PETs meet Biometric Identity: The case of World(coin) through the lens of evolving EU Data Protection Law and the Digital Omnibus Proposal

Abdullah Elbi[1][0009-0006-8713-6681], Bilgesu Sümer[1][0000-0003-0626-6726] and Ezgi Eren[1][0000-0001-8588-6776]

[1] KU Leuven Centre for IT and IP Law, Belgium

Abstract. What if everyone on the planet were given an equal, unique share of a new cryptocurrency, with their iris as the proof of entitlement? The World Network, (previously "Worldcoin") was set up by Sam Altman to become the most extensive global digital identity and financial network, anchored in biometric proof-of-human. Its operators scan irises and faces, derive an iris code, and issue a "World ID" together with cryptocurrency tokens. The project is pitched as a remedy for the surge of online AI-generated content, bots and fake accounts, a flood driven largely by the very generative AI tools the same actors are building. Multiple data protection authorities (DPAs) across the EU and outside have conducted investigations and declared World(coin) data processing operations unlawful and adopted measures ranging from temporary suspensions and fines to deletion orders and critical analysis of privacy-enhancing technologies(PETs) implemented by World. We argue that the legal and ethical risks of World(coin) reach further than what the DPAs have so far articulated, and that the picture is shifting again with the European Commission's Digital Omnibus package, which proposes a new personal data definition under Article 4 and a new derogation for biometric verification under Article 9 GDPR. We start by looking at the objective and function of World together with the EU enforcement record, and then analyse how the Omnibus proposals would change the legal analysis of World(coin) and similar technologies.

Keywords: Worldcoin, Biometric Data, Proof of Personhood, GDPR, Digital Omnibus, Privacy-enhancing technologies, Identity Management.

1 Introduction

World Network, or World, formerly Worldcoin, is a privately operated proof-of-human(PoH) network backed by OpenAI's Sam Altman. The website defines it as "*the real human network, an open-source protocol built to ensure every human benefits from the age of AI*". Its premise is that online services can no longer reliably distinguish people from bots, AI agents and synthetic identities, creating risks of disinformation, fraud and financial loss, including through deepfakes. Hence, by registering biometric

iris data of people, World promises to ensure “human uniqueness” as a response to those risks. The World network combines a Proof-of-Humanity (PoH) protocol, also known as proof of personhood (PoP), with a payments application (World App), the credential (World ID), and the application through which the credential is held and presented[1].

Registration requires attendance at an Orb, a purpose-built spherical device deployed across a number of countries and operated either in supervised settings or, more recently, on a self-service basis. The Orb captures images of the face and eyes and derives an iris code, and the user receives a World ID. Early enrolments were accompanied by the distribution of cryptocurrency tokens[2]. World reports that more than 18 million people are registered in multiple countries, and the issued World ID credentials have been used more than 450 million times as of June 2026.

World is expanding its services in recent months and now has promoted the World ID for dating, gaming and event ticketing, where access may depend on one-person-one-account rules, and has entered into integrations including age assurance with Tinder in Japan and facial verification for enterprise communications with Zoom[1]. Further proposed uses related to the electronic signatures and confirmation that a human authorised an action taken by an AI agent.

The lawfulness of the processing of iris data in return for tokens has been contested since the introduction of World(coin). Based on the data protection rules, supervisory authorities and courts inside and outside the European Union(EU) have ordered suspensions, corrective measures and fines, on grounds including the validity of consent, the enrolment of minors, transparency and the exercise of data-subject rights [Bavarian DPA (BayLDA) (under appeal)[3]; Spain AEPD[4]; Portugal CNPD[5]; South Korea[6]; Kenya ODPC Kenya[7]; Hong Kong PCPD[8]; Brasil ANPD[9]].

World has been changing that architecture. Enrollment data is held on the user's device. Comparison of protected representations is distributed across independently operated parties using privacy-enhancing technologies(PETs), in particular secure multi-party computation(SMPC). Zero-knowledge proofs allow attributes of the credential to be presented without disclosing the underlying representation to the relying party[1]. These measures redistribute where personal data are held and which entities can access them. That fragmentation complicates supervisory intervention and poses challenging questions for data protection authorities to enforce applicable data protection rules, including data-subject rights in relation to the processing of sensitive iris data.

Early discussion of World focused on its recruitment practices, including the use of cash and token payments in exchange for iris scans during the testing phase[2]. Jutel places such practices within accounts of crypto-colonialism, in which blockchain ventures test extractive data practices in lower-income jurisdictions under the language of development and inclusion[10]. Siad and Sagar approach the issue through the digital divide, extending the concept beyond access to connectivity to inequalities in how personal data are collected and used[11]. As World’s technical architecture became clearer through published documentation by World and the DPA proceedings, scholarship turned to the purposes and legal implications of its technology use and data handling. Martin and Weitzberg argue that proof-of-personhood (PoP) systems repurpose biometrics from distinguishing individuals from one another to distinguishing humans

from AI agents. They also maintain that privately issued credentials acquire institutional value only where states, which continue to control legal identity, recognise them[12]. Mutung'u, Martin and Brewczyńska analyse legal proceedings and DPA decisions against the World practices in Kenya through the concept of regulatory entrepreneurship, whereby firms treat legal change as part of their market strategy, noting challenges arising from enforcement of data protection rules[13].

