the iris codes for the purpose of passive matching.

505 Consent is defined in Article 4(11) as any *freely given*, *specific*, *informed* and *unambiguous indication of the data subject's wishes* by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

506 In accordance with Articles 7(1) and 5(2) of the GDPR, the controller is required to prove that the data subject has consented to the processing of his or her personal data.

507 According to the facts established, the Worldcoin Foundation obtains consent to the processing of in the context of the registration of a user for the World-ID infrastructure via the "World App". In the registration dialogue, the user must actively accept the "Biometric Data Consent Form". Irrespective of the fact that this is a multi-layered approach to obtaining consent and the first layer lacks any "basic information" such as the identity of the controller or the purpose of the processing (cf. recital

42 sentence 4 of the GDPR; EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, footnote 42), the consent given, according to the clear wording of the 'Biometric Consent Form', covers only the case of 'to calculate derivatives of the Image data (like the Iris Code) and actively compare it against our database'. The storage of the iris code after registration and the passive comparison is not covered by this. With regard to these processing steps or – in other words – with regard to the purpose of passive comparison, the Worldcoin Foundation asserts a legitimate interest in defending itself against fraudulent users who unlawfully try to register more than once.

508 Therefore, irrespective of the fact that consent may be invalid on the basis of other factors, there is already no declaration of consent by the data subjects for the further storage and the passive comparisons. These specific cases (cf. Article 4(11) of the GDPR) or – in other words – the purpose of carrying out passive comparisons (cf. Articles 9(2)(a), 6(1)(a) of the GDPR) is not covered by the consent statement of data subjects.

bb. Unlawfulness of the processing of the SMPC-Shares for the purpose of passive comparison under Article 9(1) of the GDPR

509 What is stated under aa. applies mutatis mutandis with regard to the processing of the SMPC shares. Likewise, the processing of the SMPC shares for the purpose of passive comparison is in violation of Art. 9 (1) GDPR.

510 The SMPC-Shares constitute, even if potentially in pseudonymised form, biometric data pursuant to Article 4(14) of the GDPR (see II. 1. a. aa. (2)).

511 The SMPC-Shares are also processed 'for the purpose of uniquely identifying a natural person' within the meaning of Art. 9 (1) GDPR.

512 According to Worldcoin's statement, following the introduction of the SMPC system, only SMPC shares are processed for the purpose of passive comparison instead of plain text iris codes. As already described under II. 1. a. aa. (2), this does not fundamentally change the processing procedure. Instead of comparing a sample iris code with all stored iris codes, the sample iris code is compared with the SMPC shares stored by the respective processors - Worldcoin Europe GmbH and Tools for Humanity GmbH. The total distances are then calculated from the partial distances and used to determine whether a person is already registered or not. As already explained under II. 1. a. aa. (2), the only thing that ultimately changed is an increase in the number of calculations (in addition to a possible improvement of security). The purpose of the processing, which is aimed at recognising a person and thus at 'uniquely identifying a natural person', has not changed with the introduction of SMPC shares.

513 Likewise, the terms of the declaration of consent, which is submitted by users as part of the registration dialogue and only covers the collection of the iris code and the active comparison of the iris code with the stored SMPC shares of other users, but not the permanent storage of the SMPC shares and the passive comparison with them, remains unchanged.

514 Consequently, no exception under Article 9(2) of the GPDR applies to the processing of the SMPC shares for the purpose of passive comparison, resulting in a violation of the prohibition of Art. 9(1) GDPR and, therefore, in the unlawfulness of the processing.

b. Unlawfulness of the processing of the iris codes and the SMPC-Shares for the purpose of passive comparison under the first subparagraph of Article 6(1) GDPR

515 As is apparent from the wording of Article 6(1) of the GDPR, processing of personal data is lawful only if and to the extent one of the provisions of the first subparagraph of Article 6(1) of the GDPR are fulfilled. If the processing does not fall within one of these cases, the processing is unlawful (see, one for many, CJEU, judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), paragraph 90; so-called 'prohibition subject to authorisation').

516 As the CJEU has recently clarified and as follows from sentence 6 of recital 51 GDPR, Article 6 GDPR remains applicable even if Article 9 GDPR applies to the processing (CJEU, judgement of 21. December 2023 in Case C-667/21 (Krankenversicherung Nordrhein), paragraphs 71 et seqq.). Processing of personal data covered by Article 9 GDPR is therefore lawful only if it not only complies with the requirements of one of the exceptions laid down in Article 9(2) of the GDPR, but also meets the requirements of at least one of the provisions under Article 6(1) (CJEU, judgement of 21. December 2023 in Case C-667/21 (Krankenversicherung Nordrhein), paragraphs 71 et seqq.).

517 The iris codes have been and, insofar as the SMPC system - contrary to the statements of the data controllers - is not yet (fully functional) in use (which remains to be examined separately), are still being processed for the purpose of passive comparison in violation of Art. 9(1) GDPR (aa.).

518 The same is true for the SMPC-Shares (bb.).

aa. Unlawfulness of the processing of the iris codes for the purpose of passive comparison under the first subparagraph of Article 6(1) GDPR

519 The processing of the iris codes of the data subjects for the purposes of passive comparison is unlawful in the absence of any relevant justification under Article 6(1) of the GDPR.

520 In the present case, the processing of the Iris codes by the Worldcoin Foundation does not meet the requirements for a ground of justification in the first subparagraph of Article 6(1) of the GDPR, in particular, there is no valid consent of data subjects to the processing of the iris codes for the

purpose of passive comparison pursuant to point (a) of the first subparagraph of Article 6(1) GDPR (1) nor can the Worldcoin Foundation rely on overriding legitimate interests in accordance with point (f) of the first subparagraph of Article 6(1) GDPR (2).

(1) Lack of valid consent of data subjects to the processing of the iris codes for the purpose of passive comparison

521 In accordance with point (a) of the first subparagraph of Article 6(1) of the GDPR processing of personal data is lawful where the data subject has given consent to the processing of the data for one or more specific purposes.

522 However, data subjects have not given consent to the processing of their iris codes for the purpose of passive comparison (see above II. 3. a. aa. (3) on Article 9 GDPR).

(2) No justification for the processing of the iris codes for the purpose of passive comparison under point (f) of subparagraph 1 of Article 6(1) of the GDPR

523 In the absence of valid consent pursuant to point (a) of the first subparagraph of Article 6(1) GDPR the processing of the iris codes for the purpose of passive comparison must meet the conditions of another legal basis under the first subparagraph of Article 6(1) GDPR in order to be lawful.

524 As the CJEU has held, "[...] the justifications provided for in that latter provision [Note: points (b) to (f) of the first subparagraph of Article 6(1) of the GDPR], in so far as they allow the processing of personal data carried out in the absence of the data subject's consent to be made lawful, must be interpreted restrictively" (CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), paragraph 93).

525 For the processing of the iris codes for the purpose of passive comparison, point (f) of the first subparagraph of Article 6(1) GDPR – on which the Worldcoin Foundation according to its 'biometric consent form' also relies – is the only legal basis of the ones mentioned in the first subparagraph of Article 6(1) GDPR whose application is conceivable.

526 However, the requirements of point (f) of the first subparagraph of Article 6(1) of the GDPR are not met in the present case, because the interests and fundamental rights of the data subjects override the legitimate interest of the Worldcoin Foundation and any third parties pursued with the processing of the iris codes.

527 For processing to be lawful under point (f) of the first subparagraph of Article 6(1) GDPR three cumulative conditions must be met:

528 'First, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or fundamental freedoms and rights of the person concerned by the data protection do

not take precedence over the legitimate interest of the controller or of a third party' (CJEU judgment of 4 July 2023, Meta Platforms and Others, C-252/21, paragraph 106).

529 As regards the legitimate interest, the existence of a legitimate interest is not subject to excessive requirements. In principle, any economic, legal or moral interest is sufficient.

530 In the present case, the Worldcoin Foundation is pursuing the purpose of creating a 'Proof of Personhood' with its Worldcoin or World ID project. This should also have advantages for third-party providers. Third parties who connect their services to the World ID infrastructure (e.g. app or website operators) can therefore assume with greater certainty that the person registering with the service is a real person and not an automated software service than is the case when simply requesting 'classic' registration methods such as entering an email address including username and password. Furthermore, a person who has been blocked by a third-party service, e.g. because they have violated the terms of use, can be excluded from registering again, e.g. with a different email address.

531 The Word ID infrastructure of Worldcoin therefore also fulfils the role of a new type of identity provider in such a way that the uniqueness of a user for a service can be ensured (by means of certain character strings in the zero-knowledge protocol).

532 Thus, the operation of World ID Infrastructure serves the interest of third parties connected to the infrastructure to protect their systems (cf. Recital 49 sentence 4 GDPR).

533 The processing of the iris codes for the purpose of passive comparison also serves the Worldcoin Foundation's interest in preventing multiple registrations and the accompanying payment of the cryptocurrency Worldcoin to the same individuals. Irrespective of whether multiple registration would constitute criminal fraud (Section 263 of the German Criminal Code (Strafgesetzbuch – StGB) (cf. Recital 47 sentence 6 GDPR), the processing takes place in the pursuit of a legitimate (economic) interest of the Worldcoin Foundation.

534 However, it should be noted that the payment of the cryptocurrency, which must first be "requested" by a user after registration (via the World app) (so-called " WLD Grants "), whereby a reservation of WLD-Grants is also possible before registration (so-called " WLD Reservations "), is made on a purely voluntary basis by another company, World Assets Limited. According to Section 2.12 of the Terms of Use, neither the Worldcoin Foundation nor World Assets Limited or any other company involved in the Worldcoin project is under any contractual obligation issue the grants (see the FAQs on the Worldcoin homepage at "Will I receive Worldcoin (WLD) tokens after I verify my uniqueness?" available at https://worldcoin.org/faqs; for the Terms of Use see https://worldcoin.pactsafe.io/rkuawsvk5.html#contract-qx3iz24-o).

535 However, in the present case, the interests, freedoms and fundamental rights (Articles 7 and 8 of the Charter of Fundamental Rights of the European Union) of the data subjects override the interests of the Worldcoin Foundation and any third parties pursued by the processing.

536 The iris code is – as already mentioned in section II. 1. a. aa. (1) – biometric data in accordance with Article 4(14) of the GDPR and thus particularly sensitive data.

