Anonymization: Silver bullet or just a (not quite) modern fairy tale?

Katharina A. Weimer and **Melanie Ludolph** of Fieldfisher Germany discuss issues surrounding anonymization techniques and the status of anonymized data.

At a time when technological progress is moving faster every day to day, uncertainty about essential concepts such as anonymization and pseudonymization can be frightening. For technologies based on large amounts of data such as big data analysis in the med tech sector or AI systems, these core concepts can be decisive for permissions in data processing. There is often no clear distinction between anonymity and identification, and if there is one at all, it becomes increasingly blurred. Clarifications are clearly needed.

Privacy vs. modern technologies

Even though social media often paint a different picture, people still have a strong interest in privacy. The fundamental right to data protection, also reflected in the European General Data Protection Regulation 2016/679 (GDPR), legally protects this desire. Conflicting with this desire is an ever-increasing interest in all areas of human life, such as online browsing and purchasing behaviour, financial situation and health, physical activity or communication patterns. People freely disclose this type of data but are often reluctant for companies to analyse and possibly monetize it. Fundamental principles of data protection law, such as data minimization and purpose limitation, present limitations when it comes to gaining insights that can drive not only profit and customer-friendly products, but also advances in science and medicine. Other prime examples of the application of data analysis for the benefit of the consumer are the further development of AI-based tools (e.g. speech recognition software) or analyses of trends in the business sector. It is a fact that anonymization is an essential element in today's world and is often seen as the "silver bullet" of data protection by design where legal and technical challenges arise.

Anonymity and pseudonymity according to the GDPR

Whenever information identifies, or can identify, an individual it is considered personal data and thus falls within the scope of GDPR. However, if the individual is not, or is no longer identifiable – regardless of whether the data was collected anonymously from the outset or anonymized later – it does not constitute personal data and is therefore excluded from the scope of the GDPR (recital 26 of the GDPR).

This seemingly easy concept is riddled with trapdoors though. The GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject')" (Art. 4 No. 1 GDPR). While "identification of a person" is further defined[1], it remains unclear how concrete the reference to a natural person must be for the data to be personal and thereby in scope of GDPR.

Absolute vs. relative anonymization

The question of whether data is anonymous or not has long been discussed among privacy experts, since the legal situation pre-GDPR also lacked clarity. Initially, the key question revolved (and partly still does) around the concept of "absolute vs relative anonymity". Absolute anonymity means that re-identification is impossible for everyone, whereas for relative anonymity, such re-identification only fails because the effort (in terms of time and cost) would be disproportionately high or is legally prohibited. This situation of relative anonymity often arises in cases of transfer of limited or pseudonymized sets of data: the data can, in theory, still be re-identified (e.g. by the sender of the data) but the recipient is unable, factually and legally, to re-identify the data.

This differentiation, which initially appears to be purely conceptual, is of great importance in practice.

Here is an example: A controller transmits raw data to a cloud provider, which is encrypted in transit and at rest[2] at the recipient cloud provider, using state-of-the-art technology. It is impossible for the cloud provider to access the key or decrypt the data at any time. Requiring absolute anonymity, the cloud provider would be qualified as a processor, since it is in theory still possible to relate the data to a person – with the knowledge of the controller (who has the key to the encrypted data). As a legal consequence, the relevant legal and contractual processor obligations from Art. 28 GDPR apply to it.

In the case where the concept of relative anonymity is assumed, the regulations of the GDPR would not apply – it is not possible for the cloud provider to overcome the encryption and therefore, from its point of view, no personal identification can be made at any time. Data protection regulations would not apply in this context.

The opportunity to clarify this controversy came with inception of the GDPR – and went. In Art. 4 No. 5, GDPR chooses a compromise: The definition of pseudonymization in Art. 4 No. 5 GDPR as well as recital 26 both refer to additional knowledge or technical measures in the context of a possible identification, which, however, only have an effect if using them does not require a disproportionately large financial or other economic effort, and is legally permissible. A reliable guarantee of anonymity cannot be derived from a legal point of view.

