TFH

WORLDCOIN
Contributor Company

COMUNICACÃO ELETRÔNICA
VERSÃO PÚBLICA

22 de novembro de 2024

Prezado Sr. De Lima,

Escrevemos em resposta ao seu e-mail de 12 de novembro de 2024. A presente deve ser considerada uma resposta em conjunto da Worldcoin Foundation e da Tools for Humanity Corporation. A relação entre essas duas pessoas jurídicas está descrita no Apêndice na seção 1.

Inicialmente, gostaríamos de notar que a correspondência foi endereçada à Sra. Carvalhido. No futuro, gostaríamos de solicitar que todas as correspondências fossem endereçadas aos nossos Diretor de Privacidade [*Chief Privacy Officer*] e Diretor de Proteção de Dados [*Data Protection Officer*], responsáveis por essas questões. Como observado durante a nossa reunião realizada nesta semana, eles poderão ser contatados via e-mail, no endereço dpo@toolsforhumanity.com, disponível para que as Autoridades de Proteção de Dados possam ser corresponder diretamente com as equipes de Privacidade e Proteção de Dados da Tools for Humanity.

Conforme solicitado em seu e-mail, em anexo como o **Anexo A**, encontra-se uma cópia do respectivo Relatório de Impacto à Proteção de Dados (RIPD) em relação ao tratamento de dados do Orb, como o **Anexo B** o RIPD em relação à verificação da íris singular ambas contendo também o trecho relevante dos Registros de Atividades de Processamento (ROPA). Note-se que todos os anexos e apêndices são apresentados nas suas versões originais. Nossos RIPDs são preparadas com o intuito de atender os princípios geralmente aceitos para os RIPDs independentemente da legislação aplicável de proteção de dados, visando assegurar uma avaliação igualitária e prática dos produtos e serviços em caráter global, tendo em vista a natureza global do projeto da Worldcoin.

Na hipótese de qualquer dúvida sobre os RIPDs apresentadas, não hesite em nos contatar.

Separadamente, em anexo como o **Apêndice 1**, suas perguntas foram detalhadamente respondidas.

Ademais, segue uma cópia cortesia desta resposta em português.

Permanecemos à disposição de V.Sas. para qualquer dúvida adicional.

Atenciosamente,

Damien Kieran
Diretor Jurídico [Chief Legal Officer]
Tools for Humanity

Apêndice 1

1.1 Indicar as etapas necessárias do tratamento de dados pessoais para a consecução do protocolo World ID, especificando os agentes de tratamento responsáveis em cada operação.

Para responder esta pergunta, é importante ter uma boa compreensão de como um World ID é criado e distinguir a situação atual e a situação futura, a qual é esperada até o término do ano. Por conseguinte, descrevemos a seguir as etapas necessárias para a criação de um World ID e um comparativo entre a situação atual e a situação futura no que diz respeito a quem é o controlador dos dados.

