Notes on Consent and Anonymisation

Consent

> Collecting robustly anonymised data does not require consent by law.

http://www.highlights.rsc.mrc.ac.uk/PIHR/index.html#/lessons/0aWbhlBbF3dIBhw2dIgLtY66OUtsr51K?_k=dr7ymo

> Release of 'anonymised data' does not constitute a breach of confidence where the risk of (re)identifying an individual is sufficiently mitigated.

http://www.highlights.rsc.mrc.ac.uk/PIHR/index.html#/lessons/NCX9Obsk1qN5cBc3BgPcxJq1DAHeSjns?_k=djj3i1

Anonymisation and pseudo-anonymisation

Pre-GDPR

The ICO's Code of Conduct on Anonymisation provides a guidance on anonymisation techniques. However, it is not yet updated for GDPR.

http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf is also not yet updated for GDPR. Some quotes from p.10

> Anonymised data are personal for the original data controller but non-personal for other users of the data… We hold the second of these positions as it directly ties the concept of anonymisation to the notion of the context of personal data. …
>
> This interpretation is also shared by the UKs data protection regulator the ICO. However, in other jurisdictions the first resolution of the paradox is favoured:
>
> *Thus, it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data.*
>
> EU: Article 29 Data Protection Working Party; Opinion 05/2014 on Anonymisation Techniques page 9

GDPR

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

> Pseudonymisation is defined within the GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual" (Article 4(3b)).

Recital 26

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person

Example

Whilst the second team cannot identify any individual, the organisation itself can, as the controller, link that material back to the identified individuals.

This represents good practice under the GDPR.