Focusing on World's earlier architecture, Sümer and Elbi argue that the processing of iris data remains subject to the GDPR and that deriving a biometric template constitutes a security measure rather than anonymisation, contrary to the position defended by World before DPAs[14]. Orsini examines the classification of the uniqueness check as biometric identification under Article 9 GDPR requiring a suitable derogation and notes that, against private-owned identity management like the case of World, eIDAS 2.0 retains public oversight of legal identity within the EU[15]. However, these analyses predate World's post-2024 architectural changes and do not examine them against the subsequent development of EU data protection law.

Under the EU's simplification agenda for digital rulebook, the Digital Omnibus Proposal (DOP) proposed amendments to the applicable GDPR provisions including the very concept of personal data, a mechanism for specifying when pseudonymised information ceases to be personal data, and a new Article 9 derogation for biometric verification where the biometric data, or the means required for verification, remain under the data subject's sole control[16]. In parallel, the European Data Protection Board (EDPB)'s Guidelines 01/2025 on Pseudonymisation[17] and draft Guidelines 02/2026 on Anonymisation address how identifiability is to be assessed by reference to a particular entity and a particular processing operation[18].

This article uses World as a use case of the proposed reform in the GDPR and the recent EDPB guidelines. It asks how the DOP and the developing interpretation of personal data and anonymisation would change the classification of the biometric information processed within World ID, and whether and how the proposed biometric verification derogation under Article 9 GDPR would affect similar biometric identity systems.

These questions are not confined to World. Reliance on biometric data in identity management is increasing across the EU beyond its common use in law enforcement and border management. The revised eIDAS framework provides for European Digital Identity Wallets, which will be available by 2030. To allow people to use their phones like a travel document, the Commission has been working on digital travel credentials (DTC), which are a digital representation of passports and identity documents[19]. These systems differ from the World in purpose, legal basis, and institutional setting, it shows the direction towards more digitalisation in legal identity, relying on more and more processing of personal and biometric data of individuals.

Section 2 describes World's successive architecture following the DPA decisions by the BayLDA and outside the EU. Section 3 examines the World's data processing operations in the light of EU case law and guidelines on personal data and under the proposed amendments in the DOP. Section 4 ends with moderate policy recommendations and concluding remarks.

2 "In progress" from Worldcoin to New World: Regulatory Pressure and Architectural Redesign

This section sets out how World's architecture and, in particular, processing of iris data changed over time following the DPA decisions. The new World redesign changed the flow of processing biometric iris data at two points. First, the enrolled iris data moved to the user's phone. Second, the complete iris codes of all enrolled people were replaced by distributed shares for de-duplication checks.

2.1 Changes for local storage of iris codes and additional encryption measures – "Personal Custody"

World's iris capturing and processing functions in the following manner: The Orb captures the face and eyes and performs the initial enrolment as a first step to get the World ID. The captured images of the user's face and eyes are used to derive a numerical representation of the iris, referred to as an iris code. The system then compares the new iris code against the enrolled population. The purpose is to determine whether the person has already registered, and this process is called "uniqueness check", "duplicate biometric enrolment check" or more generally "de-duplication checks"[20]. Since there is no reference template previously supplied by that user, the new representation must therefore be compared against the representations of existing enrollees. It is important to note that the uniqueness check at the registration stage differs from later biometric authentication, where an individual uses World ID to access services. Later authentication can instead compare the current user against a reference associated with the verified World ID. The legal classification of these operations, namely biometric identification(1:n) vs verification (1:1), is addressed in Section 3.

World's earlier architecture relied on a centrally managed database of iris codes to support the so-called population-level deduplication checks. The central management of this database could be deemed a riskier choice, but World notes that access to the database was restricted through encryption, hardware security modules and organisational controls to increase security. In March 2024, the Spanish and Portuguese supervisory authorities temporarily restricted World's biometric processing[21]. Authorities in Hong Kong and South Korea later adopted enforcement measures[22]. The BayLDA completed the first stage of its EU investigation in December 2024. Its decision required changes concerning erasure and consent, while other issues remained under examination or appeal. These proceedings did address the security of the iris codes stored in the centrally managed database, but they did not stop there. The published decisions and notices also concerned transparency, consent, children's data and the exercise of data-subject rights such as right to erasure.

In parallel to the ongoing DPA proceedings, World introduced Personal Custody feature in March 2024[23]. Under the published design, the Orb encrypts facial and iris images, metadata and derived information generated during enrolment. The encrypted package is transferred to the user's device and the Orb deletes its local copy after the

transfer. Hence, Personal Custody, which attempts to allow users to be in control of their biometric data, changed where enrolled biometric data were retained.

2.2 Introduction of distributed shares for de-duplication checks

While the changes above have addressed some of the security and transparency issues raised during the proceedings, they did not remove the need to compare a new iris code against those already enrolled. World therefore introduced secure multi-party computation(SMPC) in 2024 for the deduplication stage.

Under SMPC, each iris code is divided into secret shares. Separate computing parties receive different shares. They perform the comparison jointly without first reconstructing the complete iris codes in one location. World announced in May 2024 that it had deleted the former central database consisting of iris templates after deploying this system. The first deployed SMPC arrangement involved entities connected to Tools for Humanity, the Orb and technology provider of the World, and the World Foundation.

The SMPC approach did not remain in place for much long. World later replaced it with what it calls anonymised multi-party computation (AMPC) and the migration was completed in January 2025. World argues that AMPC retains secret sharing but changes the output of the comparison and reveals only whether a match was found[24]. The iris templates and associated masks remain divided between the nodes during the calculation. The participating organisations for the AMPC also changed in a manner that neither Tools for Humanity nor the World Foundation operates a node. According to World website, the AMPC node operators consist of commercial entities and university research centres, including the University of Erlangen-Nuremberg (FAU), UC Berkeley Centre for Responsible Decentralised Intelligence (RDI), the Korea Advanced Institute of Science and Technology (KAIST), the University of Tokyo and Nethermind, including commercial entities and university research centres, noting that the list may change over time. The protocol and parts of its implementation are all publicly available.

