

[REDACTED] (CNECT)

From: [REDACTED] (CNECT)
Sent: 08 November 2016 17:28
To: TIMMERS Paul (CNECT)
Cc: [REDACTED] (CNECT); [REDACTED] (CNECT); [REDACTED] (CNECT)
Subject: minutes Deutsche Telekom 8/11

Minutes meeting between Deutsche Telekom ([REDACTED] and [REDACTED]) and Paul Timmers and [REDACTED]
[REDACTED] 8/11

- DT gave an insight into their data privacy policy as a strategic asset. They focus on trust with technical and organisational safeguards and transparency towards citizens.
- The conversation focused on the use of pseudonymised data. Following the GDPR discussion, it is unclear for DT what exactly is 'pseudonymised'.
- To respect rights of consumers and maintain trust, but at the same time enhance business opportunities, DT has a privacy friendly business model. They argue that it would fit if they could use pseudonymous instead of anonymous data under the ePD, with high safeguards (encryption, transparency, possibility to opt-out etc.). Pseudonymisation should be an additional legal basis to process data, on top of consent, just as in the GDPR.
- On a consent basis it is difficult to create databases that are big enough + the purposes for which the data is used may change, therefore consent would need to be asked multiple times.
- Anonymous data has limits: it's very hard to reach anonymity; you cannot re-identify while individuals may derive interesting data from data sets; they are a snap shot of a moment which makes it hard to analyse a development. Pseudonymised data is a basis for better services because they can be personalised. Before this service would be provided, consent would be needed.
- DT puts forward they don't see why location data from a GPS (GDPR) is under a different legal regime than location data derived from cell towers (ePD).