537 The high sensitivity of a biometric date, and therefore the iris code, is based in particular on the following four characteristics of a biometric date:

538 First, biometric data, such as the Iris code, allows to uniquely identify a person (Article 4(14) of the GDPR). This property is inherent to a biometric data. Unlike with other personal data (and other identifiers within the meaning of the second part of Article 4(1) GDPR), the identification of a specific person among a number of persons, possibly covering the entire world population, is possible without the need to combine more than one information just on the basis of the biometric date alone. In contrast, for example, the name of a person on its own usually (provided that the group in question is not particularly small or the name is extremely rare) does not allow for the identification of that specific person. The name needs to be combined with other information, such as the date of birth, the residential address and/or the place of birth, in order to be able to identify a person remotely as reliable as by biometric data.

539 Secondly, biometric data is immutable or, quite precisely, can only be modified if the person inflicts physical suffering on him- or herself. In order to change the biometric data collected in the present case, the iris code, a person would either have to remove the eye or undergo a surgery which changes the iris. By contrast, changing 'simple' personal data is often easily possible. A person can change his/her home address, e.g. by moving. Accordingly, the person is no longer 'Thomas Müller, residing in Munich', but 'Thomas Müller, residing in Nuremberg'. The outdated information is therefore of no value and anyone who only has this outdated information will no longer be able to identify the person behind that information. 'Other personal data' therefore changes or may change over time, while for biometric data this is principally not the case.

540 The third aspect, which makes a biometric date particularly sensitive and can be described with 'honesty' of a biometric date, which is closely linked to the aspect of immutability. The word honesty is principally positively connotated in society, while the word 'lie' is often attributed a negative meaning. However, there are situations where it is practical to be able to lie. A simple example of a practical lie could be if one is, for example, coerced into providing his or phone number in an online shop. Because one does not want to receive unsolicited advertising calls, one gives a wrong phone number. However, there are not only situations in which the possibility to lie is practical, but rather necessary or even vital. For example, in (German) labour law there is also a right to lie on particularly intimate questions of the potential future employer which are unrelated to work, such as pregnancy,

illness, trade union membership, religious affiliation, existence of debts, etc. The possibility to lie about one's identity and not being (simple) to single out is not only important for prisoners of war and political dissidents, but can relevant to each and every one. However, biometric data deprives a person of this possibility.

541 That point gives rise to the fourth and final characteristic of biometric data resulting from the three 'basic characteristics' described above, namely the potential for abuse inherent in biometric data and already mentioned under II. 2. For example, if further information can be linked to a biometric date, a profile of that person can be created which is permanently attached to that person. The person cannot separate him- or herself from that profile either by changing factual circumstances or by lying.

542 A biometric date is therefore more closely related to a personal identification number (cf. Article 87 of the GDPR) than to other personal data or identifiers, such as the name.

543 In addition, in the specific case, the risks of abuse go beyond the general risks associated with the processing of biometric data and are particularly high.

544 The Iris code is not any biometric date, but an even more sensitive date compared to other biometric data.

545 The Iris code is extremely reliable in identifying a person. Other biometric data, such as those resulting from behavioural characteristics (Article 4(14), third variant, of the GDPR) are not nearly as reliable.

546 The Iris code is simpler to use and can be used in a wider spectrum of situations. Today, there are not only extremely many cameras in the public sphere, such as public spaces, traffic lights, railway stations, etc., but also in the private sphere, such as in workplaces, shops, banks, etc. In addition to this amount of image data of a person, which is often produced by a third-party unknown to the person, there is also image data from the person him- or herself, such as posted on social media or job portals.

547 Unlike a fingerprint, which cannot be used in a simple manner because it disappears quickly (fully or partially), is covered by other prints (fully or partially) and because close contact with the person is necessary to remove it, the iris code obtained from images of the face can be used in a more straightforward, versatile and clandestine way.

548 Other factors which in the present case create a particularly high risk to the fundamental rights of the data subjects are the central storage of the iris codes and the inappropriateness of the security of the processing of the iris codes in accordance with Articles 5(1)(f) and 32 of the GDPR.

549 The Iris codes are processed by the Worldcoin Foundation in a central database. If a third party, such as a public authority or a malicious attacker, obtains access to this database, that third party has

access to all collected iris codes. The aim of the Worldcoin project is to provide an identification for everyone in the world. Such a large central database of such sensitive biometric data under the control of a single private organisation entails risks of magnitude that cannot yet be estimated today.

550 In addition, the Iris codes are not processed with the appropriate security, in plain text, so that, in addition to the risk arising from central storage, there is the risk resulting from the lack of security measures at data level (for this point, see II. 2.).

551 The special sensitivity of the iris code is also recognised by the Worldcoin Foundation.

552 The consent text of the Biometric Data Consent Form states that the Iris code is regarded as biometric data and is treated with particular caution and care.

553 At the same time, the data processing operations carried out in the context of the World ID project are (artificially) split into two blocks, 'Creation of image data, calculation of the iris code and active comparison' and 'Iris code storage and passive comparison'.

554 As explained above under aa., the declaration of consent made by the data subjects upon registration only covers the first block. Temporarily, this block ends in the moment the registration is completed, i.e. when, after actively having compared the just created iris code of the person to the iris codes of all registered users in the database, the Orb informs the user whether the registration was successful or not.

555 The second block, on the other hand, is not covered by the declaration of consent. However, it is the larger block in time and the block in which the more intrusive and high-risk processing of (permanent) storage of the iris code takes place.

556 This approach is not in line with the principles of transparency and fairness (variants 2 and 3 of Article 5(1)(a) of the GDPR).

557 By obtaining consent a user is led to believe that the processing can only take place if he or she gives his or her consent and as long as he or she does not withdraw it pursuant to Article 7(3) of the GDPR (see Article 17(1)(b) of the GDPR). However, in the details of the consent text, the processing is artificially split into the two blocks just mentioned and no consent from the user is sought for the permanent and more intrusive form of processing.

558 The user's right to withdraw consent can only be exercised during the time between ticking the consent box in the app and registering with an Orb operator. This period may range only from a few minutes to a few days.

559 After registration and for the permanent and risky processing of the storage and comparison of the iris-code in the moment a new user is trying to register somewhere, the user is not entitled to this right.

560 Such an approach is not in line with the principles of transparency and fairness set out in Article 5(1)(a), variants 2 and 3 of the GDPR, because it is contradictory and suggests wrong circumstances to data subjects. Even if such conduct could be made compatible with those principles by making it clearer, it does not do so in the present form. Such an essential aspect would have to be presented more clearly and intelligible to data subjects (see the first sentence of Article 12(1) and Article 13(1)(c) of the GDPR).

561 The infringement of the second variant of Article 5(1)(a) of the GDPR (principle of fairness) becomes even more apparent by taking into account the fact that the data subjects are rewarded with Worldcoins for registration with the World ID infrastructure.

562 The overall behaviour of the Worldcoin Foundation, namely the reward for registration, the permanent storage of the iris codes without the consent of data subjects, the lack of the possibility of withdrawal as regards the storage and the (previously) inability of data subjects to request erasure of their iris codes gives the impression that the Worldcoin Foundation wishes to buy the Iris codes of the data subjects. By paying out the cryptocurrency, data subjects should be encouraged to visit an Orb location and once the Iris code is stored, the data subject should factually be without rights in relation to his or her iris code.

563 This conduct is in contradiction to the principle that personal data do not constitute a commodity (Recital 24 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services).

564 In addition, taking into account the need to protect biometric data, the confusing and non-transparent nature of the processing, which is contrary to good faith within the meaning of the second variant of Article 5(1)(a) GDPR, must also be assessed with regard to the effectiveness of consent given by the data subjects for the purpose of "active comparison". The fact that data subjects are led to believe that they have control over the processing of their particularly sensitive personal data cannot be disregarded when assessing the requirements of Article 4(11) GDPR, in particular with regard to the criteria of “informed” and “freely given”. However, a final assessment is reserved for separate investigations into a violation of Article 9(1), 6(1) GDPR concerning the processing of iris codes for the purpose of "active comparison", in particular in the context of the concurrent individual complaints pending.

565 Finally, it should be pointed out that, if the processing of the iris codes for the purpose of passive comparison is considered lawful under point (f) of the first subparagraph of Article 6(1) of the GDPR, it would legitimise the processing of the iris codes by the Worldcoin Foundation for an indefinite time period.

566 As mentioned above, the Worldcoin Foundation justifies its interest in processing the iris codes for the purpose of passive comparison with the need to prevent multi-registrations by the same individual and the accompanied payments of the cryptocurrency Worldcoin to such individual.

567 The processing of the iris codes would thus be linked to the lifespan of the Worldcoin Foundation or the World ID project run by it. As long as the Worldcoin Foundation, the project and the database are existing, the Worldcoin Foundation has an interest in preventing multiple registrations.

568 That this assumption is also in line with the view of the Worldcoin Foundation is apparent, inter alia, from the (previously) impossibility for data subjects to request the erasure of their iris codes and from paragraphs 5 and 22 of the Worldcoin Foundation's statement of 14 May 2024. In paragraph 5, the Worldcoin Foundation expressly states: "The aforementioned erasure was carried out on a purely voluntary basis, without any corresponding legal obligation to do so".

569 If the Worldcoin Foundation's interest in preventing multiple registrations of users were given greater weight than the interests and fundamental rights of the data subjects (Articles 7 and 8 of the Charter of Fundamental Rights of the European Union), the Worldcoin Foundation would be able to process the Iris codes indefinitely.

570 Even if the Worldcoin Foundation were to introduce an option for data subjects to erase their iris codes, this would not alter that finding. In that regard, it would merely be a voluntary option which could be withdrawn at any time by the Worldcoin Foundation. There would be no legal obligation to erase data because the data processing would be considered lawful (see variant 1 of Article 17(1)(c) and Article 17(1)(d) of the GDPR).

571 This would lead to the complete disempowerment of data subjects in relation to their personal data and thus infringe the essence of the right to informational self-determination (Articles 1 and 2(1) of the Basic Law of the Federal Republic of Germany) and the right to privacy and data protection (Articles 7 and 8 of the Charter of Fundamental Rights of the European Union) (see CJEU judgment of 6 October 2015 in Case C-362/14 (Schrems), paragraph 95).

572 Overall, taking into account all the circumstances of the case and the need for a strict interpretation of the situations referred to in points (b) to (f) of the first subparagraph of Article 6(1) GDPR (CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), paragraph 93), point (f) of the first subparagraph of Article 6(1) GDPR does not apply to the processing of the iris codes for the purpose of passive comparison by the Worldcoin Foundation.