World relies on these features to describe the AMPC shares as anonymous. Its argument is that an individual node, in this case each one of the research centres, receives neither the complete iris code nor sufficient information to attribute its share to a person, and the nodes receive only the result required for deduplication. However, this legal position is not tested and confirmed by any DPA in the EU yet.

Importantly, the BayLDA decision, like the other DPA decisions, concerned an earlier version of World's architecture and the changes introduced during the relevant investigations. It does not assess the current AMPC arrangement and iris data processing in its deployed form. The following section therefore examines that new architecture, referring both to SMPC and AMPC, in light of the BayLDA's reasoning, the proposed Digital Omnibus amendments and the EDPB's recent guidance on pseudonymisation and anonymisation.

3 Analysis of World's data processing operations in light of EU case law and authoritative guidelines

3.1 Iris codes: Biometric, Personal or Anonymous Data?

World argues that their processing technique of iris images, decentralised storage solutions and SMPC/AMPC applications answer most personal data challenges under the GDPR by ensuring efficient anonymisation. More specifically, it argues that SMPC (and later AMPC) prevents the encrypted secret shares relating to the iris code from being reconstructed, effectively anonymising the iris codes.

The BayLDA had decided in December 2024 that this was not the case and the iris codes and secret shares encrypted under SMPC remained personal data and biometric data[3]. Significantly, the technical changes introduced by World and the changes proposed under the DOP might impact BayLDA's line of reasoning regarding controllership and personal data. Therefore, in this section we will assess the BayLDA decision in light of the recent developments in EU law including the case law and the EDPB guidelines, asking whether World's proposed decentralised storage solutions and SMPC/AMPC applications would allow to categorise the processed data as anonymous. We will tackle this question from the two different perspectives presented by absolute (simplified) and relative (contextual) approaches. Our assessment will also look at the actors: If the data would still be deemed personal data, for whom would this be the case? For instance, would the contractual arrangements between World entities and further division of processing to universities achieve non-identifiability? As will be explained below, we believe it is still possible to argue that the data processed by World is personal data and further biometric data, since the parties might have 'the means' that are reasonably likely to be used to identify the data subjects.

The GDPR – definition of personal data. Personal data is defined in the GDPR as any information relating to an identified or identifiable natural person. Recital 26 adds that in assessing whether a person is identifiable, one must consider all means reasonably likely to be used, whether by the data controller or *by any other party*, to identify them either directly or indirectly.

Currently, there are two readings of the GDPR's definition of personal data: absolute (objective) and relative approaches. Some scholars consider that the GDPR takes a comparatively absolute approach in defining personal data[25].

This camp reads *all the means reasonably likely to be used by any other party* to imply that if some data are personal for one entity, it is regarded as personal data for everyone, regardless of who is processing it. Some argue the reading of the CJEU also leans towards an objective approach[26, 25], while others disagree[27, 28].

The objective reading of the GDPR is seen problematic as the definition becomes too broad and thus inapplicable in practice[29].

Relative approach, in contrast, considers a person identifiable only if the processing entity or the recipient has the reasonable means to identify them[25]. Below, we explain both of these approaches in the context of World's processing.

The absolute (simplified) approach. The absolute or the "simplified" approach according to the new EDPB guidelines on anonymisation considers data identifiable when any party, regardless of the controller, can identify the data subject. Accordingly, as long as there is a possibility for the re-identification, the data at hand is deemed personal.

As for SMPC/AMPC, we argue that these methods do not completely preclude the possibility of reconstructing the personal data at the origin. For instance, if an attacker (or a legal order) can compel decryption secrets from several participating parties at once, they may be able to decrypt the secret shares and reconstruct personal data. Therefore, according to the absolute approach, SMPC is not an anonymisation technique. It can rather be construed as a decentralising security measure and ultimately merely as a pseudonymisation technique.

As will be explained below, the DOP emphasises the 'relative (contextual) approach, specifically through a change in the scope of personal data in GDPR Article 4(1)(a). Under the proposed wording, information would not constitute personal data for a given entity where that entity lacks means reasonably likely to identify the person concerned, even if another entity possesses such means. Therefore, the absolute approach is likely to soon take a back seat in the interpretation of the definition of personal data and the above reasoning may not be the prominent one in future proceedings by DPAs and before courts.

The relative (contextual) approach. The relative or the "contextual" approach as named by the EDPB, takes a narrower stance and considers specifically the means available to the entity that processes the data, by taking into account the specific facts of the situation. The question "who can realistically gain access to the data" takes on a key importance.

Some seminal CJEU decisions are worth mentioning here, namely Breyer[30], Scania[31] and SRB[32]. In Breyer, the Court held that, in the context of dynamic IP addresses, information can qualify as personal data even where the data necessary to identify the individual is not all held by one single entity (para 43). To assess whether a person is identifiable, all means reasonably likely to be used must be taken into account (para 42). In this case, the entity in question had legal means to obtain additional data from a third party that could enable identification. The Court held that data qualifies as personal even where identifying an individual would require recourse to legal means. This extends to scenarios where a data controller might approach a competent authority to obtain data through legal proceedings, in order to identify relevant individuals, for instance, in the aftermath or during a cyberattack (para 47).