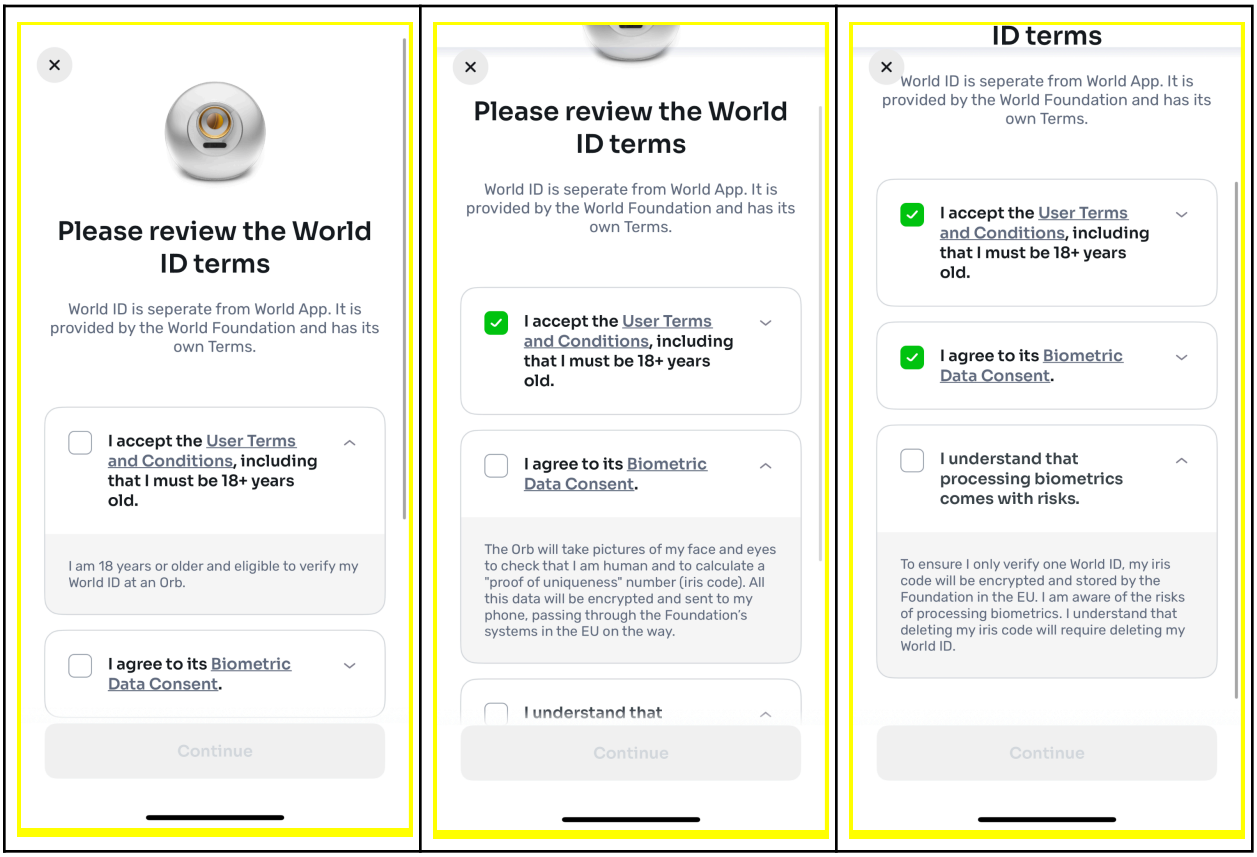
Situação Atual

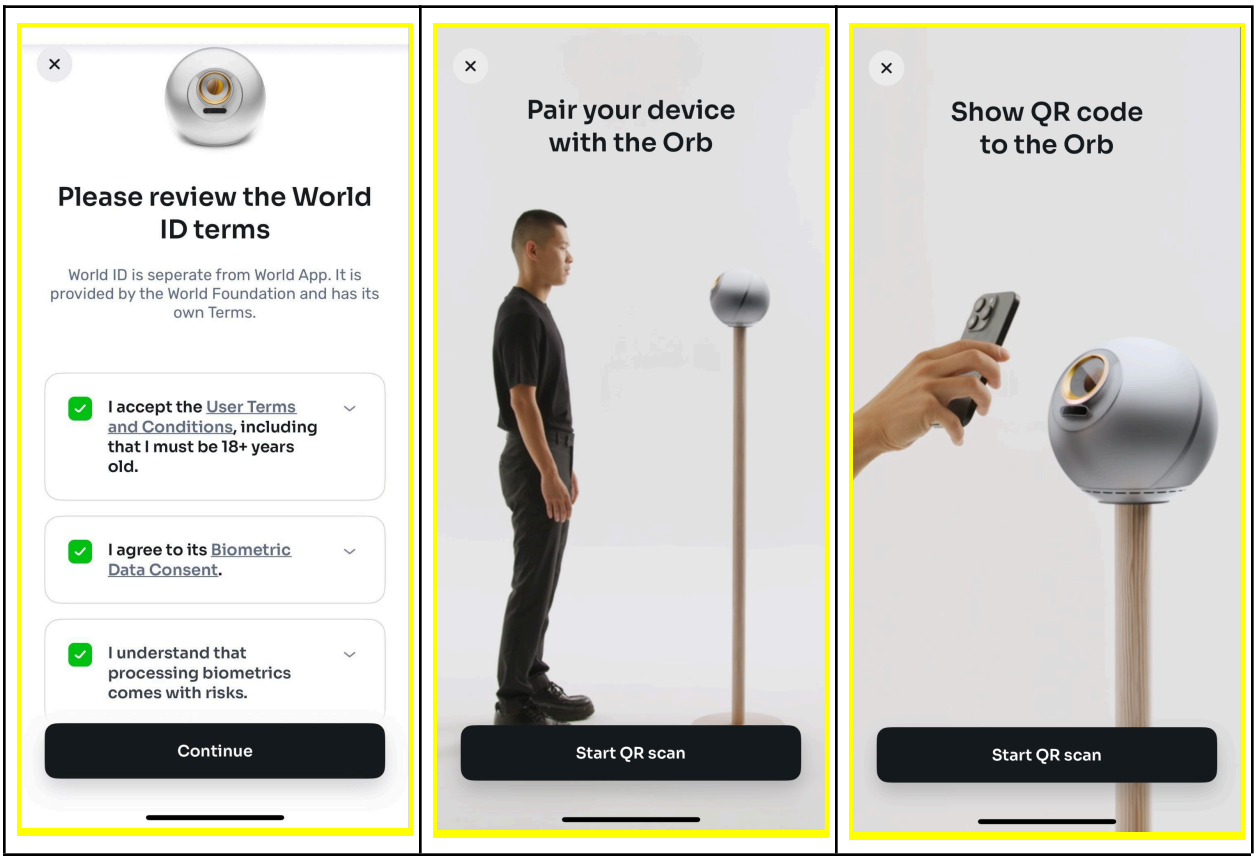
Atualmente, a World Foundation ("Foundation") é a controladora dos dados pessoais utilizados para a disponibilização do World ID às pessoas. A Foundation é uma organização sem fins lucrativos sediada nas Ilhas Cayman. A Foundation utiliza um prestador de serviços e operador, a Tools for Humanity (TFH), uma sociedade norte-americana.

A TFH é responsável pela fabricação da câmera avançada (i.e., o Orb) utilizada para a verificação de humanos únicos na rede de World ID, pela operação da infraestrutura de computação em nuvem para a disponibilização das verificações de World ID e pela disponibilização física das câmeras avançadas a humanos, seja diretamente nos locais físicos da parte principal ou por empresas terceirizadas (i.e., operadores) e parcerias.

Atualmente, quando um titular de dados for criar um World ID, o titular de dados irá primeiramente efetuar o download de um aplicativo chamado World App. O World App é um aplicativo desenvolvido e operado pela TFH. A TFH é a controladora do World App. O World App não se confunde com o World ID. O World ID pode ser melhor descrito como um número secreto ("Número Secreto") que é armazenado somente no dispositivo do titular de dados. Esse número pode ser utilizado por meio de uma prova de conhecimento zero [*zero knowledge proof*] para certificar que o World ID é parte da lista de World IDs verificados, sem revelar o Número Secreto ("Prova de World ID"). O World App não é necessário para essa Prova de World ID. No futuro, espera-se que possam existir vários aplicativos, nos quais um titular de dados possa manter ou armazenar o seu World ID. O World App é simplesmente o primeiro desses aplicativos.

Ao efetuar o download do World App, não é necessário que o titular de dados forneça qualquer dado pessoal. O titular de dados pode opcionalmente fornecer um número de telefone para que possa encontrar pessoas que conheça na rede. Entretanto, qualquer dado compartilhado com o World App ou por meio do World App é assim compartilhado com a TFH, na capacidade de controladora e em conformidade com a Declaração de Privacidade da TFH, em anexo como o **Anexo D**. As telas iniciais do World App são apresentadas a seguir.





Atualmente, todas as etapas a seguir de tratamento de dados são conduzidas pela TFH na capacidade de operadora para a controladora, a Foundation.

Um titular de dados que pretenda verificar o seu World ID deverá estar próximo à câmera avançada, o Orb. No World App, o titular de dados indica se está próximo ao Orb, e um código QR é exibido em seu dispositivo. Em seguida, o titular de dados mostra o código QR ao Orb, que inicia uma interação entre o dispositivo do titular de dados e o Orb. O dispositivo do titular de dados irá prosseguir com as etapas de verificação. Primeiramente, o titular de dados receberá o consentimento apropriado buscando assegurar que o titular de dados esteja suficiente informado e concorde com a coleta inicial de dados. As telas do World App explicam quais tipos de dados pessoais serão coletados, que serão somente armazenados no dispositivo do titular de dados e que, após a verificação, os dados serão anonimizados. Essas telas são demonstradas a seguir.

O Orb tira fotos da face e olhos dos titulares de dados. Essas fotos permanecem no Orb. O Orb hospeda diversas redes neurais destinadas a determinar se o titular de dados é humano e se está vivo, o que é realizado por meio da análise das imagens coletadas. O objetivo é assegurar que alguém não está tentando enganar/fraudar o Orb apresentando, por exemplo, uma tela ou fotografia de alta resolução.