573 The Worldcoin Foundation's arguments in its statement of 14 May 2024 (para. 19 et seqq.) that the Worldcoin project is a voluntary offer and that only longer-term storage - independent of the will of the users - makes sense does not affect the above conclusion.

574 These two arguments are in themselves contradictory.

575 Naturally, a person must first voluntarily visit an orb operator so that the Worldcoin Foundation can even gain possession of the person's iris code. The data subject's consent is also obtained for the collection of the iris code and the active comparison with the other iris codes already stored. However, as already mentioned, the long-term and intrusive processing for the purpose of passive comparison takes place without the consent of the data subject and thus independently of his or her will. The voluntary nature of the Worldcoin project therefore ends for a user upon successful registration. From this point onwards, the user loses control over his or her iris code, a particularly sensitive personal datum which makes him or her permanently identifiable, and is - according to Worldcoin's concept - a permanent part of the Worldcoin project and the biometric database operated by the Worldcoin Foundation.

576 This disempowerment, however, as already explained, is not overriden by the (private commercial) interests pursued by the Worldcoin Foundation and the third parties participating in its system. Just because longer-term storage independent of the will of the data subjects may be useful or necessary for the design of the project envisaged by the Worldcoin Foundation, this alone cannot justify processing that interferes so deeply with the interests and fundamental rights of the data subjects, as the processing of the iris codes for the purpose of passive comparison, independently of the will of the data subjects.

577 In its statement of 26 June 2024, the Worldcoin Foundation reiterated that the Worldcoin project was a voluntary offer for users and that users in no way lose power over their data after registration. In addition, the Worldcoin Foundation argued that the mere comparison of data in the context of a database is by no means associated with high risks for the concerned user, which cancel their freedom of self-determination (para. 3 of the statement). In addition, the fundamental model underlying the Worldcoin project is misunderstood. The Worldcoin Foundation is by no means pursuing private commercial purposes; in particular, the Worldcoin Foundation does not intend to use iris codes for commercial purposes (para. 4 of the statement).

578 Regarding the argument that the Worldcoin project is a voluntary offer for users, reference can be made to the above considerations at para. 575. According to the current concept of the Worldcoin project, the voluntary nature of participation ends with registration. There is no argument that contradicts this statement in the statements of the Worldcoin Foundation, in particular in the statement of 26 June 2024, nor elsewhere.

579 Rather, it is clear from the statements of the Worldcoin Foundation, in particular para. 19 et seqq. of the statement of 14 May 2024 (see already para. 577 above), that the processing of iris codes is and is intended to be carried out independently of the will of the users, because this is the only way to achieve the purpose of the World ID system. In the statement of 26 June 2024, the only argument put forward in favour of voluntariness is that the iris codes are not personal data and that there is therefore no "loss of power" that falls within the competence of the data protection authorities.

However, as already explained in detail, iris codes are indeed personal data (see above II. 1. a. aa. (1)). Consequently, the Worldcoin Foundation did not submit anything that contradicts the statement made in para. 575.

580 The processing of iris codes is also associated with high risks for the data subjects, which has already been described in detail at para. 536 et seqq. Insofar as the Worldcoin Foundation argues that the comparison of iris codes does not entail high risks, this is to be rejected.

Firstly, the incorrectness of the data comparison can have serious negative consequences for the respective data subject. Especially if one were to assume that the World ID infrastructure were to become established as an authentication method and providers were only to allow access to their services with proof of a valid World ID, this could mean that in the event of an incorrect rejection of an actually unregistered user as supposedly already registered, the user would no longer have access to the services. In today's interconnected world, this would represent a (possibly) not insignificant social and, in individual cases, economic disadvantage (see first sentence of recital 75 GDPR and first sentence of recital 85 GDPR). It must be taken into account that biometric authentication methods are always probabilistic procedures that always have a certain error rate ("false positive rate" ("FPR") and "false negative rate" ("FNR")).

Secondly, the high risks do not primarily result from the data comparison, but above all from the (permanent) storage of the iris codes. In this respect, reference can be made to the explanations at para. 536 et seqq.

581 As far as the pursuit of non-commercial purposes or interests by the Worldcoin Foundation is concerned, this circumstance has no (decisive) impact on the legal assessment.

582 Even if the Worldcoin Foundation (also) operates the World ID infrastructure for idealistic reasons (without the intention of making a profit and only with the intention of covering costs), e.g. to generally contribute to an increase in security in the internet (by protecting the integrity of online spaces) and to generally increase the privacy of internet users (cf. para. 22 of the Worldcoin Foundation's statement of 14 May 2024) or to create the world's largest identity and financial network in order to "[...] provide universal access to the global economy - regardless of geographical borders or social backgrounds in order to empower all of humanity" (cf. https://worldcoin.org/community-grants), this cannot justify the ongoing intrusion associated with the permanent storage of iris codes independent of the will of the data subjects.

583 First, it should be noted that the interests mentioned are interests of the general public or society as such (public interests).

584 However, the pursuit of such interests cannot by itself justify data processing in accordance with point (f) of the first subparagraph of Article 6(1) GDPR (with the possible exception of further processing if Articles 6(4) and 23(1) of the GDPR apply at the same time). It is not a suitable interest

within the meaning of point (f) of the first subparagraph of Article 6(1) GDPR that a private operator could rely on (even if the Worldcoin Foundation is a foundation, it is a private operator and the operation of the World ID infrastructure is a private (and not state/public) endeavour). Rather, the requirements of point (c) and (e) of the first subparagraph of Article 6(1) GDPR are decisive for the pursuit of such an interest (for all of that, see CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), para. 124).

585 However, if the interests of the general public pursued by the processing overlap with equally pursued specific interests of the controller or a (specific) third party, the interests of the general public may be considered in the balancing of interests to be carried out in accordance with point (f) of the first subparagraph of Article 6(1) GDPR.

586 Second, as regards the above-mentioned interests of "increasing the privacy of Internet users in general" and "creating universal access to the global economy for everyone", these interests not only overlap with the interests of the data subjects participating in the World ID system, but are fully congruent with them. Only persons who participate in the World ID system (and are therefore data subjects) can benefit from this objective of the Worldcoin project.

587 However, the interests of the data subject are no more suitable interests within the meaning of point (f) of the first subparagraph of Article 6(1) GDPR, on which the controller could rely, than the interests of the general public. This is clearly expressed in the wording of point (f) of the first subparagraph of Article 6(1) GDPR, which states that the processing must be "[...] necessary for the purposes of the legitimate interests pursued by the *controlle*r or by a *third party* [...] (italics are author's emphasis)". According to Art. 4 No. 10 GDPR, a third party is "a natural or legal person, public authority, agency or body *other than the data subject* [...] (italics are author's emphasis)".

588 This statement also fits into the regulatory framework of Article 6(1) GDPR.

589 A controller acting (only) in the interests of the data subject should of course not be allowed to process the data of the data subject independently of (or against) their will. Otherwise, a data controller could virtually become the custodian of the interests of the data subject and make decisions regarding their personal data over their head, without being able to demonstrate a (valid) reason for the data processing. This would be in obvious contradiction to the fundamental concept of protection of the GDPR established in Article 5(1) GDPR and Article 6(1) GDPR.

590 Third, the interest of "increasing security on the internet" overlaps on the one hand with the interest of the Worldcoin Foundation to prevent multiple registrations in order to prevent payment of the cryptocurrency (see also para. 533), and on the other hand, especially, with the interests of the (specific) third parties (service/service providers) participating in the World ID system (para. 530-532) and - depending on the specific service offered - possibly with the interests of the users of the service offered by the third party.

591 However, as far as the Worldcoin Foundation's interest in preventing multiple registrations is concerned, it should be noted that the permanent processing of iris codes for the purpose of passive comparison independent of the data subject's will, is not necessary to achieve this interest within the meaning of point (f) of the first subparagraph of Article 6(1) GDPR.

592 The specific circumstances of the data processing must be considered not only in the balancing of interests to be carried out under point (f) of the first subparagraph of Article 6(1) GDPR, but also when examining the necessity criterion (CJEU judgment of 11 December 2019 in Case C-708/18 (Asociaţia de Proprietari bloc M5A-ScaraA), para. 47 et seqq.). The necessity test is closely related to the principles of data minimisation, accuracy and storage limitation pursuant to Article 5(1)(c) - (e) GDPR (CJEU judgement of 24 September 2019 in Case C-136/17 (GC u.a.), para. 74; cf. also CJEU judgement of 20 October 2022 in Case C-77/21 (GC u.a.), para. 55 et seqq. and CJEU judgement of 4 July 2023 in Case C-252/21 (Meta Platforms u.a.), para. 109). When assessing the necessity, it is decisive whether the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), para. 108; CJEU judgment of 11 December 2019 in Case C-708/18 (Asociaţia de Proprietari bloc M5A-ScaraA), para. 47).

593 The prevention of multiple registrations serves, in addition to the above-described ideal interests pursued with the World-ID infrastructure and the interests of the participating third parties, on the part of the Worldcoin Foundation, primarily the Worldcoin Foundation’s concrete financial interest in preventing multiple payments of the cryptocurrency Worldcoin to the same person due to successfully registering more than once.

594 However, this interest can also be achieved just as effectively by a less restrictive, equally effective means than the permanent storage of the iris codes. Permanent storage of the iris codes is not necessary to prevent multiple registrations. In this respect, temporary storage would also be sufficient. In any case, given the current value of the cryptocurrency of around USD 2, it cannot be assumed that multiple registrations with the Worldcoin project will be regarded by people as a suitable source of income as long as an immediate further registration is not possible. [redacted]

595 [redacted]

[redacted] The financial interest of the Worldcoin Foundation in preventing multiple registrations is therefore only of low weight in the overall assessment of the circumstances of the individual case and the balancing of the interests.

596 With regard to the interests of the third parties participating in the World ID system (service providers) and, where applicable, the interests of their users, the following should be noted:

597 The interests of the third parties participating in the World ID system consist on the one hand of the interest in the technical protection of their IT systems (cf. forth sentence of recital 49 GDPR) and on the other hand, depending on the service offered, possibly also of the interest in protecting the integrity of their online spaces.