In Scania, the Court held that a vehicle identification number (VIN) constitutes personal data where a party (repairer) possesses the means to link it to a specific natural person. While a VIN may not, in and of itself, constitute personal data for every entity that holds it, it can nonetheless acquire that status indirectly once it is disclosed to another party equipped with the means to identify the individual concerned (para 49).

Finally, in SRB, the Court ruled on pseudonymised data, which links it to this article since encrypted data is usually considered pseudonymised[17, 33, 34] and World's data was deemed to be pseudonymised by BayLDA[3]. The SRB case concerned whether pseudonymised shareholder comments that were gathered in connection with a bank resolution process qualified as personal data after it is shared with a third-party auditor. The Court found that personal opinions expressed in the comments are inherently linked to individuals and the SRB retained the means to identify the commentators, hence, the information in question constituted personal data from the SRB's perspective.

The relative approach emphasises the necessity of considering each situation in its own context, taking into account all the means that are available to controllers or processors, and whether these means are reasonably likely to be used. In the case of World, the analysis concerning the identifiability of the data processed by World, according to the relative approach, is not straightforward due to so-called decentralised features (in particular of SMPC/AMPC) of the technology. As explained above, SMPC and AMPC operate with secret shares that are available to different parties. These are encrypted pieces of the personal data at the outset and are arguably not themselves identifiable.

However, based on the current data protection guidelines and case law, it is possible to argue that the AMPC simply achieves pseudonymisation from the perspectives of the processing entities. As acknowledged by the EDPB in its 01/2025 Pseudonymisation Guidelines, pseudonymisation secrets are a core part of the additional information defined in Art 4(5) GDPR[17, para 86]. As an extra security measure, such secret information can be divided into pieces, and each can be stored by different entities, as in the case of World's AMPC[17, para 108]. The technique ensures that no single entity can reverse the original data or input without the cooperation of other parties involved. In other words, with the cooperation of the parties holding the "additional identifying" data, it is still possible to reverse the original data. That said, it should not be neglected that this technical possibility diminishes as the number of independent parties involved increases. The same logic can be also found in BayLDA's reasoning: splitting the secrets into shares while cooperation between different entities holding the shares is still possible achieves at most pseudonymisation and not anonymisation[3, para 345] .

EDPB also expressly mentions in its anonymisation guidelines that an individual would be considered indirectly identifiable for a specific entity, if that entity could, by using means that are reasonably likely for them to use, "[apply] methods (such as decryption of encrypted parts of the data) that are controlled by other parties" [18, para 20]. The mere fact that the decryption methods for encrypted shares are controlled by other parties does not preclude identifiability, "provided that these elements can be combined through means reasonably likely to be used by the respective entities" [3, para 20; 30, para 43; 31, paras 45-49]. Here, the likelihood of identifiability does not have to be zero: a likelihood that is insignificant in reality, taking into account the context and the actors, would be sufficient to declare the data anonymous[18, para 22; 32, para 82]. The EDPB notes the CJEU's approach to the reasonably likelihood is focused on the elements that would prevent the use of the means in question. According to the CJEU in SRB, the likelihood of reidentification would be deemed insignificant either because of a factual impossibility, a need for disproportionate effort or a legal prohibition. [18, para 26; 32, paras 82-32]. In the context of World, BayLDA stated that there

was no evidence showing a practical impossibility through disproportionate effort or a specific legal prohibition that would prevent bringing different shares back together [3, paras 363-367].

Additionally, EDPB notes that the term “means” should be interpreted broadly, and that the possibility for an entity to take advantage of another entity’s means would also fall under this [18, para 28]. In World’s case, the economic and infrastructural collaboration between different entities could provide such additional means and thus facilitate the identifiability.

Following the Breyer, the additional identifying data might be obtained from a third party or transmitted to a recipient. If the parties who are supposed to be independent instead cooperate covertly, they can regenerate the secret without the user's knowledge or consent[35]. If different secret shares can be brought together through cooperation or collusion between different parties, the data may become personal again. The key question is who holds the pieces and whether they can be made to cooperate, and BayLDA decided in line with Breyer in its December 2024 decision. In World’s earlier SMPC infrastructure that BayLDA took into consideration, two parties involved in Shamir’s secret sharing, including Tools for Humanity and the Worldcoin Foundation's EU entity, are closely affiliated with each other rather than being fully independent parties. [3, paras 346-348]. Moreover, the written contractual provisions aiming to prevent bringing the shares back together between them would not provide any real challenge [3, para 360], especially if both parties wanted to violate the contract provisions in the same direction.

A significant development since the BayLDA decision is that World is extended to include new and relatively independent third parties under the new AMPC architecture, such as universities. Yet, it is crucial to note that these parties already agree to work together, that they are parties to a business. The technical infrastructure does not protect against the potential reconstruction through their collaboration, therefore it does not preclude identifiability. In this technical context, only institutional independence and legal barriers to compelled disclosure do, and we believe whether World's current infrastructure achieves anonymity is still open to debate and needs legal clarity .

Another important perspective to this debate regards the common infrastructure as technical means used by the parties. It is noted by BayLDA that the parties use the same cloud computing infrastructure (Amazon AWS), which makes the separation of shares less secure. The first reason for that is centralised servers as such create a single point of failure, hence vulnerable to internal and external adversaries[3, para 350]. Moreover, it is not impossible for large cloud service providers to be attacked and hacked, they are rather frequently attacked. It is worth noting that under the new AMPC architecture, each party is still using the same cloud providers, namely (Amazon AWS) as in the case previous one. Therefore, BayLDA’s line of reasoning for this point remains applicable to the current functioning of World.

