PICCASO

Privacy & Security Insights with PICCASO

Privacy for Blockchain

Ash Costello, Partner

gunnercooke

Sponsored by

PrivacyCulture

PICCASO

Privacy for Blockchain

Crypto entities, and other organisations leveraging blockchain and distributed ledger technologies, are built on a tech stack that differs fundamentally from the tech stack of traditional industries. These differences include transparency, immutability and the potential for immediate global publication. These differences are the features which enable the innovative products, services and operational efficiencies enjoyed in this industry.

Regardless of the tech-stack used by an organization, compliance with all relevant laws is still mandatory. Hence, even in the blockchain and crypto industry, financial services licenses must be applied for, taxes must be paid, and the protection of personal data must be hard-wired 'by design and default' into an organization's practices and procedures.

The UK's data protection regime comprises the UK GDPR (that is, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679), along with the Data Protection Act 2018 (DPA 2018).

Any organisation that processes the personal data of UK individuals must comply with the UK's privacy laws. This includes ensuring that individuals' rights are protected: the right to be informed about how their personal data is being processed and shared; the right of access to the personal data an organisation holds about them; the right to have their personal data be rectified; the right of erasure of their personal data from an organisation's systems; the right to restrict processing in certain circumstances; the right to object to processing, and rights related to automated decision making including profiling.

Earlier blockchain technologies struggled to comply with these and other GDPR requirements. Data shared over these technology stacks often cannot be changed: it is permanent and immutable. These factors are one of the greatest advantages of blockchain technology: they foil attempts to 'hack' or fraudulently interfere with the data.

Similarly, these earlier blockchain tech stacks can be, and often are, global by definition. Therefore, the data is exported over international borders and to countries who are not approved by the UK's Data Regulator (the Information Commissioner's Office or "ICO").

To lawfully send personal data outside the UK, organizations must apply appropriate safeguards to ensure that the recipient applies the same standards of data protection as the UK GDPR. These safeguards include contractually obliging the recipient to protect the data (for example using 'standard contractual clauses') or by transferring data only to an 'approved country'.

However, blockchain entities cannot usually comply with these requirements. The immutability and transparency of blockchain, and its potential for immediate global publication, often means that any personal data which has been moved on-chain has been transferred outside the UK, cannot be removed or corrected, and is potentially accessible and visible globally. Picture a 'peer to peer' exchange, or the interactions between nodes on a protocol, or the interactions between wallets: these interactions are made possible by the real-time transmission of data on a decentralized basis. Requiring each node on a protocol or each counterparty in a peer-to-peer exchange to complete the vendor due diligence or other privacy compliance safeguards before sending them any data would defeat the beauty of blockchain's speed and transparency.

How then can blockchain entities comply with the UK GDPR? How can they mitigate their risk of regulatory fines or legal actions from individuals?

Often, such entities tell themselves that any public data is not personal data. Although some States in the US concur that certain types of publicly available personal data are not 'personal' for privacy law purposes, in Europe and the UK, all personal data is 'personal' for privacy laws – even if it is publicly available. Any data which can identify an individual (either alone, or when used with technology or other information) is personal data. This includes work email addresses, work titles, social media handles, wallet addresses, public keys, IP addresses, telephone numbers, digital identities among other identifiers. Whether this data is already publicly available is irrelevant. There are very few exceptions to compliance with UK GDPR, and 'public personal data' is not among them.

So how can they comply? There is debate among regulators about whether UK GDPR compliance is in fact possible. The consensus is that where personal data must be moved onchain and cannot first be anonymised by technologies such as zero knowledge proofs (also known as ZKPs), arming individuals with sufficient information to enable them to give valid and fully informed consent is the best route to breach-mitigation and towards compliance. This requires full disclosure about the use of any personal data, its transmission onchain, and explaining that being onchain means that personal data is being transferred globally (potentially), and that individuals will be unable to avail of UK GDPR protections such as the rights to deletion and correction.

What are the penalties for breach?

Failing to comply with the UK GDPR could attract enforcement by the ICO. Their powers include assessment notices, warnings, reprimands, enforcement notices, and administrative fines. Serious breaches of the data protection principles can attract fines of up to £17.5 million or 4% or annual turnover, whichever is higher.

In October 2022, the ICO issued a fine of £1,350,000 for contravention of one of the core transparency principles by collecting, processing, and using personal and special category data in an unsatisfactory manner.

Other recent monetary penalties issued by the ICO include a fine of £12.7 million for numerous breaches by a number of breaches by TikTok, and TikTok), and a fine of £78,400 against a hospital trust for sending bulk emails to its users.

PICCASO

Listen now on:

Spotify

Google Podcasts

YouTube

Apple Podcasts

About us:

We are a UK based non-for-profit privacy special interest group, led by seasoned volunteers who are senior leaders in privacy and data protection.

The primary aim of PICCASO is to create a community of professionals that share the value of exchanging 'know how', insights, clarity and explanation on specific privacy and data protection topics designed to distinguish between legal requirements, operational implementation, and strategic objectives, with the aim of greater understanding in how to achieve optimal outcomes based on good practice and thought leadership.

The PICCASO community is drawn from across the UK, Europe, and beyond, and from all industry sectors.

Contact us:

www.piccaso.org
Bouverie House | 154-160 Fleet St | London | EC4A 2DQ
T. +44 (0) 207 112 9360 | hello@PICCASO.org
https://www.linkedin.com/company/piccaso/