Se o Orb determinar que as fotos são de um humano que está vivo, o Orb, sem que nenhum dado seja transferido do dispositivo, examinará as fotos dos olhos do titular de dados e criará uma abstração no formato de um código de íris. O código de íris é um código binário representando as características da foto do olho. Em seguida, o Orb irá garantir que o código de íris seja único (i.e., que um código de íris similar não tenha sido anteriormente verificado), o que é realizado comparando-se o código de íris aos conjuntos de dados anonimizados representando humanos anteriormente verificados. A comparação efetivamente devolve o equivalente técnico a um sim ou não quanto à existência do código de íris nos códigos de íris anteriormente anonimizados, mas não identifica nem divulga o código de íris, o qual permanece anonimizado.

Se o código de íris tiver sido anteriormente apresentado, o processo não poderá prosseguir tendo em vista que o titular de dados já criou um World ID.

Se o código de íris não tiver sido anteriormente apresentado, o processo poderá prosseguir. O Orb irá então anonimizar os dados, empregando uma Tecnologia para Aprimoramento de Privacidade (*Privacy Enhancing Technology* - "PET"), conhecida como Secure Multi-Party Computation ("SMPC"). Na instanciação inicial da SMPC, o código de íris foi processado em dois fragmentos separados de SMPC, cada um dos quais individualmente incapaz (i.e., segurança da computação quântica) de ser novamente associado ao código de íris e, a partir de então, cada fragmento foi armazenado em bases de dados separadas (i.e., nodes), um detido e operado pela Foundation e um pela TFH. Esse processo está em fase de mudança (i.e., Situação Futura, conforme discutido a seguir) e resultará que a Foundation não será mais controladora com relação a qualquer aspecto do fornecimento do World ID.

Assim que os fragmentos de SMPC são armazenados, o Orb tira fotos do titular de dados, todas as abstrações das fotos, incluindo o código de íris, e alguns metadados, criptografa esses dados em um pacote conhecido como Pacote de Custódia Pessoal (*Personal Custody Package* - "PCP"), e transfere esse pacote com segurança ao dispositivo móvel do titular de dados. O titular de dados pode realizar o back-up do PCP em sua própria nuvem pessoal, para a sua segurança.

Todos os dados pessoais são excluídos do Orb assim que o PCP é enviado ao dispositivo do usuário. O Orb não armazena dados pessoais.

Do início ao fim, o processo de verificação dura menos do que dez segundos. Após esses dez segundos nenhum dado pessoal decorrente da verificação é armazenado pela TFH ou pela Foundation.

Nesse momento, o World ID está integralmente criado e pode ser utilizado pela pessoa física para demonstrar com segurança e anonimamente que é um humano único para os serviços que possa utilizar.

Durante o uso do World ID, nenhum dado pessoal é tratado por qualquer parte. Pelo contrário, o indivíduo mantém e controla todos os seus dados pessoais, e, com o emprego de outra PET conhecida como Zero Knowledge Proofs ("ZKP"), o indivíduo conseguirá provar, em caráter anônimo e indubitável,

às partes on-line que é um humano único, substituindo elementos como CAPTCHAs, que já podem ser derrotados por IA, e até mesmo mecanismos de single sign on, permitindo uma maneira anônima e segura de entrar em um sistema.

Situação Futura

Conforme anunciado em 17 de outubro de 2024, a Foundation e a TFH estão finalizando o desenvolvimento da Anonymizing Multi-Party Computation ("AMPC"), uma evolução da SMPC. As etapas para a criação de um World ID permanecerão conforme descrito acima. **[RESTRITO]** Todos os fragmentos anonimizados serão armazenados em nodes operados por terceiros de confiança, incluindo Universidades e firmas independentes de auditoria de TI. Os primeiros terceiros que irão operar essas bases de dados são a University of Berkeley, a Friedrich-Alexander University em Nuremberg e a firma de auditoria de TI Nethermind. Esperamos que os nodes sejam operados por vários outros terceiros de confiança no futuro. Para evitar dúvidas, nenhum destes operadores de confiança armazena quaisquer dados pessoais, incluindo o código da íris, e os dados anónimos que armazenam individualmente não podem ser relacionados com uma pessoa.

[RESTRITO]

1.2 Por que o agente quer tratar os dados pessoais?

O projeto World tem por missão construir ferramentas que habilitem humanos em um mundo de IA, construindo, portanto, a maior rede mundial de humanos apta a gerar segurança digital e inclusão financeira.

O rápido avanço da IA irá trazer diversos benefícios, mas sem as ferramentas apropriadas que habilitem a navegação por humanos em um mundo impulsionado pela IA, vários desafios poderão surgir. Por exemplo, já atualmente, em um mundo pré-IA, estamos já lutando para confiar nas interações on-line. Exemplificado pela manipulação e desinformação no X (i.e. Twitter) que são alimentadas por agentes autônomos (bots) e deepfakes, podemos observar porque é indispensável saber se estamos interagindo com um humano real, responsável pelos seus atos. Na medida em que a IA se torne onipresente, mais inteligente e apta a devidamente imitar um humano, será ainda mais difícil distinguir humanos e computadores. De fato, hoje os CAPTCHAs já podem ser derrotados pela IA e, portanto, todos os meios conhecidos existentes para distinguir humanos de computadores estão falhando.[1]

Portanto, assegurar que existam as ferramentas apropriadas para habilitar os humanos a prosperar na IA é fundamental, tanto para desbloquear o valor da IA quanto para garantir a segurança e proteção dos

---

1 https://arstechnica.com/ai/2024/09/ai-defeats-traffic-image-captcha-in-another-triumph-of-machine-over-man/

humanos. Aqui o tratamento temporal dos dados pessoais (i.e., em menos do que 10 segundos, dados pessoais são coletados, tratados e armazenados) é necessário para assegurar que seja possível anonimamente distinguir humanos dos computadores em interações digitais (i.e., qualquer interação digital, incluindo a criação ou consumo de conteúdo, mensagens de texto, ligações telefônicas, compra ou venda de bens ou serviços etc.).

1.3 Que benefício o agente pretende obter com o tratamento de dados pessoais?

Acreditamos que com a construção de uma rede descentralizada (i.e., que não seja detida ou operada por uma única entidade e, por conseguinte, não esteja sujeita a pontos de falha ou exploração singulares) de humanos únicos, anônimos e verificáveis, uma utilidade para a segurança digital em um mundo de IA no qual negócios, entretenimento e outros possam florescer, pode ser criada. Acreditamos que os benefícios diretos poderão ser vários e irão evoluir ao longo do tempo. A médio prazo, esperamos, por exemplo, que a TFH será um dos maiores fabricantes e fornecedores da câmera avançada, o Orb, necessária para as verificações ou que a TFH criará aplicativos que possam utilizar o protocolo para trazer serviços significativos a humanos únicos verificados.