As noted by EDPB anonymisation guidelines, in certain cases, the data may become identifiable due to actions of unauthorised or malicious actors. To address the risks posed by internal and external adversaries, it is important to securely pseudonymise personal data as stated by the ENISA[33]. EDPB lists some factors that are relevant to realistically assess the likelihood of such identifiability occurring, such as “evidence

that the legal prohibition is not effectively monitored, enforced and sufficiently dissuasive", "evidence that the gains from breaking the legal prohibition might outweigh costs, effort and potential risks of doing so" and "and evidence that the prohibition has previously been breached or circumvented in comparable situations"[18, para 33]. BayLDA decision also addresses the possibility of attackers hacking World's databases. It mentions the sensitivity, importance and scale of the processing done by World and reminds that it would attract not only ordinary hackers but also skilled attackers and criminals. In this context, such third parties the means that are reasonably likely to be used by them should also be included in the assessment of identifiability[3, para 378].

Importantly, both BayLDA and EDPB's anonymisation guidelines refer to the impact of the purpose and effect of data processing activity, in determining whether the data is anonymous or not: as the main purpose of the processing of the secret shares is to identify or single out the individual and this processing creates a direct effect on the individual, namely to decide whether they can register or pay using the World system, it would be self-contradictory to deny the personal data nature of the secret shares [3, paras 351 and 452; 18, para 16], Following this line of reasoning, BayLDA also determines that the split shares of iris code i.e., the numbers that are produced by an algorithm, are still biometric data. This is because while the random numbers may have seemingly no relation to the actual iris codes or the images, but they still function to create impacts on the individual, and thus conserve the risks and effects of the iris codes. [3, Para 354]

By the same vein, BayLDA stated that World's processing of iris images entails a number of fundamental data protection risks for a number of data subjects, and it does not comply with GDPR[3]. Accordingly, an order to erase presupposes the existence of personal data, not data that are already rendered anonymous.

The DOP Changes. Under the DOP amendment of personal data this legal claim can be more likely to be true considering DOP proposes to amend the definition of personal data by adding the following paragraph: *"Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.*" (emphasis added, DOP Art 3(1)(a)). By this definition, each individual share, in isolation, may fall outside the definition of personal data because the parties (nodes) cannot reconstruct an iris code from their single share; they might easily argue that they lack the means reasonably likely to be used to identify natural persons. Notably, after objections from the EDBP and EDPS[36], a leaked draft of the Council seems to remove the proposed definition of personal data, thus at the moment it is not certain whether the proposed definition will stay in the aftermath of the legislative trilogue[37].

The proposal also adds a new Article 41 a: the Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities". This technology-specific approach of the legislation, if it passes as it is, can still provide some level of legal protection or clarity. However, it is worth noting that this provision was criticised by scholars as it might lead to an unfair application of the GDPR[38].

In addition, the EDPB and EDPS objected this provision, stating that the Commission should not decide what is no longer personal data after pseudonymisation techniques applied[36].

Potential of PETs to achieve anonymisation. It is important to emphasise that the BayLDA does not argue that anonymisation cannot ever be achieved via privacy enhancing technologies such as SMPC. It rather states that the specific technologies and security measures deployed by World at the time of the decision were not sufficient to achieve anonymisation, considering World's specific context.

In light of the BayLDA's nuanced approach to PETs, the recent case law including the SRB case, and the anonymisation guidelines by the EDPB, it may indeed reasonably possible to achieve anonymisation, especially from the perspective of the relative or the "contextual" approach. The three criteria specified by the EDPB, namely no record isolation, no linkage, no inference, bring clarity on how to assess identifiability and technical aspects of anonymisation in a number of scenarios and may facilitate PET developers to achieve full anonymisation[18, section 3.4].

Similar to the EDPB, the Norwegian Data Protection Authority has also acknowledged the future potential of privacy enhancing technologies such as fully homomorphic encryption (FHE), to increase the security of encryption and encrypted data, "as well as its potential use in other areas that can benefit from analysing and processing data, such as on cloud while preserving confidentiality" and therefore without revealing personal data[39].

3.2 World's biometric verification would still fall under the GDPR Article 9(2)

With regard to the initial biometric data processing, the Orb processes iris images only locally and deletes them after extracting the biometric references. No raw biometric image is stored. This on-device processing both on the user's phone and at the Orb still falls under the definition of biometric data under the GDPR, as the GDPR applies exactly to the biometric references and templates that went through specific processing rather than biometric images in Article 4(14). Hence, an appropriate legal basis is required for processing such data; in World cases, they were relying on explicit consent for the users and legitimate interest for the de-duplication checks.

The current version of the GDPR applies to both verification (one-to-one comparison) and identification (one-to-many comparison) functions, and these are listed among the prohibited processing operations in Article 9, subject to limited derogations.

The World employs a bundle of decentralised solutions that can nuance our answer. Instead of one company running a centralised 1:many match against a database under its full control, the uniqueness checks are split across parties who each see encrypted fragments of the biometric template. The comparison is done too on these encrypted fragments. This itself does not change the fact that the uniqueness check is being done. Moreover, the Orb is still connected to centralised hardware and an enrolment system that later transmits biometric data into a cryptographically split multi-party storage and computation layer, which can be seen as a security measure.

The DOP introduces a new exemption under Article 9(2) GDPR to allow processing of biometric data where necessary to confirm the identity of a data subject (verification) or to authenticate an individual, provided that biometric data remain under the sole control of the data subject[1]. This exemption brings two main issues to our attention: 1) the distinction between identification and verification; 2) the condition for the biometric data to remain under the "sole control".

