Context

The telecommunications industry does not have a good track record of keeping Personally Identifiable Information (PII) properly protected. For example:

- In 2016 TalkTalk was fined £400k for failing to prevent hackers stealing the PII of 156,959 customers[1]
- In 2017 EE was fined £200k for failing to prevent hackers stealing the PII of 114,000 customers
- Also in 2017 O2 was fined £100k for failing to prevent hackers from stealing the PII of 50,000 customers.
- In 2019 BT was fined £400k for failing to prevent hackers stealing the PII of millions of customers.
- In 2021 T-Mobile experience a hack which resulted in the personal data of nearly 50 million customers being exposed[2]

These incidents demonstrate that Communication Providers (CPs) and the PII data they hold are a clear target for hackers and other data security attacks.

Given this context it is somewhat surprising that industry players, as data controllers, are contemplating allowing TOTSCo to become a data processor of their unencrypted PII. Afterall the TOTSCo hub presents a more attractive attack surface to a hacker than an individual communication provider. Afterall the TOTSCo Hub will be handling the PII of customers from all communications providers, not just one.

In its current guidance the ICO states that in a case of PII data loss[3]:

> "Where such losses occur, and where encryption has not been used to protect the data, it is possible that regulatory action may be pursued. This is particularly the case given the widespread availability of encryption solutions, and the ease with which you can deploy them in your organisation."

The Electronic Communications (Security Measures) Regulations 2022 4(5) states:

> "A network provider must use within the public electronic communications network signals which, by encryption, reduce the risks of security compromises occurring."

[1] https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/).

[2] h]ps://www.tmobile.com/news/network/cybera]ack-against-tmobile-and-our-customers

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-s-required-under-the-uk-gdpr/

The consultation document itself includes the statement from the ICO on the requirement to encrypt personal data:

> "The UK GDPR includes encryption as an example of a technical measure that can be appropriate to protect the personal data you hold. Ultimately, whether or not encryption is the right measure to put in place depends on your circumstances—the sort of processing you are undertaking, the risks that may be posed to individuals' rights and freedoms, and the state of the art of technology available to you to protect that data"

The fact that the consultation acknowledges that E2EE is possible would itself indicate that it is a state of the art technology that is available.

We appreciate the acknowledgement in the consultation document that the implementation of E2EE would have no significant impact on the Hub architecture. It is worth noting that such a statement might be taken into account by the ICO or other authorities in any future investigation.

Our understanding from the consultation is that the reasons for not adopting E2EE of messages from launch are:

- Inexperienced CPs may struggle to implement encryption of their messages
- Key issuers might need to store and decrypt against old keys if another CP sends them messages using a deprecated key.
- Additional failure modes will need to be tested during end-to-end testing which might extend the process.

One key benefit that has not been highlighted in the consultation is that TOTSCo would no longer be a data controller which would make its processes and information and security policy more simple.

With developer's guides and software development kits provided by TOTSCo, do you feel confident that you could implement E2EE?"

We think that CPs that do not have the capability to encrypt PII that they send to third parties are unlikely to meet the UK data security regulations and would be subject to sanction if their PII data was compromised.

CPs that do not have this capability should seek to use a third party portal service to interact with the Hub and that third party service provider should ensure that their PII data is properly secured.

The TOTSCo Developer's Guides are simple to follow and can be used by CPs to put in place the necessary security measures.

"Would this delay your development? Does it affect your confidence around testing and going live?"

No - We do not anticipate any delay. On the contrary we would expect a faster delivery from TOTSCo because TOTSCo will no longer be a Data Processor and so its operating and security

processes can be more simple . Implementing E2EE will help CPs to meet existing and new security regulations and avoid the PII data leaks experienced by the industry in the past.

"Do you anticipate operational complications?"

No – The opposite as our relationship with TOTSCo will be simplified by the fact that TOTSCo will not be acting as a data processor of our PII.

We do anticipate complications in **not** having E2EE and message signing in place as it would make it difficult for us to defend any PII data breach with the relevant UK authorities.

"Do you think that adding E2EE would impact your ability to meet the 60s SLAs?"

No – adding encryption to messages take fractions of a second and will not be a significant factor compared to the time required to carry out a data query which in most cases we anticipate will be sub-second in any case. Some members have tested adding E2EE to the specified TOTSCo messages and have seen no measurable impact on response times.

"On balance, do you think that E2EE should be implemented.
- never
- at go-live
- maybe after go-live?"

It is essential that E2EE is implemented for go live.

The defence that it was too difficult for some CPs to implement in the light of a data breach is unlikely to be effective given the guidance from the UK authorities.

We must ensure the confidentiality of consumer data and deliver the HUB as fast as possible. E2EE simplify the HUB development and processes while protecting the industry from what happened in previous data breaches.

"For which development languages would you like to see example of implementation of E2EE to be provided by TOTSCo e.g., Java, PHP, Python, C#"

The example already provided by TOTSCo is sufficient. Most competent coders will already be proficient in the techniques for including encryption of data into any APIs they are writing.