1.4 Algum terceiro se beneficiará com o tratamento de dados pessoais?

Sim, acreditamos que muitos terceiros serão beneficiados.

1.5 Destaque os benefícios identificados com o tratamento de dados pessoais para os titulares afetados?

Abaixo estão alguns dos benefícios e beneficiários:

- humanos verificados se beneficiarão, estando aptos a se distinguirem dos computadores com certeza;
- humanos com interação com humanos verificados se beneficiarão tendo em vista que terão um meio fácil de alta segurança para determinar se alguém com quem estejam interagindo é de fato um humano único (e.g., resolvendo problemas, tais como bots na plataforma, ou serviços de relacionamento on-line);
- governos podem se aproveitar da natureza anônima do World para assegurar que seus cidadãos não comprometam os seus dados pessoais on-line (i.e., a maioria dos serviços on-line não precisa de nível elevado de KYC, mas, pelo contrário, exige poucos sinais de elevada segurança para permitir o seu uso), compartilhando dados pessoais granulares com serviços on-line quando não forem necessários;
- governos poderiam se aproveitar do World ID para reduzir fraude dos sistemas, como previdência social, benefícios ou votação) se estiverem aptos a anonimamente garantir a um humano único um pacote de benefícios ou um voto;

- serviços on-line ou digitais poderiam minimizar a sua necessidade de coleta de dados pessoais tendo em vista que a maioria dos serviços on-line não precisa saber quem você é, resolvendo, assim, várias preocupações atuais de KYC;
- serviços on-line ou digitais podem cessar fraudes e ataques aos seus sistemas, com a coordenação dos sistemas (i.e., bots que atacam redes sociais, ou jogos);
- serviços on-line ou digitais podem cessar a disseminação de informações incorretas e desinformação por computador ou IA com a coordenação de *bad actors*;
- entes sem fins lucrativos e esforços humanitários podem se beneficiar da natureza inclusiva do World ID para assegurar que mesmo comunidades remotas e desprivilegiadas possam ser incluídas em novas tecnologias ou recebam assistência e benefícios de maneira justa e equitativa; e
- habilitar operações financeiras inclusivas entre todos os humanos únicos verificados na terra.

1.6 De que maneira o tratamento de dados ajudará o controlador a atingir a finalidade pretendida?

Ao ser capaz de temporariamente tratar dados pessoais para determinar que um titular de dados é um humano único, e então anonimizar os dados relevantes, o controlador pode criar uma rede de humanos anônimos e verificáveis, com elevada segurança e inclusiva, que pode ajudar a distinguir se alguém com quem estamos interagindo digitalmente é um humano ou um computador. Em outras palavras, atualmente não há método técnico alternativo para atingir o mesmo objetivo de forma que possa ser escalonado exponencialmente, que seja tão inclusivo e anônimo quanto o tratamento de dados envolvidos no World ID.

1.7 De que maneira o tratamento de dados é proporcional?

Consulte os RIPDs anexados no **Anexo A** e **Anexo B** para uma análise detalhada. No entanto, tendo em vista que dados pessoais são somente temporariamente coletados e tratados, com consentimento completo e informado do titular de dados, e então devolvidos ao titular de dados para que o titular de dados – e somente ele – possa controlar e supervisionar os seus dados pessoais, o fato que quaisquer dados mantidos sejam anonimizados em meios de segurança da computação quântica e armazenados em meios descentralizados seguros, o tratamento muito limitado é proporcional face aos benefícios apresentados pelo tratamento, aos danos limitados que possam ocorrer aos dados pessoais mesmo se todas as salvaguardas falharem e, particularmente, em comparação aos riscos muito maiores apresentados pela IA se não formos capazes de distinguir humanos dos computadores, de maneira confiável e em escala.

1.8 O controlador poderá atingir o objetivo do protocolo World ID sem o tratamento dos dados pessoais que pretende coletar?

Não, não seria possível. Foi conduzida uma análise detalhada. Consulte, por exemplo, o White Paper em anexo como o **Anexo E** nos termos da seção "solving PoH at scale". Está claro que em um mundo de IA, tudo que é extrínseco ao corpo humano (incluindo o exterior do corpo humano) poderá ser replicado (i.e., fraude) por IA. Por exemplo, atualmente, as identidades governamentais podem ser compradas e vendidas, não são inclusivas tendo em vista que a maioria das pessoas não possui uma identidade governamental, não comprovam a humanidade, mas meramente comprovam o acesso a um documento. Da mesma forma, o reconhecimento facial não é efetivo uma vez que a IA pode criar um deep fake de uma face humana e, assim, retratar-se como um humano. Portanto, é imperativo o uso de biometria intrínseca relacionada a dados para resolver o problema de distinção entre um humano e a IA. Ademais, a solução desse problema será crítica para a sobrevivência da humanidade em um mundo de IA. É também importante lembrar que nenhum dado pessoal é mantido ou armazenado para habilitar o World ID.

1.9 O controlador poderá atingir o mesmo objetivo tratando uma quantidade menor de dados pessoais?

Não, não seria possível. Ademais, a quantidade de dados pessoais tratados é mínima. Conforme discutido na resposta à Pergunta 1.1 acima, os dados pessoais são temporariamente coletados e tratados, devolvidos ao titular de dados e excluídos. Os únicos dados mantidos são dados anonimizados. Ademais, não há meios alternativos que produzam os mesmos resultados. Por exemplo, a utilização de identidades governamentais resultaria na coleta de identificadores associados a um humano, que não são resistentes a fraudes por IA, podem ser adquiridos ou replicados e não são inclusivos. De fato, a solução desse problema exige o uso de dados biométricos e, portanto, a importante necessidade de garantir a anonimização dos dados mantidos.

2.1 Qual a data em que foi iniciada a coleta de dados pessoais (caso não tenha iniciado a operação, indicar a data pretendida para o início)?

No Brasil, o tratamento dos dados se iniciou em 12 de novembro de 2024.

Sobre os dados pessoais coletados:

2.2.1 Qual a fonte dos dados pessoais coletados para a criação de uma World ID.

Consulte a Pergunta 1.1 acima, para uma resposta detalhada. A fonte dos dados pessoais coletados para a criação de um World ID é diretamente do titular de dados, o qual deverá prestar os dados por conta própria.

2.2.2 Quais os tipos de dados (nome, endereço, telefone, conta bancária, números de registro oficial etc.) coletados para cada etapa de tratamento?

Consulte a Pergunta 1.1 acima, para uma resposta detalhada. Os tipos de dados coletados para a criação de um World ID são fotos da face e olhos do titular de dados.