Verification vs identification. The proposed provision draws an explicit distinction between verification and identification. In other words, it aims to create an additional legal basis for processing biometric data particularly for biometrics verification that aims to establish the claimed identity of individuals.

As explained in Section 2, World changed its infrastructure architecture, in response to ongoing or completed DPA proceedings. Now the iris codes are stored locally on each user's mobile device. This change would not change the status of the World's biometric data processing according to the current version of the GDPR Article 9. Even if considered as verification, such processing would still be subject to the prohibition in Article 9 on special categories of data. However, if the DOP provision passes as drafted, it is possible for the Foundation to argue that the special category prohibition in Article 9 would not be applicable, since biometric data are stored only in the user's device.

On the other hand, as explained in Section 2, the deduplication checks are still done with 1:many comparison to ensure the new user is not registered to the system before, which would still fall under Article 9 restrictions, even with the DOP exemption. It is important to note that the World Foundation describes deduplication checks as a necessary step to avoid fraud and ensure trust towards the identity by comparing the new Iris codes against the ones stored before, currently consisting of more than 18 million samples. Moreover, they argued in the BayLDA investigation that they do not do biometric recognition but only check human uniqueness (which, as a term, does not exist directly within biometric technical standards). Relying on this argument, World treated the processing of iris codes as non-sensitive personal data processing and based the processing activity on legitimate interest to ensure trust in the service, according to GDPR Article 6(1)(f). However, as explained above, BayLDA did not agree and stated

[1] The wording used by the DOP for this new exemption is as follows: *"(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'"* (DOP Article 3(3)(a))

that such uniqueness checks are processing of sensitive data, hence the requirement for the World to identify a legal basis under GDPR Article 9 for this processing [3, paras 502-508]. This raises the question of whether one of the already existing exemptions under Article 9 could apply to such processing. Currently, there is no guidance on how this very common procedure will be categorised under the GDPR. In our view, due to the highly sensitive nature of biometric data and the risks related to their processing, such processing for biometric verification purposes should still be subject to the general prohibition of Article 9. Moreover, it should not be neglected that biometric verification systems operate with unique identifiers that are often connected to user accounts that consist of various types of personal data depending on the service provided. In this case, third parties such as Tinder and Zoom indeed use such unique identifiers relying on the verification carried out through World ID. While these unique identifiers can be special category or regular personal data, their processing is still subject to the GDPR and requires a valid legal basis. Identifiability of this type, i.e., biometric verification connected to user account data vaults, is not risk-free. First of all, biometric data function as the key to the rest of the digital identity of the data subjects. Compromise of these data would result in the leakage of the rest of the data vault, often without available means to become aware of it or contest it by the data subject. Where biometric verification is used, it provides certainty that the person is indeed the one originally registered, for example, through a uniquely assigned identifier[40].

Second, biometric verification systems might not eliminate surveillance risks that are often attributed to biometric identification systems. As Renieris writes, "even as the digital realm becomes more invisible, human beings are becoming more machine readable through the proliferation of biometric-enabled digital identity tools and technologies"[41]. Biometric verification systems still require capturing and storing biometric data, which can later be repurposed, linked across contexts, leaked or accessed by third parties. Moreover, the infrastructure, such as the sensors, templates, or algorithms, can be redirected towards identification functions. Thus, it is plausible to argue that the distinction between these two functions may be more fragile in practice. Consequently, it should not be neglected that framing biometric verification systems as inherently privacy-preserving risks undermining the surveillance capacity they actually create.

4 Conclusion

The legal proceedings and DPA decisions concerning World have demonstrated that data protection law serves as a core basis for public intervention against large-scale biometric digital identity systems managed by private entities. As highlighted above, authorities within and outside the EU have issued enforcement decisions, corrective orders and fines, while several proceedings remain pending, exposing serious problems in World's large-scale collection and use of iris data and facial images.

The regulatory backlash also pushed World to redesign its architecture and introduce new safeguards and PETs. Yet it is hard to argue that these changes could resolve all the legal issues resulting from World's biometric data processing operations, and indeed not all of them were about the security of the biometric data at stake. Questions

concerning consent, economic inducement, transparency, and large-scale biometric enrolment remain open and are connected, hinging on the applicability of the GDPR and the legal nature of World's processing of biometric data with PETs.

The Digital Omnibus Proposal now aims to amend the GDPR under which those interventions by the EU DPAs were made. This article has examined two of its elements with regard to World, the treatment of the personal-data concept and the proposed derogation for biometric verification under Article 9.

On the first, the proposed approach to identifiability, if the Commission text prevails on this point, would have consequences across biometric and other identity systems built on PETs. It strengthens the position of a private actor asserting that distributed processing has rendered the information anonymous from its own perspective. Where that assertion succeeds, personal data and biometric data definitions' threshold cannot be reached, and the Article 9 strict regime falls away together with other data protection obligations, while the risks to fundamental rights and freedoms related to biometric data processing remain. Considering the questions raised by the BayLDA about the efficiency of anonymisation in such distributed processing cases, ultimately, this change is likely to weaken the data subject rights and protections granted by the GDPR and enforced by DPAs so far, which initially compelled World to redesign its systems in accordance with applicable data protection rules.

On the second, there is little doubt that Orb enrolment constitutes processing of personal data and biometric data. The open question concerns what happens to the iris templates afterwards, following the introduction under the multi-party arrangement of the so-called AMPC.