Factual difficulties

In addition to legal uncertainty comes a factual uncertainty which is often "homemade": Due to the size of data lakes, even if data was originally anonymized, the sheer mass of accumulated information can lead to a

greater risk of re-identification, especially if health and/or genetic data is involved.

Anonymization requirements – the legal context

There are two use cases in the context of anonymous data: it was either collected anonymously from the outset or was later anonymized. This distinction is relevant: If data is "collected" anonymously, GDPR does not apply. Art. 4 No. 2 GDPR necessarily links the term "processing" (including collection) to personal data[3].

Subsequent anonymization of personal data is itself a processing step, with the consequence of requiring a legal basis. Since the GDPR itself does not offer a specific legal basis for anonymization, all legal bases mentioned in Art. 6 GDPR and Art. 9 (2) GDPR are eligible.

Non-special categories of personal data

In addition to consent (Art. 6 (1) lit. a GDPR), the legitimate interest under Art. 6 (1) lit. f GDPR is the legal basis most relevant to controllers in practice. This involves balancing whether the interests of the controller or a third party in anonymization override the interests of the data subject worthy of protection. Due to common sense, this balancing must always be in favour of the controller when anonymization is concerned, since it does not result in any further impairment of the rights of the data subject and no special need for further protection arises. This presupposes though that the controller has technical control over the anonymization process (see the requirements of Art. 32 GDPR).

Special categories of personal data

As far as the anonymization of special categories of personal data[4] is concerned, only the limited scope of Art. 9 (2) GDPR is applicable. In practice, anonymization of such data is often only possible with consent (Art. 9 (2) lit. a GDPR), since the other constellations only cover a very narrow range of areas. A recourse to a balancing of interests as before is not envisaged for special categories of personal data, although the positive effects mentioned above would also make sense for the data subject with regard to this category of data.

Anonymization as change of purpose

There may also be situations in which it is possible to justify anonymization on the basis of Art. 6 (4) GDPR. Often, the personal data to be anonymized is collected for a specific other purpose. Subsequent anonymization in these cases therefore constitutes further processing, the purpose of which must be compatible with the original purpose of collection. If this compatibility is found, the legal basis for anonymization as further processing continues to be the same legal basis that legitimized the original processing (see recital 50 GDPR). However, for anonymization of special categories of personal data, it is still being debated whether Art. 6 (4) GDPR is applicable.

Anonymization – the technical aspects

In addition to the legal uncertainty of anonymization, it is also technically unclear when a personal reference no longer exists. There are different methods to anonymise personal data, however, for simplification, it is assumed that the data to be anonymized is organized in a structured way. Some of the most common methods are the following:

- **Deletion**: Parts of a data record are deleted to generalize the information.
- **Falsification**: Part (or all) of the data is changed by e.g. swapping parameters within the data record or an artificial data record is created using the original data record as an example.
- **Clustering**: Individual data are combined, for example, by forming the median value from the individual data.

Furthermore, scientific approaches to the development of formal anonymity models have also been in development for a while.

But anonymity of data is difficult to achieve, and while many companies have a sound grasp of these technical solutions there are thousands of companies who have not, and are thus vulnerable in their approach to anonymization.

Example: Voice recognition

A prime example of the difficulties regarding anonymity of data are speech recognition systems/software. Such software is often employed for training of employees in customer service centres. The systems record the calls and usually make them available for the supervisors to review them and thereupon train the employees. However, the recordings are also often used to improve the software, and to provide statistical analysis back to the customer service centres. In order to do so, the recordings are cut into fragments of as little as parts of a second – but often up to several seconds. Clearly the software provider is unable to identify the speakers in those fragments. However, individuals at the call centre are likely able to identify the employees according to their voices. If the recordings are considered personal data, the use of the fragments is fully subject to GDPR, requiring a legitimate justification for the use of the employee data. If it were considered non-personal information, the service provider would be free to use the data. Thus it is essential for the business of the service provider to be able to use the information.

