

Anonymisation and pseudonymisation



“And I sit here without identity: faceless. My head aches”

Sylvia Plath

The Article 29 Data Protection Working Party adopted Opinion 05/2014 regarding anonymisation techniques in April 2014:

“Once a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies.”

Anonymisation of data

Manipulating a dataset such that individuals are no longer identifiable and their data are “anonymised” can be a good strategy to release the data from the legislative regime. The benefits of anonymisation are clear – issues of consent no longer apply, the data can be exported internationally, the data can be kept for however long the controller wants to – and such a position provides a clear incentive for data controllers to anonymise their datasets. However, anonymisation is an irreversible process that removes the ability to identify the data subjects, which may devalue the data such that it is no longer of any use. Proper anonymisation may therefore simply not be an option for many data controllers.

Pseudonymisation of data

Data controllers often misunderstand the requirements for anonymisation and the resulting manipulation will probably still allow for the singling out of a specific individual, linking to other data about an individual, or the identification of an individual’s identity. The Article 29 Working Party notes, in Opinion 05/2014, that resulting data from an attempt at anonymisation is often pseudonymised data, to the extent that it involves, “replacing one attribute (typically a unique attribute) in a record by another. The natural person is therefore still likely to be identified indirectly”. This is often achieved through the use of hashing, encryption or tokenisation of an identifier.

Reidentification

The likelihood of re-identification of individuals from a purportedly anonymised dataset or pseudonymised data may become much more significant under the GDPR than it was under the Directive, due to the exponential rate of technological progress and an increase in entities wishing to combine datasets in order to mine a greater detail about individuals than was previously possible.

Advantages of pseudonymisation

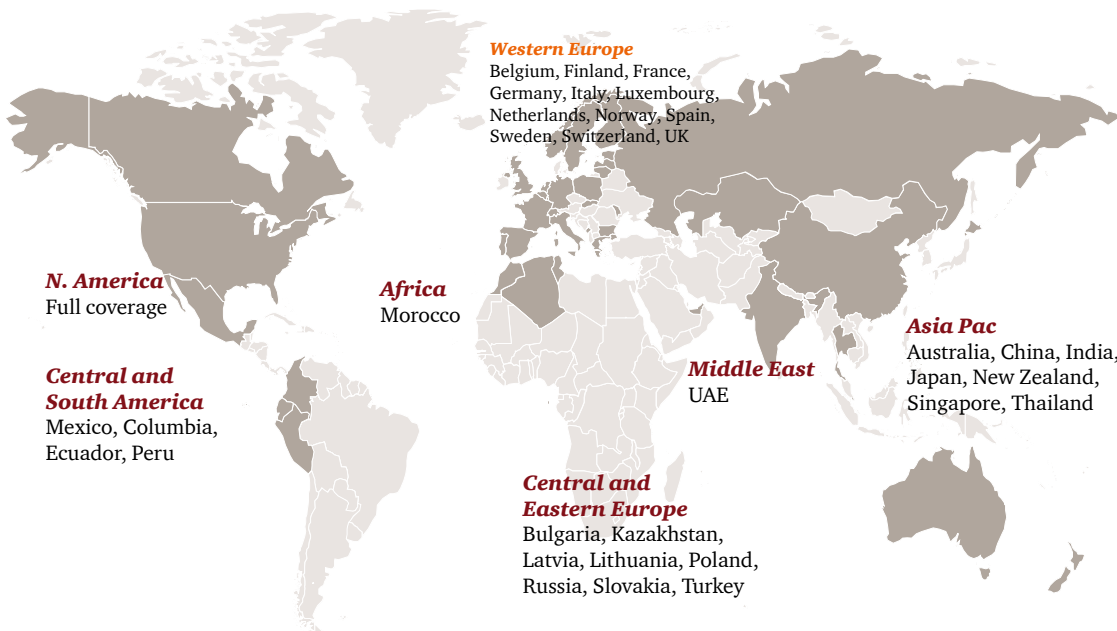
While personal data is most definitely the class of information covered by the GDPR and anonymised data is not regulated by definition, pseudonymised data represents a useful compromise position. It allows a data controller to afford some protection over

the data, by, for example, minimising the chances that the underlying identities will be revealed.

Data controllers are often in the position that fully anonymised data is simply not an option and pseudonymisation is an ideal method of respecting the privacy of the data subjects while still enabling the commercial value to be retained. Reversibility may also be an important element of a dataset, for example in the context of clinical drugs trials that leads to a necessity to contact the test patients. Pseudonymisation is often a more palatable option for many data subjects who would be particularly concerned at the prospect of the data being directly linked to them, but do not have any such worries about tokenised identifiers.

Data protection authorities will evidently look to pseudonymisation as a method of ensuring that the principle of data minimisation is satisfied and it is an approach which could satisfy the requirements of privacy by design and by default and with respect to ensuring the security of data held. The question of whether data can be pseudonymised is likely to become a feature of Privacy Impact Assessment and disclosure to a Data Protection Authority with regard to undertaking particularly risky processing activities.

PwC's global privacy practice



PwC Luxembourg Contacts



Vincent Villers
Partner
2367
vincent.villers@lu.pwc.com



Frédéric Vonner
Partner
4173
frederic.vonner@lu.pwc.com



Sami El Euch
Director
2685
sami.eleuch@lu.pwc.com



Cédric Nédélec
Data Protection Officer
2186
cedric.nedelec@lu.pwc.com

Document version 2. This publication has been prepared by PricewaterhouseCoopers Legal LPP (1, Embarkment Place, London, UK, WC2N 6RH) for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Legal LLP (London), its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.