598 The interest in protecting the IT system can be divided into preventive and repressive protection interests.

599 Preventive protection is intended to prevent (fully) automated access to the service or (fully) automated use of the service. Access or use is made dependent on the presentation of a (valid) World ID. Examples include the prevention of DDOS attacks, of successful registration of bots or of mass (spam) messages from bots. To this end, so-called captchas, i.e. puzzles that are supposed to be easy for humans but difficult for machines to solve, are usually used to date.

600 In addition to the question of whether possible solutions that only process personal data selectively at the moment of access to the service, such as captchas or AI-based countermeasures, are an equally effective but less restrictive means, it should be noted [redacted] As long as a data subject chooses to be or remain registered, it is not possible for them to register again, as their iris code is (legitimately) processed for the purposes of comparison and determining whether they are already registered. If a data subject decides that they no longer wish to participate in the World ID system, they will not have a World ID to "identify" themselves to the provider (unless the provider provides other mechanisms, they will not have access to the service). If the person would to be register again, they receive a new World ID; however, as already explained, the person could (normally) not receive multiple World IDs. The preventive security interest of the third party is therefore also achieved when giving data subjects sovereignty over their iris codes.

601 Likewise, the permanent storage of iris codes, independent of the will of the data subjects, is not strictly necessary to achieve the repressive protection interests of the third parties involved in the World ID system.

[redacted]

602 Repressive protective measures are primarily the blocking of access to the service (blocking of an account) from which malicious behaviour originates or originated.

603 In the present case, access would be blocked by blocking the respective nullifier (as a product of the zero knowledge proof) that applies to the respective service (cf. white paper, PoP, footnote 5, available at https://whitepaper.worldcoin.org/#footnotes), or by linking a pseudonym with the user's public key stored in the blockchain (see para. 161 above).

604 However, the effective enforcement of such measures is also possible without the indiscriminate, permanent storage of the iris codes independent of the will of the data subjects. The repressive protective interest in longer-term (or possibly permanent) processing of an iris code only materialises when a protective measure has been taken against a data subject and the data subject requests the deletion of their iris code. If the iris code were then deleted, the data subject could circumvent the blocking of their access because they could re-register with the World ID infrastructure and receive a new World ID (which is of course different from the old "blocked" World ID). The data subject could use this new World ID to access the service again, as the service would consider the new World ID to be a different person (the service does not see the iris code itself) (see already para. 161 for this).

605 In this respect, it would also be sufficient if the connected services were to be "asked" by means of a signal whether the respective nullifier or the pseudonym associated with the public key is blocked for logging into the service before the iris code and the associated world ID are deleted. Only with a positive response would the permanent processing of the associated iris code, independent of the data subject's will, be necessary for the protection of repressive security interests. This is not the case beforehand; instead, every user is placed under general suspicion of being blocked (and having done something to interfere with the security of a service), without the actual existence of such a block.

606 It is also not necessary to process iris codes permanently and independently of the data subject's will for the purpose of protecting the integrity of the online spaces of third parties (service providers) connected to the World ID infrastructure.

607 Especially services that enable social exchange between people, i.e. primarily social media services such as social networks and internet forums, but also other services that integrate social media elements such as comment functions, may have an interest in protecting the integrity of their online spaces. This regularly involves the enforcement of their terms of use, which determine what content a post or comment may contain. Users who violate this are sanctioned accordingly, in the worst case in the form of (temporary or, in exceptional cases, permanent) blocking of their access to the service. Effective enforcement of the terms of use not only serves the (economic) interests of the service

provider, but also the interests of other users in orderly interaction with one another in accordance with the terms of use.

608 However, also regarding these interests, it is not necessary to process the iris codes permanently and independently of the will of the data subjects. As with regard to the repressive security interests, a "feedback mechanism" can be considered as a less restrictive means according to which the connected services are "asked" whether there is a block on their side in the event of a request for erasure of the iris code.

609 In addition to the lack of necessity for the permanent processing of the iris codes, the interests and fundamental rights of the data subject also override the interests of the Worldcoin Foundation and any third parties (service providers and possibly their users) in the processing, even if the pursuit of idealistic interests is included in the balancing of the interests on the part of the Worldcoin Foundation.

610 As already described in detail above, this result follows from the non-transparent and contrary to good faith design of the processing (see above para. 553 - 563), the insecurity of the data processing (para. 548 - 550) as well as the particular sensitivity of the iris codes (para. 536 - 547) and the complete loss of power of the data subjects over their iris codes associated with the data processing (para. 565 - 571).

611 [redacted] the ideal interests pursued with the Worldcoin project, which, however, largely coincide with the interests of the data subjects and the third parties (service providers) participating in the World-ID infrastructure, as well as the security interest of the participating third parties and, if applicable, their interest and those of their users in protecting the integrity of the online spaces.

612 In addition to the reasons already discussed, the fact that the data subjects could not or did not have to expect their iris codes are to be processed for the purpose of enforcing (account) blocks is another factor leading to the interests and fundamental rights of the data subjects overriding the interests of the Worldcoin Foundation and the third parties (and, if applicable, their users) (sentence 3 and 4 of recital 47 GDPR). The reasonable expectations of the data subject(s) are an essential factor in the balancing of the interests under point (f) of the first subparagraph of Article 6(1) GDPR and are decisively influencing the outcome of the balancing (cf. CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), para. 112, 116 et seq., 123). An average user of the World ID system will assume that their personal data will be processed in order to provide the functions that are useful to him or her, such as the option to apply for funding (https://worldcoin.org/community-grants) or to use the World ID as an authentication factor. Even if the financial interest of the Worldcoin Foundation in preventing multiple registrations may be foreseeable to him or her, this is

not the case with regard to the processing for the purpose of enforcing (account) blocks in the interest of third parties connected to the system and, if applicable, their (other) users. An average data subject can and will assume that third parties participate in the World ID infrastructure in order to comply with legal requirements regarding IT security (NIS2 Directive, Art. 5 para. 1 letter f, 32 GDPR, etc.) or because they want to offer their users added value with the connection to the World ID system. However, they do not have to expect that their personal data (World ID and iris code) will be processed to their detriment for the purpose of enforcing (account) blocks.

613 Finally, it must also be taken into account that the relationship between the data subject and the Worldcoin Foundation as well as the relationship between the data subject and the third parties is (only) of private nature, the focus of which is the fulfilment and enforcement of private civil law obligations. However, if, according to the case law of the CJEU, the permanent storage of biometric data independent of the data subject's will is not limitlessly permissible for the purpose of preventing, investigating, detecting or prosecuting criminal offences (CJEU judgement of 30 January 2024 in Case C-118/22 (Direktor na Glavna direktsia "Natsionalna politsia" pri MVR - Sofia) concerning the "sister directive" of the GDPR (EU) 2016/680), then it is out of question that a different assessment applies in the case of the pursuit of private interests, such as here.

(3) Interim result

614 Since the processing of the iris codes for the purpose of passive comparison is not lawful under any of the points (a) to (f) of the first subparagraph of Article 6(1) GDPR, in particular neither by the consent of the data subjects in accordance with point (a) of the first subparagraph of Article 6(1) GDPR nor by way of an overriding legitimate interest of the Worldcoin Foundation or a third party in accordance with point (f) of the first subparagraph of Article 6(1) GDPR, the processing of the iris codes for the purposes of passive matching is unlawful in accordance with Article 5(1)(a) variant 1 and the first subparagraph of Article 6(1) of the GDPR.

bb. Unlawfulness of the processing of the SMPC-Shares for the purpose of passive comparison under the first subparagraph of Article 6(1) GDPR

615 In the same way, the processing of the SMPC-Shares for the purpose of passive comparison is unlawful under the first subparagraph of Article 6(1) GDPR.

616 As already explained in the context of Art. 9 GDPR under II. 3. a. aa. (3), the data subjects have not given their consent to the processing of the SMPC shares for the purpose of passive comparison, which includes the processing steps of storing the SMPC shares and matching them in the event of a new user registration. Article 6(1)(1)(a) GDPR is therefore not fulfilled.

617 The processing of SMPC shares for the purpose of passive comparison is also not justified under Article 6(1)(f) GDPR. In this respect, please refer to the considerations regarding the iris codes above under II. 3. b. aa. (2).

618 Although splitting the iris code into shares may provide a certain security advantage, the shares are still biometric data in accordance with Art. 4(14) GDPR, even if they are potentially pseudonymised (see II. 1. a. aa. (2)). The effects and risks associated with the processing of biometric data and already identified with regard to the iris codes therefore also exist in the context of the processing of the SMPC shares.

619 As also described under II. 1. a. aa. (2), the shares are processed - albeit formally by two different processors (Worldcoin Europe GmbH and Tools for Humanity GmbH) - using the same cloud infrastructure or the same cloud service provider. Due to this centralisation, even if one wants to ascribe a security benefit to the introduction of the SMPC system, this benefited is very limited. The centralisation of the SMPC system mentioned above under II. 3. b. aa. (2) and the associated risks are therefore still present after the introduction of the SMPC system.

620 Finally, even after the introduction of the SMPC system, the disempowerment of data subjects with regard to their particularly sensitive personal data remains. According to the Worldcoin Foundation, the SMPC shares, which can also be reassembled into the Iris code by the Worldcoin Foundation without any significant effort, are to be processed permanently and without any possibility of intervention by the data subject.

c. Obligation to erase the iris codes and SMPC-Shares without undue delay pursuant to Article 17(1)(d) of the GDPR

621 Under Article 17(1)(d) of the GDPR, personal data which is processed unlawfully must be erased without undue delay. According to the wording of Article 17(1) of the GDPR, that obligation does not arise only with a data subject's request for erasure, but exists independently of such a request. The controller therefore has a obligation to erase without undue delay in the case of unlawful processing of personal data, independent of a request made by the data subject (CJEU judgment of 14 March 2024 in Case C-46/23 (Újpesti Polgármesteri Hivatal), paragraph 37 et seqq.).

622 An exception under Article 17(3) of the GDPR is not applicable.

623 There is no obligation, based on European or Member State law, to further process the iris codes or the SMPC-Shares (Article 17(1)(b) of the GDPR).

624 Furthermore, the processing of the iris codes and SMPC-Shares is not necessary for the 'establishment, exercise or defence of legal claims' (Article 17(3)(e) of the GDPR). This exception must be interpreted narrowly. It serves to ensure the functioning of the judiciary and the right to be heard.