In this scenario, the differentiation between relative and absolute anonymity becomes very clear. If only absolute anonymity were sufficient, the service fragments would clearly be considered personal data and thus be subject to much stricter limitations and obligations, and the customer service centres may not even be able to provide for a safe processing for the purposes of the service provider even though the service provider itself has no way of identifying the individual.

Is it reasonable to assume a relative anonymity in this case and maintain this as sufficient? From the perspective of the service provider, for sure. But customers are often of a different view and are reluctant to agree to this concept, thereby inhibiting the further development and improvement of the product they are using.

Conclusion

The use of anonymous data is not only beneficial for controllers, who are provided with the opportunity to process

large amounts of data for a wide variety of economic, scientific and other purposes, but also for data subjects whose fundamental rights remain protected. However, there are still uncertainties at many points, for example with regard to terminology, legal bases or a clear definition of when anonymity is ensured. Particularly with regard to special categories of personal data, there are unnecessary hurdles to anonymization that do not add value, because data subjects can hardly be better protected than by using anonymous data.

AUTHORS

Katharina A. Weimer, LL.M. is a Partner, and Melanie Ludolph is an Associate at Fieldfisher Germany.
Emails:
Katharina.Weimer@fieldfisher.com
Melanie.Ludolph@fieldfisher.com

REFERENCES

1 "An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"
2 Information is at rest when it is not being accessed, it is located in a database, stored in a local drive, network shared drive or in cloud storage.
3 It would therefore be more accurate in this case to use the term "handling" and not "processing" personal data.
4 e.g. personal data revealing religious beliefs, health data or data concerning a natural person's sex life or sexual orientation.

Belgium's DPA to take down non-compliant websites

The Belgian Data Protection Authority is suspending websites that are linked to infringements of the GDPR, law firm Hunton Andrews Kurth LLP reports.

The DPA has signed a cooperation agreement with DNS Belgium, which manages domain names. The purpose of the cooperation agreement is to allow DNS Belgium to suspend ".be" websites.

DNS Belgium will provide the Belgian DPA's Investigation Service with the information it requires for its investigations. If the Belgian DPA considers a data processing activity to infringe the GDPR, and the responsible data controller or data processor does not comply with the DPA's order to suspend, limit, freeze (temporarily) or end the data processing activity, DNS Belgium will inform the website owner about the infringement and re-direct the relevant domain name to a warning page of the Belgian DPA.

"If, at the expiration of a 14-day period, the website owner indicates that it has taken the appropriate remediation measures to stop the infringement and the Belgian DPA does not contest it, the relevant domain name will be restored. During the 14-day period, website owners can make a request to stop or suspend the Notice and Action procedure, in which case the domain name may be restored until a decision regarding the procedure has been taken. If the infringement is not remediated during the 14-day period, the website will continue to be re-directed to the Belgian DPA's warning page for a period of six months, after which the website will be cancelled and placed in quarantine for 40 days before becoming available for registration again. The Inspector General or the Director of the Litigation Chamber of the Belgian DPA can, at their discretion, provide extra time to the website owner to comply with the relevant data protection requirements," Hunton Andrews Kurth LLP reports.

• *See www.lexology.com/library/detail.aspx?g=0ee39d9b-9223-493e-8549-9c9de507aa67*

Still no progress with EU e-Privacy regulation

The EU Council has failed to find a common position on the German Presidency's proposal on e-Privacy. The file will now be forwarded to the next Presidency, Portugal.

The German proposal put much emphasis on consent as opposed to legitimate interests. Some Member States are now saying that the Council should return to the proposal made by the Finnish Presidency.