2.2.3 Qual o formato desses dados (imagem, texto, áudio etc.)?

Consulte a Pergunta 1.1 acima, para uma resposta detalhada. Os únicos dados pessoais coletados do titular de dados são fotos de alta resolução.

2.2.4 O titular recebe algum tipo de compensação pela coleta de seus dados pessoais?

Não. O titular de dados não recebe nenhuma compensação pelos seus dados pessoais. De fato, nenhum dado pessoal originado das verificações do Orb é mantido pela TFH ou pela Foundation. Um titular de dados que cria um World ID pode, opcionalmente, solicitar uma concessão de Worldcoin (WLD). Isso não é obrigatório. O WLD é uma criptomoeda que dá suporte à rede World ID, opera como um mecanismo de inicialização das redes e, eventualmente, permitirá transações na rede mundial. Se uma pessoa reivindicar seu WLD, ela não poderá convertê-lo ou transferi-lo da rede para moeda fiduciária por um período mínimo de 24 horas.

2.2.5 O controlador poderá atingir o objetivo do protocolo World ID sem o tratamento dos dados pessoais que pretende coletar, inclusive biométricos?

Não. Consulte as respostas às Perguntas 1.9 e 2.1 acima.

2.2.6 O protocolo World ID utiliza ferramentas de inteligência artificial no tratamento dos dados pessoais coletados? Caso afirmativo, descreva de forma detalhada a utilização de inteligência artificial, indicando as ferramentas tecnológicas necessárias para isso.

O Orb executa diversas redes neurais simultaneamente em tempo real, para validar a humanidade (i.e., avaliar se fotos de alta resolução retratam um humano de fato vivo). Um panorama detalhado de como as redes neurais são empregadas pelo Orb pode ser encontrado no whitepaper, em anexo como o **Anexo E** nos termos da seção "why custom hardware is needed".

2.2.7 O controlador compartilha com terceiras partes os dados pessoais coletados dos titulares, inclusive dados biométricos?

Não. Consulte a Pergunta 1.1 acima. Durante a criação de um World ID, nenhum dado pessoal é mantido após a verificação e, dessa forma, nenhum dado pessoal é compartilhado com terceiros.

Durante o processo de verificação através do Orb, que demora menos de dez segundos, é necessário verificar se a pessoa que se apresenta para verificação já possui uma conta World ID. Para isso, o código da íris é enviado temporariamente para as partes de confiança do SMPC (conforme descrito acima; Estado atual: TFH e Worldcoin Europe. Estado futuro: universidades, organizações sem fins lucrativos e terceiros confiáveis). O código da íris é criptografado em trânsito e, quando chega às partes do SMPC, é armazenado na RAM por alguns segundos, onde é feita uma comparação usando matemática computacional e criptografia de última geração para determinar se o sujeito dos dados criou anteriormente um World ID. Se a pessoa previamente tiver criado uma World ID, não pode criar uma nova e, se não tiver criado uma World ID, pode prosseguir. Em ambos os casos, o código da íris momentaneamente armazenado na memória RAM é imediatamente apagado e nenhum dado pessoal é retido por nenhuma das partes, incluindo as partes do SMPC.

Em caso afirmativo, indicar:

2.2.7.1 Os agentes de tratamento com os quais compartilha os dados dos titulares.

Consulte a Pergunta 2.2.7 acima.

2.2.7.2 Quais dados pessoais são compartilhados com terceiros.

Consulte a Pergunta 2.2.7 acima.

2.2.7.3 As finalidades do compartilhamento.

Consulte a Pergunta 2.2.7 acima.

2.2.7.4 A hipótese legal que fundamenta o compartilhamento.

Consulte a Pergunta 2.2.7 acima.

2.2.7.5 De que maneira os titulares são informados quanto ao compartilhamento de seus dados pessoais com terceiros e quais informações são prestadas a ele.

Essas informações são divulgadas no Aviso de Privacidade aplicável, na seção "8. Quando compartilhamos seus dados" e no Formulário de Consentimento da Fundação, na seção "4. Com quem compartilhamos os dados".

2.3 Quais as finalidades específicas do tratamento de dados pessoais em cada etapa do protocolo World ID?

Consulte a Pergunta 1.1 acima. Dados pessoais são tratados para criar e fornecer ao titular de dados um World ID. Assim que o World ID é criado, nenhum dado pessoal originado da verificação do Orb é tratado no fornecimento do protocolo World ID. Separadamente, um titular de dados poderá prestar dados pessoais por meio do seu uso do World App, o qual não se confunde com o World ID.

2.3.1 Quais produtos e serviços estão contemplados em cada atividade de tratamento? Indicar explicitamente os que estão e os que não estão incluídos.

Consulte a Pergunta 1.1 e 2.3 acima. Na criação de um World ID, os únicos produtos ou serviços contemplados são a referida verificação de um World ID por meio do dispositivo de câmera avançada, denominado o Orb. Em seguida, um titular de dados poderá utilizar o seu World ID para provar a sua humanidade única, mas, ao fazê-lo, nenhum dado pessoal originado da verificação é tratado pelo protocolo World ID.

2.4 Qual o período de retenção dos dados pessoais coletados?

Consulte a Pergunta 1.1 acima. Dados pessoais são temporariamente coletados e armazenados no Orb para a condução do processo de verificação, o qual leva no máximo dez segundos. Durante esse processo, uma cópia criptografada dos dados pessoais é transferida ao dispositivo do titular de dados e os dados pessoais são excluídos do Orb e de todos os servidores (nos quais o código de íris foi brevemente tratado para a determinação de sua singularidade).

2.5 Qual a frequência de atualização dos dados pessoais dos usuários?

Consulte a Pergunta 1.1 acima. Os dados pessoais do titular de dados originados da verificação do Orb não são atualizados. No entanto, está previsto que, no futuro, para garantir o devido funcionamento dos recursos de segurança, com o FaceAuth, poderá ser necessário que o titular de dados devolva a um Orb e atualize as imagens de alta resolução de sua face e essas imagens atualizadas em seu PCP no seu dispositivo. Novamente, essas imagens, por opção padrão, não seriam mantidas por qualquer ente central ou base de dados.

2.5.1 Qual a frequência de atualização dos registros das operações de tratamento (ROT)?

Se e quando as operações de tratamento sofrerem uma mudança em decorrência de alterações às operações ou infraestrutura técnica, os registros de tratamento são atualizados de acordo. É importante ressaltar que esses registros não contêm dados pessoais, mas simplesmente a existência de operações de processamento.