Whether the shares are pseudonymised or anonymous under the EDPB's guidelines depends on the AMPC arrangements as deployed. However, the DOP might add a separate institutional layer. Even if the proposed amendment to the personal data definition is not retained, the Commission could still be empowered with the proposed Article 41a to adopt implementing acts specifying when pseudonymised data cease to constitute personal data for particular entities. Those acts would likely influence the classification of data processed by World and comparable identity-management systems, and therefore heavily define the scope of the GDPR for such processing activities. Two consequences follow if AMPC shares are personal data. Nodes operated outside the EU (located in the US) raise an international data transfer question. Moreover, the parties run on a common cloud provider, impacting the analyses on anonymity as the BayLDA raised similar concerns about concentration of access via the same cloud provider. Second, the newly proposed derogation for biometric verification under Article 9 GDPR could provide World with an alternative condition for processing special-category biometric data both for the existing users who verify themselves via World ID and for the de-duplication or "uniqueness" checks for new users. It would not, however, replace the need for a legal basis under Article 6 GDPR, which seemed not to be a concern since they were relying on consent for the enrolment and legitimate interest for the de-duplication checks. Its relevance lies in World's current reliance on explicit consent under Article 9(2)(a), which has been contested because token incentives may affect whether consent is freely given. Hence, the derogation could facilitate later verification based on an existing World ID. It would not cure defects in the biometric enrolment

through which that credential was created and the de-duplication process. This distinction matters where the initial collection of iris data was based on disputed consent. The strongest counterargument is that enrolment and subsequent verification are separate processing operations and may rely on different legal grounds, but this is still to be examined by the DPAs and with the fate of the DOP.

World's recent report published in June 2026, named *The Simple Plan*, states that the project entered the third phase, and among other priorities, taking the pragmatic approach, they will concentrate operations on a core set of countries where proof-of-human products already show early adoption, among them Germany, and the United Kingdom[42]. Each of those jurisdictions has relatively robust data protection laws, including the EU and UK GDPR, and their DPAs have already worked on the World's contested technology. The system is likely to continue to be built out under close scrutiny at the same time as the data protection rules governing it in the EU are being renegotiated, and World continues to add more services and biometric modalities while that is unresolved.

How the Digital Omnibus settles the personal-data definition and the biometric verification derogation will definitely shape what World operations will look like in the EU. But without doubt, World's development and evolving architecture will remain an interesting regulatory use case to test the robustness of data protection laws and fundamental rights in the EU and outside.

Acknowledgments. Abdullah Elbi's work was supported by imec through a project at the KU Leuven Centre for IT & IP Law (CiTiP) on the legal aspects of agentic AI. Bilgesu Sümer's work was supported by EU Horizon NOUS (A catalyst for EuropeaN clOUd Services in the era of data spaces, high-performance and edge computing) and by SCAMPER (Strengthened authenticated platform for private personal information by VLAIO – ICON project number: HBC.2024.0622-). Ezgi Eren's work was supported by the Mobai, funded by the Research Council of Norway (Project n° 360776 - IPNÆRINGSLIV25.

Disclosure of Interests. The authors have no competing interests.

References

1. Worldcoin website, https://worldcoin-company-website.cdn.prismic.io/worldcoin-company-website/Zuvl4bVsGrYSvlIU_WorldcoinPrivateByDesign.pdf, last accessed 2026/07/31
2. Guo, E., Renaldi, A.: Deception, exploited workers, and cash handouts: how Worldcoin recruited its first half a million test users. MIT Technology Review (2022). https://www.technologyreview.com/2022/04/06/1048981/worldcoin- cryptocurrency-biometrics-web3/, last accessed 2026/08/04
3. Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Germany: Final decision concerning the processing of biometric data in the Worldcoin project, Decision EDPBI:DEBY:OSS:D:2024:1594, 13 December 2024
4. Agencia Española de Protección de Datos (AEPD), Spain: La Agencia ordena una medida cautelar que impide a Worldcoin seguir tratando datos personales en España, urgent provisional measure against Tools for Humanity Corporation, 6 March 2024

5. Comissão Nacional de Proteção de Dados (CNPD), Portugal, Deliberação/2024/279, Process AVG/2023/1205, 9 July 2024.
6. Personal Information Protection Commission (PIPC), Republic of Korea, Worldcoin Resolution adopted at the 16th Plenary Meeting, 25 September 2024
7. Office of the Data Protection Commissioner (ODPC), Kenya, Complaint No. 1394 of 2023, 6 September 2023 and Republic v Tools for Humanity Corporation (US) & 9 others; Katiba Institute & 4 others (Ex parte Applicants), Judicial Review Application E119 of 2023, [2025] KEHC 5629 (KLR), High Court of Kenya at Nairobi, judgment of 5 May 2025
8. Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong, The Operation of the Worldcoin Project in Hong Kong Contravenes the Personal Data (Privacy) Ordinance, Investigation Report R24-01335, 22 May 2024
9. Conselho Diretor da Autoridade Nacional de Proteção de Dados, Brazil, Despacho Decisório PR/ANPD nº 6/2025, Process No. 00261.006742/2024-53
10. Jutel, O.: Blockchain humanitarianism and crypto-colonialism. Patterns 3(1), 100422 (2022). https://doi.org/10.1016/j.patter.2021.100422
11. Siad, R., Sagar, A.: AI-powered digital identity systems and the new digital divide: the case of World. Emerging Media 3(3), 391–400 (2025). https://doi.org/10.1177/27523543251340713
12. Martin, A.K., Weitzberg, K.: Verified human? Identity inversions in our new machine age. In: Reia, J., Forelle, M., Wang, Y. (eds.) Reimagining AI for Environmental Justice and Creativity, pp. 67–69. Digital Technology for Democracy Lab, University of Virginia, Charlottesville (2025)
13. Mutung'u, G., Martin, A., Brewczyńska, M.: Regulatory entrepreneurship's threat to digital sovereignty: the case of Worldcoin in Kenya. Sci. Public Policy 53(2), 289–299 (2026). https://doi.org/10.1093/scipol/scag010
14. Sümer, B., Elbi, A.: Worldcoin's biometric proof of personhood: what is at stake for data protection? (Part 2). CiTiP Blog, KU Leuven, 8 November 2024. https://www.law.kuleuven.be/citip/blog/, last accessed 2026/08/04
15. Orsini, V.: Biometric data protection and state prerogatives: the Worldcoin case between GDPR and eIDAS 2. Eur. J. Privacy Law Technol., Special Issue (2024)
16. Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, 2025/0360(COD), 19 November 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0837
17. EDPB: Guidelines 01/2025 on Pseudonymisation. https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf, last accessed 2025/11/19
18. EDPB: Guidelines 02/2026 on Anonymisation – Version 1.0. https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf, last accessed 2026/07/31
19. European Commission: The Digital Travel Credential Manual, https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/930451772/Travel+Credentials last accessed 2026/08/04