For it to apply a close link to (not necessarily judicial) procedure is necessary. The further processing must therefore take place within a specific procedural framework (see EDPB Guidelines 2/2018 on exceptions under Article 49 of Regulation 2016/679, page 11 et seq.). This illustrated by the third sentence of recital 52 of the GDPR relating to the parallel-provision of Article 9(2)(f) of the GDPR, which reads as follows:

625 'A derogation should also allow the processing of such personal data [Note: sensitive data within the meaning of Article 9(1) of the GDPR] where necessary for the establishment, exercise or defence of legal claims, *whether in court proceedings or in an administrative or out-of-court procedure*.'

626 That finding is further supported by the wording of the Italian language version of Articles 9(2)(f), 17(3)(e) and 49(1)(e) of the GDPR. The German language version of the predecessor or model provision to Article 9(2)(f) of the GDPR, namely Article 8(2)(e) of the Data Protection Directive 95/46/EC, also clearly expresses the need for a specific connection with a procedure by the term 'in front of a court'.

627 Consequently, Article 17(3)(e) GDPR is in any event not applicable if there is only the (abstract) possibility of legal proceedings or formal procedures (cf. EDPB Guidelines 2/2018 on exceptions under Article 49 of Regulation 2016/679, page 11).

628 Thus, the Worldcoin Foundation violated its obligation to erase without undue delay in the case of unlawful processing of personal data. As a result, the erasure of the iris codes and SMPC-Shares had to be ordered (see IV. for more details).

d. Interim result

629 The processing of the iris codes and SMPC-Shares by the Worldcoin Foundation for the purpose of passive comparison, which includes the processing steps of storing the iris codes as well as the comparison with them in the event of a new registration of a user, is unlawful not only under Article 9(1) GDPR but also under the first subparagraph of Article 6(1) GDPR.

630 The legal consequence of the unlawful processing of the iris codes by the Worldcoin Foundation is the obligation of the Worldcoin Foundation to erase the iris codes and SMPC-Shares processed for the purpose of passive comparison without undue delay pursuant to Article 17(1)(d) of the GDPR.

4. Infringement of Article 17(1) of the GDPR

631 The Worldcoin Foundation also infringed Article 17(1) of the GDPR by not allowing data subjects to obtain the erasure of their iris codes, let alone request it.

632 Under Article 17(1) of the GDPR, the data subject has the right to obtain from the controller that personal data concerning him or her be erased without undue delay, provided that one of the grounds referred to in Article 17(1)(a) to (f) applies.

633 Under the first sentence of Article 12(2) of the GDPR, the controller must facilitate the exercise of the data subject's rights under Articles 15 to 22.

634 In the present case, the Worldcoin Foundation not only did not facilitate the exercise of the right to erasure, but did not even give data subjects the opportunity to request erasure of the iris codes and/or the files derived from them ('SMPC shares').

III

Competence

635 The BayLDA is the competent supervisory authority pursuant to Articles 51(1) and 56(1) of the GDPR in conjunction with the first sentence of Section 19(1) of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) and Section 40(1), first sentence, of the BDSG in conjunction with the first sentence of Article 18(1) of the Bavarian Data Protection Act (BayDSG).

636 The competence of the BayLDA as lead supervisory authority under Article 56(1) of the GDPR in conjunction with the first sentence of Section 19(1) of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) arises from the fact that the Worldcoin Europe GmbH, established in Munich, is the only EU-establishment of the Worldcoin Foundation **(1.)**that there is cross-border processing within the meaning of Article 4(23)(b) of the GDPR **(2.)** and, unlike in the case of the main establishment under Article 4(16) of the GDPR, it is not necessary for Worldcoin Europe GmbH to have decision-making powers with regard to the purpose and means of the processing **(3.).**

1. Worldcoin Europe GmbH as the only establishment of the Worldcoin Foundation in the EU

637 As mentioned under II. 1. b. bb., the Worldcoin Europe GmbH is an establishment of the Worldcoin Foundation.

638 According to the findings, the Worldcoin Europe GmbH is also the only establishment of the Worldcoin Foundation in the EU.

2. Cross-border processing pursuant to Article 4(23)(b) of the GDPR

639 The processing within the Worldcoin project amounts to cross-border processing within the meaning of Article 4(23)(b) of the GDPR.

640 According to Article 4(23)(b) of the GDPR cross-border processing means processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

641 In the present case, the data processing – as was already discussed under II. 1. b. bb. on the territorial scope of the GDPR – take place in the context of the activities of the Worldcoin Europe GmbH's, i.e. in the context of the only establishment of the Worldcoin Foundation in the EU.

642 The data processing also "substantially affects or is likely to substantially affect data subjects in more than one Member State".

643 The services provided in connection with the Worldcoin project are offered not only to German data subjects but also to data subjects in other Member States, such as Spain, Portugal, Austria and Poland. Insofar as the activities of the Worldcoin Foundation have stopped in the two member states mentioned first, this, according to the view of the Worldcoin Foundation, only constitutes a temporary suspension.

644 As regards the concept of 'significant affect', paragraph 12 of the 'Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority' contains a non-exhaustive list of factors to be taken into account when assessing whether this criterion is fulfilled. Without presenting this list in detail here, the data processing operations carried out in the context of the Worldcoin project undoubtedly significantly affect data subjects in at least one more Member State than Germany, or have the most likely potential to do so (see II. 3. a. bb.).

3. No need for decision-making power of Worldcoin Europe GmbH

645 Finally, it should also be noted that the Bavarian Data Protection Authority for the Private Sector does not understand the EDPB's "Opinion 04/2024 on the notion of main establishment of a controller in the Union under Article 4.16(a) GDPR" requiring for the one-stop-shop mechanism to apply in the case of a single EU-establishment that the single establishment has the power to take decisions on the purposes and means of processing and to have them implemented.

646 In our view, this cannot be inferred from the wording of the Opinion, which deals solely with the concept of 'main establishment' within the meaning of Article 4(16)(a) of the GDPR and presupposes the existence of several establishments (see, in particular, paragraph 37).

647 On the contrary, footnote 30 specifically suggests that the one-stop-shop (OSS) mechanism is applicable in the case of a single establishment even if the establishment has no decision-making power as to the purposes and means of the processing.

648 Paragraph 30 of the Opinion to which footnote 30 refers to reads:

„Accordingly, the Board takes the view that when there is no evidence that decision-making power on the purposes and means for a specific processing (as well as the power to have these decisions implemented) lies with the PoCA [Anmerkung Verfasser: "place of central administration"] in the Union or with "another establishment of the controller in the Union", i.e. if it lies outside the Union, there is no main establishment under Article 4(16)(a) GDPR for that processing. Therefore, in that case, the one-stop-shop mechanism should not apply [30]."

649 Footnote 30 specifies the applicability of the OSS in cases where there is a single establishment in the EU and the decision-making power lies outside the EU:

„This is without prejudice to other cases where the one-stop-shop mechanism may apply, such as a single establishment of a controller or processor."

650 The statement made by the EDPB in footnote 30 is in line with the EDPB's previous publications.

651 The annex to the "Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority" (page 13 of the English version) also shows that a verification of whether the decision-making power lies in the EU is unnecessary in the case of a single establishment.

652 As follows from an overall analysis of Opinion 04/2024 (para. 30 and footnote 30), the Guidelines 8/2022 (cf. page 13, in particular paras. 48, 49) and the 'Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR' (footnotes 6 and 7 and para. 16), the OSS is only inapplicable in the following five cases:

1. The requirements of Article 55(2) GDPR are fulfilled;

2. There is more than one establishment in the EU/EEA but none has the decision-making power (Opinion 04/2024);

3. The controller has no establishment in the EU/EEA (Guidelines 8/2022, para. 49);

4. There is no cross-border processing pursuant to Article 4(23)(a) or (b) GDPR (Guidelines 8/2022, para. 49 and Internal Document 1/2019, para. 10);

5. Though there is cross-border processing as defined in Article 4(23) GDPR, one of the two criteria in Article 56(2) GDPR applies and the lead supervisory authority does not decide to deal with the case itself pursuant to Article 56(3) to (5) GDPR (Internal Document 1/2019).

653 In addition, the OSS mechanism aims to encourage controllers (and processors) to establish themselves in the EU in order to benefit from the OSS (cf. Council document 17831/13, fn. 416, available at https://data.consilium.europa.eu/doc/document/ST-17831-2013-INIT/en/pdf).

654 Finally, the OSS also serves to avoid duplication of competences and the general disadvantages associated with it, such as the waste of resources, the risk of conflicting decisions and the emergence of disputes between supervisory authorities (cf. Council document 17831/13, fn). 417, available at https://data.consilium.europa.eu/doc/document/ST-17831-2013-INIT/en/pdf).

655 The place of a single establishment is a criterion which allows a supervisory authority to be given a leading role on the basis of an objective circumstance, because it distinguishes that supervisory authority from the other supervisory authorities. In the case of several establishments, this is not possible solely on the basis of the place of establishment, so in this case (and only in this case) it is necessary, in addition, to consider where the decisions on the purposes and means of processing are taken.

IV.

Orders and Deadlines for Compliance

656 The orders made under points I. to XVII. of this decision are lawful and necessary in the exercise of the discretion granted to the BayLDA in determining remedial and enforcement measures (1. and 2.). Circumstances which would confirm the Worldcoin Foundation's argument that the envisaged remedial deadlines are too short, disproportionate and therefore not within the limits of the BayLDA's discretion are not identifiable (3.).

1. Legal basis and exercise of discretion with regard to points I., II., IV., VI., VIII. and points X., XII., XIV., XVI. of the decision

657 The legal basis for the orders made in points I., II., IV., VI. VIII., X., XII., XIV. and XVI of the decision can be found in Article 58(2)(b), (d),(f) and (g) of the GDPR.

658 Article 58(2) of the GDPR contains a (non-exhaustive, cf. paragraph 6) list of corrective powers of a supervisory authority, but does not itself specify when and how the powers should be used.

659 The competent supervisory authority thus has a margin of discretion as to whether it exercises a corrective power and what power it exercises (very instructive with regard to the discretion of a supervisory authority under Article 58(2) GDPR, see the Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 (Land Hessen), paragraphs 40 et seqq.).