2.5.2 Por quanto tempo são mantidos os históricos de tais registros?

Os registros de processamento são mantidos. Em seguida, são atualizados, conforme descrito na resposta à Pergunta 2.5.1, acima, quando são feitas alterações no processamento que exijam sua atualização.

2.6 Os dados pessoais coletados passam por procedimentos de pseudonimização ou anonimização?

Sim. Consulte a Pergunta 1.1 acima. Nenhum dado pessoal é armazenado no fornecimento do World ID. Os dados armazenados são anonimizados conforme descrito na resposta à Pergunta 1.1.

Em caso afirmativo:

2.6.1.1 Descrever tais procedimentos.

Conforme descrito em um anúncio recente[2], a AMPC é utilizada para anonimizar os dados mantidos no fornecimento do World ID. Publicamos um vídeo[3] com a arquitetura principal do sistema que ajuda a explicar da forma mais simples possível como o processamento criptográfico é conduzido para a anonimização dos dados. **[RESTRITO]**

2.6.1.2 Indicar em quais etapas do tratamento de dados pessoais isso ocorre.

A anonimização ocorre durante as etapas de verificação descritas na resposta à Pergunta 1.1 acima.

2.6.1.3 Indicar se foi realizada análise prévia quanto à eventual possibilidade de reidentificação dos titulares. Caso afirmativo, compartilhe os principais resultados da análise realizada.

[2] Ver https://world.org/blog/engineering/introducing-ampc-another-leap-privacy-performance-world-id
[3] Ver https://youtu.be/xQDXr8AZFGM?si=haRJHlcVVTA-EGSr

Sim, a empresa de auditoria de TI confiável e independente Least Authority foi contratada para realizar uma auditoria das partes relevantes do protocolo, e essa auditoria está disponível publicamente.[4]

2.6.1.4 Indicar se mantém um processo gerenciável de anonimização ou pseudominização.

Sim, consulte as respostas às Perguntas 1.1 e 2.6 acima.

2.6.2 Em caso negativo, justificar a não necessidade de anonimizar os dados pessoais.

Não aplicável. Consulte as respostas às Perguntas 1.1 e 2.6 acima.

3.1 Qual a hipótese legal utilizada para o tratamento em análise?

O consentimento é a hipótese legal utilizada para a coleta e tratamento dos dados no Orb durante a verificação e ainda para o processo de anonimização.

3.1.1 Especificar se há diferença de hipótese legal para cada etapa da atividade de tratamento.

Não aplicável. Consulte a resposta à Pergunta 3.1 acima.

3.2 Caso a operação de tratamento seja realizada com base no consentimento explícito do titular, indicar:
3.2.1 De que maneira o controlador assegurará que o consentimento do titular será obtido em conformidade com a LGPD.

Durante o processo de verificação, são apresentadas ao titular de dados telas claras buscando o seu consentimento específico para o tratamento dos dados, conforme demonstrado nas telas exibidas acima.

3.2.2 De que maneira o titular poderá revogar o seu consentimento.

O tratamento dos dados pessoais para o World ID é temporário (i.e., menos de 10 segundos) através do qual dados pessoais são coletados pelo Orb, tratados para verificação, anonimizados, sendo uma cópia dos dados pessoais criptografada e enviada ao titular de dados em seu dispositivo móvel, e todos os dados pessoais são excluídos do Orb, não sendo mantido nenhum dado pessoal. Portanto, um

[4] Ver https://leastauthority.com/blog/audits/audit-of-worldcoins-mpc-protocol/

mecanismo para revogar o consentimento não seria praticamente necessário, uma vez que o titular de dados poderia simplesmente interromper o processo de verificação a qualquer momento ou, após o processo de verificação, poderia excluir os seus dados pessoais do seu dispositivo móvel– cujos dados pessoais são mantidos somente pelo titular dos dados –é claro excluindo todos os dados do seu dispositivo cessaria a capacidade de uso pelo titular de dados do seu World ID. Adicionalmente, apesar de um mecanismo de revogação do seu consentimento não ser necessário pelos motivos expostos acima, mecanismos de suporte são disponibilizados aos titulares de dados caso possuam qualquer dúvida ou preocupação, inclusive relacionada a dados pessoais, cujos mecanismos são acessíveis diretamente no World App.

3.2.3 Em caso de exercício do direito de exclusão pelo titular, referir quais dados pessoais serão excluídos, indicando se o controlador se reserva o direito de manter algum dado pessoal anteriormente coletado sob a sua custódia.

Consulte a resposta à Pergunta 3.2.2. acima. O titular de dados poderá eliminar os seus dados pessoais do seu dispositivo móvel – cujos dados pessoais são mantidos somente pelo titular dos dados – a qualquer momento.

3.3 Os efeitos advindos do exercício do direito de revogação do consentimento pelo titular.

Consulte a resposta à Pergunta 3.2.2. acima. O titular de dados não conseguirá utilizar o seu World ID se os seus dados pessoais tiverem sido excluídos.

4.1 Indicar o nome e o canal de identificação do encarregado pelo tratamento de dados pessoais da controladora, bem como onde tais informações podem ser encontradas no sítio da empresa, conforme estabelecido pelo art. 9ª, §1º, da Resolução CD/ANPD nº 18/2024 ("Regulamento do Encarregado").

[RESTRITO]

4.2 Quais informações são prestadas aos titulares no momento da coleta de seus dados pessoais? De que forma essas informações são prestadas?

Conforme descrito na resposta à Pergunta 1.1 acima, ao criar um World ID, ao titular de dados são exibidas uma variedade de telas e informações de contratação no World App, incluindo os Termos de Serviço, a Declaração de Privacidade, os consentimentos necessários e informações adicionais. Todas essas informações têm por objetivo assegurar que o titular de dados compreenda quais dados pessoais estão sendo coletados e como os dados pessoais são tratados.

4.3 Indicar se o controlador disponibilizou aos titulares informações claras e atualizadas sobre:

4.3.1 A hipótese legal do tratamento.
4.3.2 A finalidade do tratamento.
4.3.3 Os procedimentos de coleta dos dados.
4.3.4 As práticas utilizadas para o tratamento de dados.
4.3.5 Os mecanismos para o exercício dos direitos previstos no art. 18 da LGPD.

Sim. **[RESTRITO]** No entanto, vale notar, conforme discutido acima na respostas acima, que, tendo em vista que os dados pessoais não são retidos para o fornecimento do World ID, a necessidade de satisfazer determinados direitos é negada (i.e., por exemplo, se nenhum dado pessoal é mantido ou armazenado, seria impossível disponibilizar um meio para a atualização dos referidos dados). Contudo, por abundância de zelo e caução, são disponibilizados mecanismos para assegurar que os titulares de dados possam contatar o suporte ou o Escritório de Proteção de Dados para que suas dúvidas ou preocupações possam ser respondidas.