20. ISO/IEC 2382-37:2022(En), Information Technology - Vocabulary - Part 37: Biometrics' <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:2382:-37:ed-3:v1:en> last accessed 2024/08/30
21. Biometric Update: Worldcoin pivots away from Europe amid tangle of GDPR problems, https://www.biometricupdate.com/202410/worldcoin-pivots-away-from-europe-amid-tangle-of-gdpr-problems, last accessed 2026/07/31
22. Biometric Update: Worldcoin rolls out in Guatemala, receives fine from Korea. https://www.biometricupdate.com/202409/worldcoin-rolls-out-in-guatemala-receives-fine-from-korea, last accessed 2026/07/31
23. World website, https://world.org/blog/announcements/world-implements-personal-custody last accessed 2026/07/31
24. World website, https://world.org/blog/engineering/introducing-ampc-another-leap-privacy-performance-world-id last accessed 2026/07/31
25. Dalla Corte, L.: Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. Eur. J. Law Technol. 10(1) (2019)
26. Zuiderveen Borgesius, F.: The Breyer case of the Court of Justice of the European Union: IP addresses and the personal data definition. Eur. Data Prot. Law Rev. 3(1), 130–137 (2017). https://doi.org/10.21552/edpl/2017/1/21
27. Cobbe, J.: A relative mess: identifying data subjects in multi-party processing. SSRN Electronic Journal (2025). https://doi.org/10.2139/ssrn.5731364
28. Sümer, B.: Personal data in EU digital wallets in light of the recent developments in EU data protection law. Preprint, 3rd Solid Symposium, London (2026). https://openreview.net/forum?id=RQCumKaavP
29. Purtova, N.: The law of everything: broad concept of personal data and overstretched scope of EU data protection law. Law Innov. Technol. 10(1), 40–81(2018). https://doi.org/10.1080/17579961.2018.1452176
30. Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, Judgment of the Court (Second Chamber) of 19 October 2016, ECLI:EU:C:2016:779
31. Case C-319/22, Gesamtverband Autoteile-Handel eV v Scania CV AB, Judgment of the Court (Third Chamber) of 9 November 2023, ECLI:EU:C:2023:837
32. Case C-413/23 P, European Data Protection Supervisor v Single Resolution Board, Judgment of the Court (Grand Chamber) of 4 September 2025, ECLI:EU:C:2025:645
33. European Union Agency for Cybersecurity (ENISA): Pseudonymisation techniques and best practices: recommendations on shaping technology according to data protection and privacy provisions. ENISA, Athens (2019). https://doi.org/10.2824/247711
34. Agencia Española de Protección de Datos (AEPD), European Data Protection Supervisor (EDPS): Introduction to the hash function as a personal data pseudonymisation technique (2019). https://www.edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, last accessed 2026/08/04
35. Silence Laboratories website, https://silencelaboratories.com/blog/a-discussion-on-collusion-resistant-protocols-in-secret-sharing, last accessed 2026/07/31
36. European Data Protection Board, European Data Protection Supervisor: EDPB–EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus). Adopted 10 February 2026 (2026)
37. Council of the European Union: Presidency compromise text, Digital Omnibus, Interinstitutional File 2025/0360(COD), Council document 9547/26, 21 May 2026
38. Erdogan, I., et al.: 'White Paper on the Digital Omnibus Proposal and the AI Omnibus Proposal' (Social Science Research Network, 13 March 2026) https://papers.ssrn.com/abstract=6409138

39. Datailsynet: Securing Digital Identities: Biometric data and protected templates in eID solutions - Exit report from the “SALT” sandbox project with Mobai. https://www.datatilsynet.no/contentassets/fad759b2486c41bf88dd58d8743a3a7a/salt-exit-report.pdf last accessed 31 July 2026.
40. Sümer, B.: The AI Act's exclusion of biometric verification: minimal risk by design and default? Eur. Data Prot. Law Rev. 10(2), 150–161 (2024). https://doi.org/10.21552/edpl/2024/2/6
41. Renieris, E.M.: Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse. MIT Press, Cambridge (2023)
42. World website, https://world.org/blog/foundational-topics/thesimpleplan, last accessed 2026/07/31