660 The exercise of that discretion must be guided by the role of the supervisory authority to monitor and enforce the application of the GDPR (Article 57(1)(a) GDPR) (Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 (Land Hessen), paragraph 40). Accordingly, if the supervisory authority finds that there has been an infringement of the GDPR in principle, it must identify the most appropriate corrective measure(s) in order to address the infringement (CJEU judgement of 7 December 20234 in the joined cases C-26/22 and C-64/22 (SCHUFA Holding), paragraph 57; Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 (Land Hessen), para. 40; see also CJEU judgment of 16 July 2020 in Case C-311/18 (Facebook Ireland and Schrems), paragraph 111). Only exceptionally, under certain circumstances, a supervisory authority is not obliged to intervene, namely if there is no longer a situation contrary to EU law, for example because the controller has remedied the situation by taking appropriate measures itself; in such a case, a remedy may no longer be necessary to ensure compliance with the Regulation (sentence 4 of recital 129 of the GDPR; Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 (Land Hessen), point 42 et seqq.).

661 All orders issued in the present case are appropriate, necessary and proportionate to ensure compliance with the GDPR (Recital 129 sentence 4 GDPR):

662 **Point I. of the decision – reprimand regarding the infringement of Article 32 of the GDPR –**

663 With regard to the infringement of Article 32 of the GDPR, the BayLDA takes the view that a reprimand constitutes the appropriate, necessary and proportionate measure to remedy that insufficiency.

664 The adoption of a remedy in relation to the infringement of Article 32 of the GDPR was necessary in the present case, since the Iris codes have been processed for a long period of time, from 24 July 2023 to 14 May 2024, in plain text by the Worldcoin Foundation in breach of Article 32 of the GDPR.

665 Issuing a reprimand under Article 58(2)(b) of the GDPR was also proportionate.

666 The warning is, of the corrective powers available to a supervisory authority, the least intrusive.

667 It was also not appropriate to take a more intrusive remedy in the present case, as the BayLDA and the Worldcoin Foundation are in continuous exchanges with each other and the BayLDA feels that the criticisms it put forward about the security of the processing are taken into account by the Worldcoin Foundation and Worldcoin is working on improving the security, as the introduction of the SMPC system in May 2024 shows. A reprimand is the appropriate and sufficient way to amplify this criticism.

668 Furthermore, insofar as it can be assumed that the SMPC system has been (functionally) implemented by the Worldcoin Foundation, this is an infringement that took place in the past, meaning that the adoption of a corrective measure pursuant to Article 58(2)(d) or (f) GDPR is not appropriate or necessary. At the same time, however, in view of the long duration of the infringement, it was necessary to issue a warning in order to emphasise the unlawfulness of storing the iris codes in plain text and to clearly distinguish this finding from other options for action.

669 In this respect, it should be noted that these considerations solely concern the distinction between the power to remedy an unlawful situation by issuing a remedy pursuant to Article 58(2)(b) GDPR and the other powers provided for in Article 58(2) GDPR to remedy an unlawful situation, in particular Articles 58(2)(d) and 58(2)(e) GDPR, with regard to the criteria set out in recital 129 sentence 4 GDPR. They do not constitute an assessment of whether the infringement under consideration should be addressed with a fine pursuant to Articles 58 (2)(i), 83 GDPR. Insofar it must be highlighted that the insecure processing of the iris codes of several million people for almost a year is not an infringement that can be regarded as minor from the outset, which would justify excluding the imposition of a fine as an effective, proportionate and dissuasive legal consequence in accordance with the standards of Article 83 (1) GDPR without further examination – which, of course, is reserved for the separate procedural regime of administrative offence proceedings.

670 **Points II. And X. of the decision – Order for the erasure of the iris codes and SMPC-Shares within one week –**

671 Ordering the erasure of the iris codes and the SMPC-Shares within one week is appropriate, necessary and proportionate.

672 Ordering the erasure of the iris codes is necessary insofar as it is assumed that the SMPC system has not been (functionally) implemented by the Worldcoin Foundation SMPC system - contrary to the statements of those responsible - and that iris codes are still being processed by the controller for the purpose of passive comparison today. Insofar as it can be assumed that the SMPC system is fully functional and only the SMPC shares are processed for the purpose of passive comparison instead of iris codes, it was also necessary to order the erasure of the SMPC shares.

673 Ordering the erasure of the iris codes and the SMPC-Shares was also proportionate.

674 The unlawful processing of Iris codes and the SMPC-Shares by the Worldcoin Foundation constitutes a serious interference with the fundamental rights of data subjects under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (cf. II. 3. b. aa. (2)).

675 Not to order the deletion of the iris codes and the files derived from them ('SMPC shares') would only lead to the perpetuation of that interference and would also entail serious risks (not only with regard to data protection) for the data subjects (cf. II. 2. and II. 3. b. aa. (2)).

676 In addition, as described under II. 3. c., the Worldcoin Foundation is obliged to erase the iris codes and SMPC-Shares without undue delay. This violation and the associated unlawful situation can only be remedied by an order to erase. Other remedies are not suitable to eliminate this situation. Consequently, the deletion of the iris codes and the files derived from them ('SMPC shares') was the only suitable remedy to be ordered.

677 As Advocate General Pikamäe pointed out in his Opinion, where the supervisory authority finds that there is an obligation to erase and the controller has not yet erased the data, the supervisory authority must order the erasure (Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 Land Hessen, paragraph 60).

678 The time limit of one week to erase is also reasonable. The technical implementation is not particularly difficult. It can be implemented without problem within the period of one week after the decision has become final.

679 **Points IV. and XII. of the decision – Orders for the processing of the iris codes and SMPC-Shares to be brought into compliance with Articles 5(1)(a) variant 1, 9(1) GDPR and with Articles 5(1)(a) variant 1, the first subparagraph of Article 6(1) GDPR within two months –**

680 The order to bring the processing of the iris codes and the derived files ('SMPC shares') into compliance with the Articles 5(1)(a) first variant, 9(1) and the first subparagraph of Article 6(1) GDPR within two months is appropriate, necessary and proportionate.

681 As the processing of the iris codes, insofar as it is assumed that the SMPC system has not been (functionally) implemented, and the processing of the SMPC-Shares in its current form is unlawful it was necessary to take remedial action to eliminate this unlawful situation and to prevent the continuation of this situation (with regard to new iris codes / SMPC-Shares collected in the future under the same circumstances and processed in the same way).

682 The order to bring the processing into compliance pursuant to Art. 58(2)(d) GDPR is of medium intensity in terms of intrusiveness. It is between the weaker reprimand under Art. 58(2)(b) as the mildest repressive remedy and the stronger (definitive) limitation of processing under Art. 58(2)(f) GDPR as the strictest remedy.

683 In view of the seriousness of the interference with the fundamental rights of the data subjects and the risks posed by the processing of the iris codes and the derived files ('SMPC shares'), a remedial action had to be taken that would ensure with sufficient certainty that the processing would comply with the GDPR in the future. In view of these important aspects, a reprimand did not provide sufficient certainty in the present case.

684 However, it was also not appropriate to issue a definitive limitation, or even a ban, on processing. The issuance of such an order was not appropriate in the present case, as it can be assumed that the Worldcoin Foundation will bring its processing into compliance with the Regulation within the two-month period.

685 The period of two months to bring the processing into compliance is necessary and reasonable. Taking into account the circumstances of the individual case, in particular with regard to the severity of the interference and the resulting risks, a short deadline for establishing legal compliance was to be chosen (see EDPB Binding Decision 3/2022 of 5 December 2022, para. 286); at the same time, nothing impossible can be demanded of the Worldcoin Foundation. A period of two months therefore appears reasonable in this individual case.

686 **Points VI. And XIV. of the decision – ordering the processing of the iris codes and SMPC-Shares to be brought into compliance with Article 17(1) of the GDPR within one month –**

687 It is appropriate, necessary and proportionate to order that the processing of the iris codes / SMPC-Shares be brought into compliance with Article 17(1) of the GDPR within one month.

688 The right to erasure pursuant to Art. 17 GDPR is a central pillar of the GDPR (see Art. 5 (1) (d) GDPR) and an expression of the data subjects' sovereignty over their data.

689 Due to the seriousness of the infringement, which affects the essence of the right to data protection (see II. 3. b. aa. (2); CJEU judgment of 6 October 2015 in case C-362/14 (Schrems), para. 95), the issuance of an order pursuant to Art. 58(2)(d) GDPR was evidently appropriate. The current situation is such a serious deviation from the legally compliant normal situation that a reprimand would not have been appropriate.

690 In this respect, the period of one month to comply with the order is also necessary and appropriate.

691 **Points VIII. And XVI. of the decision – Orders to cease processing of the iris codes and SMPC-Shares until the obligations under points IV. and VI. as well as points XII. and XIV. of the decision have been fulfilled, respectively, within one week –**

692 The order to cease processing of the iris codes and SMPC shares for the purpose of passive comparison until fulfilment of the obligations under sections IV. and VI. as well as sections XII. and XIV. of the decision is appropriate, necessary and proportionate.

693 The order to temporarily cease processing until the processing complies with Articles 5(1)(a)(1), 6(1)(1), 9(1) and 17 GDPR was necessary to prevent further unlawful processing of iris codes and SMPC shares.

694 Without this order, the Worldcoin Foundation would be free - without fear of state intervention - to continue its processing without complying with the GDPR.

695 Even if one assumes that the Worldcoin Foundation fulfils both its obligation to erase the iris codes and the SMPC shares within one week after the decision becomes final in accordance with points II. and X. of the decision and its obligation to bring the processing into compliance with the Regulation within one month and two months in accordance with points IV, VI, XII. and XIV. of the decision, if Worldcoin were to take full advantage of these deadlines, there would be a period of one month and three weeks within which the Wordlcoin Foundation could process the iris codes or SMPC shares of newly registered users in violation of EU law without having to fear state intervention.

696 Other means of preventing further processing with sufficient certainty were not available. Setting shorter deadlines for compliance with the Regulation was not an option, as these must be set at a level that allows the controller to make the necessary adjustments with sufficient certainty.

697 The only means by which further unlawful processing by the Worldcoin Foundation can be prevented with reasonable certainty, and which is provided precisely for this purpose, is the ordering of a temporary limitation of processing pursuant to Article 58(2)(f) GDPR.

698 Consequently, the order to temporarily cease processing was necessary.

699 The order was also proportionate in view of the seriousness of the interference with the interests and rights of the data subjects associated with the processing. Tolerating the continuation of the intrusive processing - even if only for a short period of time - and not preventing it with a sufficiently

secure means was not an appropriate option. Furthermore, the order does not impose any particular hardship on the Worldcoin Foundation, as the Worldcoin Foundation is in any case obliged to bring the processing into compliance with the GDPR within one and two months of the decision becoming definitive. In this respect, the maximum period during which the Worldcoin Foundation cannot pursue its processing activities is one month and three weeks if it complies with the orders and takes full advantage of the deadlines.