5.1 Indicar os direitos à disposição dos titulares para cada etapa do tratamento de dados pessoais para a criação do World ID.

5.2 Sobre os direitos previstos no art. 18 da LGPD:

5.2.1 Quais os mecanismos para que os usuários do protocolo World ID possam exercer esses direitos? Detalhe o passo-a-passo para esse exercício.

Conforme descrito na resposta às Perguntas 1.1 e 2.6-3.1 acima, tendo em vista a natureza da operação do protocolo World ID, vários direitos que um titular de dados poderia exercer não são aplicáveis na medida em que os dados são anonimizados. O uso de PETs e anonimização significa que nenhum dado pessoal está sendo armazenado ou tratado acerca do qual os direitos do Art. 18 seriam aplicáveis. No entanto, descrevemos a seguir com maior detalhamento como isso se aplica a cada direito.

- Confirmação da existência de tratamento: Após a verificação, nenhum dado pessoal originado da verificação pelo Orb é tratado para o protocolo World ID. Somente o titular de dados mantém os seus dados pessoais. No entanto, um titular de dados poderá entrar em contato com o Escritório da Equipe de Privacidade para confirmar a existência de tratamento dos seus dados pessoais e receberá uma resposta baseada na sua dúvida explicando que nenhum dado pessoal está sendo tratado.

- Acesso aos dados: Após a verificação, nenhum dado pessoal originado da verificação pelo Orb é tratado para o protocolo World ID. Somente o titular de dados mantém os seus dados pessoais. Portanto, o titular de dados tem acesso aos seus dados pessoais e nenhum acesso adicional aos dados pessoais poderá ser disponibilizado.

- Correção de dados incompletos, inexatos ou desatualizados: Após a verificação, nenhum dado pessoal originado da verificação pelo Orb é tratado para o protocolo World ID. Somente o titular de dados mantém os seus dados pessoais. Portanto, não é necessário disponibilizar um mecanismo para a correção de dados incompletos, inexatos ou desatualizados. Conforme observado na resposta à Pergunta 2.5 acima, periodicamente no futuro, para habilitar os recursos de segurança, como o FaceAuth, poderá ser necessário que o titular de dados devolva ao Orb uma atualização das imagens de alta resolução mantidas em seu PCP.

- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei: Após a verificação, nenhum dado pessoal originado da verificação pelo Orb é tratado para o protocolo World ID. Somente o titular de dados mantém os seus dados pessoais. Qualquer dado mantido é anonimizado.

- Portabilidade dos dados a outro serviço: Após a verificação, nenhum dado pessoal originado da verificação pelo Orb é tratado para o protocolo World ID. Somente o titular de dados mantém os seus dados pessoais. Consequentemente, não há dados pessoais remanescentes que poderiam ser objeto de portabilidade a outro serviço. O titular de dados já possui uma cópia dos seus dados pessoais.

- Eliminação dos dados pessoais tratados com consentimento: Consulte as respostas às Perguntas 2.6 e 3.1 acima. Aparentemente as perguntas aqui estão duplicadas.

- Informações sobre operadores: As informações sobre operadores estão previstas na respectiva declaração de privacidade. Ademais, um titular de dados poderá entrar em contato com o Escritório da Equipe de Privacidade para as suas dúvidas, tais como as que digam respeito aos operadores e receberá uma resposta baseada na sua dúvida.

- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa: Durante a verificação, os titulares de dados são informados que a verificação não poderá prosseguir sem a coleta dos dados pessoais em questão. Tendo em vista que a coleta se baseia na hipótese legal de consentimento, se o consentimento não for manifestado, o titular de dados não conseguirá prosseguir com a verificação.

- Revogação do consentimento: Consulte as respostas às Perguntas 2.6 e 3.1 acima. Aparentemente as perguntas aqui estão duplicadas.

5.3 Especificamente sobre o direito à revogação do consentimento:

5.3.1 Explicar o passo-a-passo sobre como pode ser exercido por usuários.

Consulte a resposta à Pergunta 5.1. acima.

5.3.2 Há alguma hipótese em que o pedido de revogação do titular seja negado? Caso o tratamento desse pedido seja automatizado, como funciona a instância revisora?

Conforme observado na resposta à Pergunta 2.6 acima, não há mecanismo para a revogação de consentimento tendo em vista que, após a verificação, nenhum dado pessoal é armazenado ou tratado. Pelo contrário, o titular de dados mantém os seus dados pessoais, podendo ser livremente eliminados a qualquer momento. De fato tal mecanismo seria inútil sob as circunstâncias e, consequentemente, negamos a necessidade de mecanismo de revogação de consentimento.

5.3.3 A controladora impõe condições para o exercício de revogação do consentimento? Nesse caso, quais seriam as consequências advindas ao titular?

Consulte as respostas às Perguntas 2.6 e 3.1 acima. Conforme observado em diversos pontos, tendo em vista a operação do World ID e que nenhum dado pessoal originado da verificação pelo Orb é mantido, um mecanismo para a revogação do consentimento não seria útil. No entanto, o titular de dados poderá eliminar os seus dados pessoais no seu dispositivo móvel – cujos dados pessoais são mantidos somente pelo titular dos dados – o que seria funcionalmente equivalente à revogação do consentimento para o tratamento de quaisquer dados pessoais. Caso o faça, isso resultaria na sua incapacidade de operar ou usar o seu World ID.

6.1 Houve estudos/análise para verificar o risco de danos aos direitos à privacidade e à proteção de dados pessoais aos titulares? Em caso afirmativo, informar:

Conforme observado na página de cobertura e na resposta à Pergunta 1.7 acima, RIPDs foram realizados e são apresentados. O RIPD para o tratamento de dados relacionados ao Orb buscar avaliar os riscos aos direitos e liberdades dos titulares de dados. Os RIPDs se encontram em anexo como o **Anexo A e Anexo B**.

6.1.1.1 se foram considerados, de maneira especial, a eventual coleta de dados biométricos de grupos vulneráveis,

Os RIPDs, em consonância com as melhores práticas, buscam considerar os riscos de todos os indivíduos, incluindo, a título exemplificativo, menores. Consulte, por exemplo, a RIPD sobre o Tratamento no Orb em anexo como o **Anexo A**.

6.1.1.2 se foi considerado, de maneira específica, a coleta de dados pessoais no contexto brasileiro.

