BCLP. Client Intelligent

Insights

WORLDCOIN DIRECTED BY HK DATA PRIVACY REGULATOR TO CEASE OPERATIONS

Jun 03, 2024

SUMMARY

On 22 May 2024, the Office of the Privacy Commissioner for Personal Data ("PCPD") published its "Investigation Findings" regarding the operation of the Worldcoin Project in Hong Kong, pursuant to section 48(2) of the Personal Data (Privacy) Ordinance, Cap 486 ("PDPO").

The PCPD concluded that Worldcoin was in contravention of various Data Protection Principles ("DPPs") in Schedule 1 to PDPO relating to the collection, retention, transparency, data access and correction rights. Therefore, the PCPD served an enforcement notice on Worldcoin, directing it to cease all operations of the Worldcoin project in Hong Kong in scanning and collecting iris and face images of members of the public using iris scanning devices.

WORLDCOIN

An important component of Worldcoin's business is its "World ID", which is a registered digital identity created by collecting participants' face and iris images through iris scanning by an "Orb" (a physical imaging device). After creating a World ID at physical Orb Operators (six of which were in Hong Kong), participants gain access to the Worldcoin cryptocurrency token (called "Worldcoin" or "WLD"), which is tradeable like other cryptocurrencies.

CONTRAVENTION OF PDPO – PCPD'S FINDINGS

After investigations, the PCPD found that Worldcoin had contravened the DPPs of the PDPO below for the following reasons:

DPP 1(1): PURPOSE OF COLLECTING PERSONAL DATA

Given that iris scanning already fulfilled the purpose of verifying the "humanness" of the participants, the PCPD's view was that scanning and collection of face images was not required. In

any event, both the collection of face and iris images were not necessary and were excessive, because there were less privacy-intrusive means to verify a participant's identity.

DPP 1(2): MANNER OF PERSONAL DATA COLLECTION

PCPD concluded that Worldcoin failed to provide adequate information to participants to enable them to make an informed choice or give a real consent, because (a) Worldcoin's "Privacy Notice" and "Biometric Data Consent Form" ("**Worldcoin's Documents**") were not made available in Chinese, (b) the Orb Operators did not offer any explanation and did not confirm the participants' understanding of Worldcoin's Documents, (c) Worldcoin's Documents did not inform the participants of the possible risks regarding the disclosure of biometric data, and (d) no age verification was conducted at the Orb Operators before the collection of biometric data from the participants.

DPP 1(3): DATA USERS' RIGHT TO BE INFORMED

PCPD concluded that Worldcoin failed to inform participants (a) of the purpose for which their personal data was to be used, (b) whether it was obligatory to supply the personal data, (c) of the classes of persons to whom their personal data may be transferred, and (d) of the right and means to request access to and to correct their personal data.

DPP 2(2): RETENTION OF PERSONAL DATA

PCPD concluded that Worldcoin's policy was to retain participants' biometric data for ten years to train its AI models for its user verification process. The retention of personal data of participants for such a prolonged period was not justified.

DPP 5: INSUFFICIENT TRANSPARENCY OF PERSONAL DATA POLICY AND PRACTICES

At the material time, Worldcoin's Privacy Notice was not available in Chinese.

DPP 6: RIGHTS OF DATA ACCESS AND CORRECTION

PCPD concluded that the "Biometric Data Consent Form" did not provide the means for the participants to access and correct its personal data.

TAKEAWAY POINTS

This case shows PCPD's proactive attitude in investigating potential contraventions of requirements under the PDPO, as well as the PCPD's wide investigation and enforcement powers under the PDPO.

As consumers are becoming more careful and aware about their data privacy rights, and regulators are more proactive in policing potential data privacy breaches, companies which handle or collect personal data, especially sensitive or biometric data, should make sure that their practices and

polices comply with the requirements under the PDPO, including the DPPs. The PCPD's "Guidance on Collection and Use of Biometric Data" should be referred to before a company decides to collect biometric data, e.g. DNA samples, fingerprints, palm veins, hand geometry, iris, retina and facial images.

As this case also demonstrates, compliance with data privacy laws is so important that it can affect whether or not a company's operations remain viable.

While there is no legal requirement under Hong Kong law for companies to appoint a data protection officer, it would be good practice[1] for a senior executive (for a major corporation) or the owner/operator (for a small organisation) to act as the data protection officer to oversee the company's compliance with the PDPO and implementation of personal data policies.

---

[1] According to the "Privacy Management Programme: A Best Practice Guide" published by the PCPD.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Glenn Haley

Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450

Ian Cheng

Hong Kong SAR

ian.cheng@bclplaw.com
+852 3143 8455

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2025 Bryan Cave Leighton Paisner LLP.