2. Legal basis and exercise of discretion in relation to points III., V., VII., IX. and points XI., XIII., XV., XVII of the decision – Orders for providing proof of adherence to the substantive orders –

700 The legal basis for the orders made in sections III., V., VII., IX., XI., XIII., XV. and XVII. of the decision can be found in Article 58(1)(a) of the GDPR in conjunction with the first half of the second sentence of Article 60(10) GDPR.

701 They are necessary in order to monitor compliance with the obligations laid down in points II, IV., VI., VIII., X., XII., XIV. and XVI. of the decision and are therefore essential for the performance of the BayLDA's tasks in accordance with Article 57(1)(a) of the GDPR.

702 The deadline of one week to fulfil the orders is sufficient and proportionate, especially since the end of the deadlines provided for in the substantive orders under points II., IV., VI., VIII., X., XII., XIV. and XVI. are not identical.

3. Adequacy of the deadlines contained in points I. to XVII.

703 In its statement of 26 June 2024, the Worldcoin Foundation argued that the deadlines contained in points II., IV., VIII., X., XII. and XVI. are too short (para. 21-23 of the statement), as the implementation of these orders would involve an enormous amount of personnel, organisational and financial effort. Implementation would only be possible if the company were to initiate corresponding implementation measures before the decision becomes final. However, this would unreasonably restrict its right to an effective defence.

704 Although the appropriateness of the deadlines has already been demonstrated in the previous paragraphs, the Worldcoin Foundation's arguments will explicitly be analysed in more depth in the following paragraphs.

705 Pursuant to the second sentence of Article 36(1) of the Bavarian Administrative Service and Enforcement Act ("Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz" – "BayVwZVG"), the threat of a coercive measure (in this case the threat of penalty payments pursuant to sections XVIII. to XXXIII. of the notice; see V. below) must be accompanied by a deadline for compliance with the order for which the coercive measure is threatened in case of noncompliance within which the obligor can reasonably be expected to comply with the order.

The determination of the length of the deadline is at the discretion of the authority (*Hanno-Dirk Lemke*, Verwaltungs-Vollstreckungsgesetz, Section 13 VwVG, para. 10). In particular, the urgency of fulfilment of the order, the nature of the obligation imposed, the severity of the risk and the means and options available to the obligor for fulfilment must be taken into account (*Deusch/Burr*, BeckOK VwVfG, Section 13 VwVG, para. 9; VGH Munich (20th Senate), decision of 22 October 2009 - 20 CS 09.2006, BeckRS 2009, 43925, para. 35). Limits of this discretion are the objective impossibility as well as the subjective unreasonableness of complying with the deadline (*Deusch/Burr*, BeckOK VwVfG, Section 13 VwVG, para. 9).

706 On the basis of these requirements, setting a deadline of one week in points II., VIII., X. and XVI. was within the discretion of the BayLDA.

707 That it is objectively impossible or subjectively unreasonable for the Worldcoin Foundation to erase the iris codes and the SMPC shares pursuant to sections II. and X. within one week from the date on which the decision becomes final is not apparent.

708 Insofar as the Worldcoin Foundation asserts an "[...] enormously high personnel, organisational and financial effort [...]", this is not evident with regard to conducting an erasure of the iris codes as well as the SMPC shares and was not further explained by the Worldcoin Foundation in its statement.

709 Generally, the Worldcoin Foundation is already obliged under Article 25(1) GDPR to enable and maintain effective erasure procedures in the design of its processing, i.e. procedures that can be implemented without more than insignificant delay, in order to be able to fulfil the requirements of storage limitation (Article 5(1)(e) GDPR) and obligations under Article 17 GDPR. If this has not yet been done with sufficient effectiveness, the effort of implementing such measures cannot relieve the controller. Circumstances that would demonstrate a qualified impediment to the fulfilment of the erasure obligation despite the implementation of corresponding process control options have neither been presented nor are apparent by themselves.

710 Moreover, all iris codes and SMPC shares are stored centrally on AWS servers. It is therefore also not necessary to first carry out inquiries in order to determine the storage location of data covered by the erasure obligation.

711 The deadline of one week for erasing the iris codes and SMPC shares is therefore sufficient, adequate and reasonable, even if the period between the notification of the decision to the Worldcoin

Foundation and the finality of the decision is not being considered in the assessment of the adequacy of the deadline.

712 However, it should be noted that the Worldcoin Foundation's argument cannot be accepted in this respect and that the period between the notification of the decision and the finality of the decision can certainly be taken into account when examining the appropriateness or reasonableness of a deadline. With regard to the possibility and reasonableness of the fulfilment of the orders, the period between the announcement of the threat of coercive measures and the end of the deadline must be taken into account (*Hanno-Dirk Lemke*, Verwaltungs-Vollstreckungsgesetz, § 13 VwVG, para. 10).

Of course, the obligor cannot be expected to fulfil the obligation itself during this period. Nor can the obligor be expected to make irreversible decisions during this period. However – especially with regard to Art. 25 GDPR – it will be possible to require the data controller to mentally prepare for the fulfilment of the obligation and to take certain preparatory measures to implement the obligation in the event or at the time at which the obligation becomes final.

713 Since compliance with the one-week deadline for fulfilling the erasure orders is not objectively impossible or subjectively unreasonable for the Worldcoin Foundation, it should also be noted that the deadline is also otherwise appropriate and proportionate. As already noted under 1. above, the unlawful processing of iris codes and SMPC shares for the purpose of passive comparison constitutes an intensive interference with the data subjects' right to informational self-determination, privacy and data protection. The remediation of this unlawful situation by erasing the iris codes and SMPC shares collected to date is a matter of great urgency.

714 The same applies to the deadline of one week to cease processing the iris codes and SMPC shares until fulfilment of the obligations to bring the processing into compliance with the GDPR in accordance with sections VIII. and XVI. of the decision. There is also a high degree of urgency in this respect.

715 If, after the erasure of the previously collected iris codes and SMPC shares, the Worldcoin Foundation could again collect (or generate) iris codes and SMPC shares and continue its processing until its processing complies with the GDPR, the unlawful situation that has just been remedied would reoccur. Preventing this is of enormous importance and urgency.

716 In the case of the obligations to cease and desist, the deadline requirement of the second sentence of Article 36(1) BayVwZVG does not apply directly; rather, the obligation can also be imposed on the obligor "with immediate effect" if there is a predominant public interest and a certain time to react to the obligation is allowed before taking coercive action (VGH Munich (4th Senate), decision of 15 June 2000 - 4 B 98.775, BeckRS 2000, 22225). In the present case, however, the Worldcoin Foundation was even explicitly granted a deadline of one week from the date on which the decision becomes final to cease processing.

717 There is no apparent reason for any subjective unreasonableness of the fulfilment of the obligation to cease and desist within one week of the decision becoming final. The cessation of the processing of iris codes and SMPC-share for the purpose of passive comparison can be implemented in a variety of ways; in any case, it would be sufficient to stop any data flow to the servers. This can e.h. be implemented by "Blocking data input (at logical level)" on the server side without significant expenditure of resources and time.

718 Finally, to clarify at this point, the obligations to cease and desist under Sections VIII. and XVI. cover the period between one week after the finality of the decision and the end of the deadline for the respective obligation to bring the processing into compliance with the GDPR. As soon as the deadlines for the latter orders have expired, any further unlawful processing will only result in a penalty payment for breach of these obligations. Inherent in the order to bring the processing into compliance within a deadline is the effect that, if the order is not complied with within the deadline, the controller may not continue the processing as long as the processing is not in compliance with the GDPR. In addition to the positive component of having to take action, the order to bring into compliance also has a negative component of not being allowed to process after the deadline has expired as long as there is no legal conformity. Once the deadline has expired, the order to comply with the GDPR, which has a positive and negative component, replaces the cease and desist order, which only has a negative component.

719 In its statement, the Worldcoin Foundation also criticises the length of the deadlines for the orders to bring the data processing into compliance with Article 9(1) and with the first subparagraph of Article 6(1) GDPR (points IV. and XII. of the decision) as being too short.

720 The Worldcoin Foundation states in this regard: "Here, too, the implementation period of *one month* is not nearly long enough to make the necessary process changes [italic are author's emphasis]."

721 The Worldcoin Foundation mistakes that the deadlines for obtaining (express) consent under sections IV. and XII. of the decision are two months and not one month.

722 Two months, i.e. twice the period assumed by the Worldcoin Foundation in its statement, should therefore also be sufficient from the perspective of the Worldcoin Foundation to make the necessary changes to its processes.

723 In order to fulfil the obligations under points IV. and XII. of the decision, the Worldcoin Foundation would have to design the overall process of obtaining consent of the data subjects in a legally compliant manner, i.e. in particular in accordance with the legal requirements of Articles 4(11), 5(1)(a), 6(1)(a), 9(2)(a) GDPR. This is an obligation that at most requires a certain amount of human and financial resources, but which is far from resulting in "[...] an enormously high [...] effort". In terms of personnel it is primarily the legal staff of the controller who would have to take action, and the

financial costs for possible legal advice are within the usual range that a company has to spend in order to conduct its business in a legally compliant manner on the EU market.

724 The Worldcoin Foundation has not (explicitly) addressed the one-month deadlines for bringing the processing into compliance with Article 17 GDPR pursuant to Sections XI. and XIV. A brief reference to the reasonableness and appropriateness of the one-month period is therefore sufficient to address this issue.

725 The effort required to fulfil these obligations can be classified as low. The obligation is limited to designating a contact channel for data subjects to raise objections to the data processing of their iris code or SMPC shares and to request the erasure of their personal data. Of course, a team would also have to be available to review these requests and, if a request is justified, initiate the necessary measures to comply with the request.

726 As already explained under 1., the right to erasure is one of the central pillars of the GDPR. The fact that it is not possible for data subjects to request erasure at all is therefore a situation that is not in line with the fundamental mechanisms and notions of the GDPR. The remediation of this situation is therefore of significant urgency and the deadline of one month is appropriate.

727 The Worldcoin Foundation has also not commented on the one-week deadlines for providing proof to the BayLDA of the fulfilment of the orders pursuant to sections XI., XIII., XV. and XVII. of the decision.