Tendo em vista a natureza dos dados pessoais biométricos temporariamente coletados e tratados para permitir a verificação do World ID e que são amplamente considerados sensíveis do ponto de vista legal ou social, especial atenção foi dada a tais dados. No entanto, isso não foi feito no contexto de um país sobre outros. O projeto World ID busca assegurar que todos os humanos, independentemente de sua localização, possam verificar de maneira anônima sua humanidade única. Para a consecução de tal objetivo, todos os humanos, independentemente de sua localização geográfica, deverão receber o mais alto nível de proteção à privacidade e consideração. Consequentemente, nenhuma diferença técnica (i.e. segurança de dados) na avaliação foi apontada com base no caráter geográfico.

6.1.1.3 se foram avaliados especificamente os riscos de acesso indevido aos dados biométricos dos titulares.

Sim. Foi dada consideração específica ao acesso indevido aos dados pessoais, como pode ser visto nos RIPDs em anexo como o **Anexo A e Anexo B.** De fato, a razão para a adoção da SMPC para a anonimização e proteção de dados foi prevenir a materialização de tais riscos.

6.1.1.4 os protocolos estabelecidos para mitigar eventuais prejuízos advindos do tratamento de dados biométricos.

Conforme descrito acima, as medidas para mitigar eventuais prejuízos ou riscos relativos ao tratamento podem ser vistas nas avaliações realizadas nas RIPDs. A RIPD se encontra em anexo como o **Anexo A e Anexo B**.

6.1.2 Caso os referidos estudos/análises não tenham sido produzidos, indicar os motivos pelos quais o controlador entendeu pela sua desnecessidade.

Não aplicável. Consulte as respostas à Pergunta 6.1 acima.

6.2 Qual a periodicidade de reavaliação dos estudos/análises indicados no item 6.1?

Na medida em que o protocolo, segurança, dados envolvidos ou outras matérias sofram qualquer atualização, alteração ou avanços, os RIPDs são revisados e alterados de acordo.

7.1 Há coleta de dados pessoais de usuários menores 18 (dezoito) anos para a criação do World ID?

Não. Atualmente, é proibida a criação de um World ID por titular de dados menor de 18 anos. No entanto, antecipamos que no futuro menores de 18 anos poderão se beneficiar do uso do World ID, por

exemplo, para a comprovação anônima de que são um humano único ou maiores de determinada idade para o uso de serviços on-line.

Em caso afirmativo:

7.1.1 De que maneira esse tratamento reflete o melhor interesse de menores de 18 anos, nos termos do art. 14 da LGPD?

Não aplicável. Consulte a resposta à Pergunta 7.1 acima.

7.1.2 Indicar os parâmetros utilizados para considerar o melhor interesse no caso concreto.

Não aplicável. Consulte a resposta à Pergunta 7.1 acima.

7.2 Foi realizado teste de balanceamento para verificar se os eventuais benefícios do tratamento de dados pessoais em análise superam os riscos para crianças e adolescentes?

Não aplicável. Consulte a resposta à Pergunta 7.1 acima.

7.3 Indicar se foram publicadas, em transparência ativa, de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais desse grupo de usuários:

7.3.1 informações sobre os tipos de dados coletados;
7.3.2 a forma de utilização dos dados pessoais coletados para o treinamento do modelo de IA generativa; e
7.3.3 os procedimentos para o exercício dos direitos a que se refere o art. 18 da LGPD.

Não aplicável. Consulte a resposta à Pergunta 7.1 acima.

8.1 Quais medidas de segurança são adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão?

Conforme observado na resposta nas perguntas acima, nenhum dado pessoal é mantido ou armazenado originado da verificação pelo Orb após a sua conclusão. Pelo contrário, o titular de dados recebe uma cópia criptografada de seus dados pessoais, os quais são armazenados em seu dispositivo móvel. Consequentemente, não há dados pessoais armazenados para o fornecimento do World ID em serviços ou bases de dados que exigiriam tais medidas de segurança.

8.2 Como é garantida a segurança dos dados pessoais em repouso e em trânsito?

Durante o processo de verificação, os dados pessoais temporariamente tratados são criptografados em repouso e em trânsito. Adicionalmente, e conforme descrito acima, os dados são temporariamente armazenados (i.e., menos de 10 segundos no Orb) limitando assim o potencial período de ataque para dados pessoais em trânsito e em repouso.

8.3 Existem níveis de acesso diferenciados para garantir que apenas indivíduos autorizados possam acessar os dados pessoais e dados pessoais sensíveis? Explique o mecanismo de restrição de acesso física e diferencie do mecanismo de restrição digital.

Dados pessoais não são mantidos ou armazenados após a verificação para o fornecimento do World ID. Similarmente, dados pessoais sensíveis não são mantidos ou armazenados para o fornecimento do World ID. **[RESTRITO]** A TFH conta com uma equipe de Segurança da Informação líder na indústria, chefiada por um Diretor Presidente de Segurança da Informação veterano, que buscam garantir que todos os sistemas permaneçam seguros e sejam acessíveis somente pelos indivíduos autorizados.

[RESTRITO]

8.4 São realizadas auditorias regulares para verificar a conformidade das medidas de segurança com a LGPD? Em caso positivo, fornecer a data da última auditoria e empresa responsável.

[RESTRITO]

8.5 Como são tratadas as descobertas em auditorias e implementadas as correções necessárias?

[RESTRITO]

8.6 São utilizadas técnicas de criptografia para proteger os dados pessoais durante sua coleta, armazenamento e transmissão?

Sim. Conforme observado na resposta à Pergunta 1.1 e nas demais disposições acima, a criptografia é empregada, por exemplo, para proteger o PCP, o que inclui os dados pessoais dos titulares de dados e sua transferência com segurança ao dispositivo móvel do titular de dados.

8.7 Explique como são mitigadas as vulnerabilidades em relação à proteção de dados pessoais durante a coleta dos dados biométricos?

Conforme descrito no White Paper em anexo como o **Anexo E** o Orb é um dispositivo de hardware personalizado, seguro, resistente a fraudes e criado para mitigar vulnerabilidades que possam ocorrer durante o processo de verificação. Informações adicionais sobre como o Orb é projetado para proteger os dados pessoais durante a verificação podem ser encontradas na página 31 do White Paper.

8.8 Indicar qual é o tratamento destinado aos dados pessoais considerados não necessários para o alcance da finalidade estabelecida. Em caso negativo, indicar como o princípio da necessidade é atendido.

Como referido ao longo das respostas, o World ID funciona tendo como base a minimização de dados. Não são recolhidos nem retidos quaisquer dados pessoais que não sejam necessários para o funcionamento da World ID. Em vez disso, conforme descrito na resposta à Pergunta 1.1 acima, são recolhidos dados pessoais mínimos para efeitos de verificação, sendo depois transferidos para o titular dos dados. Apenas são retidos os dados anonimizados.