These deadlines are clearly adequate. The orders only require the Worldcoin Foundation to explain to the BayLDA what measures have been taken to implement the orders under Sections II., IV., VI., VIII., X., XII., XIV. and XVI. within one week of the implementation. It is possible for the Worldcoin Foundation to document the measures taken without significant effort while it fulfils its obligations under sections II., IV., VI., VIII., X., XII., XIV. and XVI. The commencement of the deadline depends solely on the controller's conduct.

V.

Threat of penalty payment

728 The threat of penalty payments in points XVIII. to XXXIII. of this decision is based on Articles 19(1)(1), 29, 30, 31 and 36 of the Bavarian Administrative Service and Enforcement Act ("Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz" – "BayVwZVG"). The threat of a penalty payment constitutes a notice of performance subject to a condition precedent within the meaning of Art. 23 Para. 1 BayVwZVG. If an order under points II. to XVII. of this decision is not complied with, the respective penalty payment shall become due for payment without further determination (Art. 31(1) in conjunction with (3) sentence 2, sentence 3 BayVwZVG).

729 Pursuant to the first half of the first sentence of Article 30(1) BayVwZVG, in principle, the issuing authority enforces its orders itself. Under Article 20(1) BayVwZVG, the Bavarian State Office for Data Protection Supervision is therefore responsible for the threat of a penalty payment.

730 The threat of penalty is necessary to enforce the orders that are necessary and appropriate to establish a legally compliant situation.

731 Primary purpose of the penalty payment is to exert a coercive effect on the obligor. The latter should be effectively compelled to comply with the order (VGH Munich (1st Senate), decision of 27 May 2020 - 1 ZB 19.2258, BeckRS 2020, 14657, para. 8; VGH Munich (10th Senate), decision of 19 July 2017 - 10 ZB 16.133, BeckRS 2017, 121554, para. 12).

732 Within the statutory range of EUR 15 to EUR 50,000 (Art. 31 para. 2 sentence 1 BayVwZVG), the authority has a wide margin of discretion in which the circumstances of the individual case must be taken into account (VGH München (9. Senate), decision of 9 November 2021 - 9 ZB 19.1586, BeckRS 2021, 36719, para. 10; VGH Munich (9th Senate), decision of 14 December 2022 - 9 ZB 22.1519, BeckRS 2022, 38968, para. 8).

733 Circumstances to be taken into consideration may include, in particular: The urgency and importance of the matter, the intensity of the obligor's refusal, the obligor's financial capacity and the obligor's economic interest in not complying with the order (*Troidl,* in Engelhardt/App/Schlatmann, VwVG VwZVG, Section 11 VwVG, para. 8a; *Deusch/Burr*, BeckOK VwVfG, Section 11 VwVG, para. 13; *Hanno-Dirk Lemke*, Verwaltungs-Vollstreckungsgesetz, Section 11 VwVG, para. 9).

734 The latter circumstance is particularly emphasised by the BayVwVZG in Article 31(2) sentence 2 BayVwVZG. According to Art. 31(2) sentence 2 BayVwVZG, the penalty payment is intended to cover the economic interest that the obligor has in performing or refraining from performing the act. Art. 31(2) sentence 1 BayVwZVG therefore stipulates the economic interest of the obligor in not complying with the order as the basic minimum amount of the penalty payment, without limiting

the amount ('lower limit', cf. wording of Art. 31(2) sentence 1 BayVwZVG 'should reach'). The economic interest does not have to be proven by the authority (VGH Munich (15th Senate), decision of 29 April 2008 - 15 CS 08.455, BeckRS 2008, 27867, para. 19; VGH Munich (1st Senate), decision of 27 May 2020 - 1 ZB 19.2258, BeckRS 2020, 14657, para. 8). Rather, the authority may estimate the economic interest at its own discretion in accordance with Art. 31(2) sentence 4 BayVwZVG without the need for a special justification for the estimated amount of the economic interest (VGH Munich (9. Senate), decision of 3 April 2023 - 9 ZB 23.79, BeckRS 2023, 8772, para. 9; VGH Munich (1st Senate), decision of 16 September 2010 - 1 CS 10.1803, BeckRS 2010, 31731, para. 23 f.).

735 On the basis of these requirements and taking into account the circumstances of the individual case, the penalty payments under points XVIII., XX., XXII., XXIV. and points XXVI., XXVIII., XXX, XXXII. are each necessary in the amount of the statutory maximum of € 50,000.00 in order to achieve a sufficient coercive effect to ensure compliance with these orders.

736 With regard to points XVIII. and XXVI., which are related to the erasure orders under points II. and X. respectively, it must be taken into account that a rapid and effective remedy is necessary due to the far-reaching interference with the fundamental rights of the persons concerned. A penalty payment was therefore to be threatened, which with sufficient certainty achieves the necessary compliance effect to prevent the perpetuation of this serious unlawful situation. In addition, the Worldcoin Foundation's interest in not complying with the erasure orders must be taken into account. The erasure order means that the Worldcoin Foundation must delete a large proportion of the iris codes it has collected to date and of the files derived from them (SMPC shares). In addition, the processing of the iris codes and the files derived from them (SMPC shares) is closely related to the Worldcoin cryptocurrency, the number of which is limited to 10 billion, with 25% earmarked for the initial developer team, investors and as reserves. It can therefore be assumed that the Worldcoin Foundation has a considerable interest in not complying with the erasure orders.

737 With regard to points XX. and XXVIII., which are related to the order of compliance with Articles 5(1)(a), 9(1) GDPR and Articles 5(1)(a), 6(1) subparagraph 1 GDPR pursuant to points IV. and XII., respectively, the fundamental importance of the objective pursued by points IV. and XII. must also be taken into account. The processing carried out by the Worldcoin Foundation in its current form constitutes a massive interference with the fundamental rights of the data subjects. In order to prevent a repetition of the current serious unlawful situation, the order to bring the processing into compliance provided for in points IV. and XII. must be accompanied by the threat of an effective penalty payment. It must also be considered that the order has significant consequences for the design of the Worldcoin Foundation's "product" and therefore it must be assumed that the Worldcoin Foundation has a not insignificant interest in non-compliance with the order.

738 With regard to points XXII. and XXX. of the decision, which refer to the order of compliance with Article 17 GDPR according to points VI. and XIV. respectively, the considerations already made in

the two paragraphs above apply accordingly. The right to erasure under Article 17 GDPR is, alongside the right of access under Article 15 GDPR, the central pillar of the protection of data subjects and the embodiment of informational self-determination, i.e. the sovereignty of the data subject over their personal data. Not giving data subjects the opportunity to oppose the processing of iris codes or SMPC shares and to request the erasure of this personal data constitutes an interference with the essence of the rights under Articles 1(1) and 2(1) of the Basic Law of the Federal Republic of Germany and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Therefore, with regard to the order to implement such an option, a penalty payment had to be chosen that would lead to the certain elimination of this fundamentally unlawful situation. Here, too, it was taken into account that the Worldcoin Foundation has a great interest in non-compliance with this order, as its system is fundamentally based on the fact that once the iris code has been collected, the data subjects no longer have any control over the iris codes or the SMPC shares derived from them. In this respect, the close connection between the processing of the iris codes and SMPC shares and the cryptocurrency Worldcoin should be emphasised again.

739 The above considerations also apply with regard to points. XXIV. and XXXII., which refer to the order to cease processing the iris codes and SMPC shares until the fulfilment of the obligations under points. IV. and VI. as well as points. XII. and XIV. respectively pursuant to points. VIII. and XVI. of the decision. This order is of central importance for the protection of data subjects whose iris codes and SMPC shares could otherwise continue to be processed unlawfully by the Worldcoin Foundation, without the Worldcoin Foundation having to fear state intervention. In view of the seriousness of the interference that the processing of this data entails for the interests and rights of the data subjects, a penalty payment that generates a sufficient coercive effect was to be threatened. In this respect, the high interest of the Worldcoin Foundation in non-compliance with these orders was also taken into account. The Worldcoin Foundation is convinced of the legality of the current design of the project, i.e. the processing of iris codes or SMPC shares without obtaining the consent of the data subjects, and considers this circumstance to be indispensable for its project. In addition, the close link between the processing of the iris codes / SMPC shares and the success of the cryptocurrency Worldcoin should be emphasised once again.

740 An amount of €5,000.00 was chosen for the penalty payments under points XIX., XXI., XXIII., XXV., XXVII., XXIX., XXXI. and XXXIII. because there is a high public interest not only in the fulfilment of the orders under sections II., IV., VI., VIII., X., XII., XIV. and XVI. but also monitoring proper fulfilment of these orders according to points. III., V., VII., IX., XI., XIII., XV. and XVII. is of central importance. In order to generate a sufficient coercive effect with regard to the necessary co-operation of the Worldcoin Foundation - which it is obliged to provide - the imposition of a penalty payment of €5,000 each was necessary and proportionate.

741 The deadlines for implementing the orders provided for in points II. to XVII. are necessary and proportionate in view of the scope of the infringements (see already IV. of the reasoning).

742 The BayLDA's authority to impose fines on the controller in the event of non-compliance with the orders issued with this notice pursuant to Article 58(2)(i), 83(5)(e),(6) GDPR remains unaffected by the issued threats of penalty payment.

VI.

Decision on the costs of the proceedings

743 The decision on the costs follows from the first sentence of Article 19(6) of the BayDSG (Bavarian Data Protection Law) in conjunction with Articles 1 and 2 of the Bavarian Law on costs. With reference to the second and third sentences of Article 6(1) and Article 6(2) of the Bavarian Law on costs, the amount of the fee is determined by the administrative burden incurred and the significance of the infringement at issue.

Notice of legal remedies

An appeal against that decision may be brought **within one month of its notification** to the

Bayerischen Verwaltungsgericht Ansbach

Promenade 24 - 28, 91522 Ansbach.

Information on legal remedies

The appeal may be lodged in writing, by transcript or by electronic means, in a form accepted as a replacement for a written pleading. Applying for legal remedies by simple e-mail is not allowed and has no legal effect!

The persons named in § 55d VwGO (in particular lawyers and public authorities) must generally submit complaints electronically.

Under German federal law, a procedural fee is payable for proceedings being brought before administrative courts.

<Name>

This letter has been created automatically and is valid even without a signature.

Instructions on how to process your personal data:

The data controller for the processing of your personal data in the context of this contact is the Bavarian State Office for Data Protection Supervision. For more information on the processing of your data, in particular on your rights, please consult our homepage at www.lda.bayern.de/Informationen or contact us by any other means via the above-mentioned contact details.