Speaking at a Forum Europe panel on 10 December, Birgit Sippel, MP and rapporteur on the file for the European Parliament's LIBE Committee, said that she is not very optimistic about the file – she thought that perhaps service providers are putting much pressure on Member States, which in turn are represented by different ministries – a situation that is not helpful to the negotiations.

Peter Eberl from DG Connect at the European Commission said that the Portuguese Presidency has named e-Privacy as one of its priority areas, and there are only few issues that are open. We now know that there is not much support for legitimate interests among the Member States, he said. The pandemic has brought new amendments to the text, for example use of heat maps. A regulation is needed as the GDPR does not cover all issues, for example the confidentiality of communications.

• *See the conference session, moderated by Laura Linkomies, at youtu.be/ifUpAjAcdns*

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Data transfers after *Schrems II*: Reflections from the Asia Pacific

Clarisse Girot of the Asian Business Law Institute, **Mark Parsons** of Hogan Lovells and **Olga Ganopolsky** of Macquarie Group discuss practical issues and geopolitical sensitivities.

The decision of the Court of Justice of the European Union (CJEU) in *Schrems and Facebook Ireland v Data Protection Commissioner*[1] (*Schrems II*) concerns the interpretation of the GDPR as a matter of EU law, but the implications of this ruling are global in their dimensions.

Until now, the consequences of the decision have mostly been analyzed in a transatlantic context, in the

Continued on p.3

China issues a comprehensive draft data privacy law

Draft PPIL marks a decade of evolution in the direction of a 'European style' law. By **Graham Greenleaf**.

The long-anticipated Law of the People's Republic of China on the Protection of Personal Information (Draft)[1] (PPIL) was released by the Standing Committee of the National People's Congress (SC-NPC), the second-highest legislative body in China,[2] on 21 October 2020, for brief public consultation until 19 November 2020. If this law is considered a "basic law"' it can only be enacted by the full NPC, not by the Standing Committee. It is expected that the revised

Continued on p.6

Issue 168 **DECEMBER 2020**

INTERNATIONAL report

ISSUE NO 168 DECEMBER 2020

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Clarisse Girot
Asian Business Law Institute, Singapore

Mark Parsons
Hogan Lovells, Hong Kong

Olga Ganopolsky
Macquarie Group, Australia

Gloria Marcoccio and Luciano Delli Veneri
DPOs & privacy experts, Italy

Michael Drury and Julian Hayes
BCL Solicitors LLP, UK

Jordan Greenwood
Jordan Greenwood Legal Services, Canada

Avishai Ostrin
Asserson, UK

Katharina A. Weimer and Melanie Ludolph
Fieldfisher, Germany

Frank Madden
Promontory, UK

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

All eyes and ears on data transfer solutions – everywhere

As we await the result of the Brexit negotiations and what will be the future route for EU-UK data transfers (p.23), it is clear that international data transfers is the matter of the moment worldwide. In the aftermath of the *Schrems II* decision by the Court of Justice of the European Union, the European Commission has just released its draft implementing decision on Standard Contractual Clauses for transferring personal data to third countries (p.11 and p.31). The court decision has implications also for Asia-Pacific countries. Our correspondents argue that there is concern that the decision may encourage these countries to adopt data localisation laws (p.1).

The European Data Protection Board has now adopted recommendations on supplementary measures for transfers following *Schrems II*. Whilst one would not expect immediate enforcement, there is the danger that enforcement action will have to follow if there are individual complaints.

China has issued a draft privacy law (p.1), in which one tool for data exports would be a contract with the overseas recipient, in a similar vein as the EU GDPR Standard Contract Clauses.

Looking into the future, the recent US legislative developments in California (p.13) may pave the way for a federal privacy law, which would probably resolve the dilemma with EU-US data flows. The US Senate Committee on Commerce, Science, and Transportation held a hearing on 9 December to discuss the invalidation of the EU-US Privacy Shield and other matters relating to trans-Atlantic data flows. Once the new administration is in place, we can expect more news on this front. On p.18 we bring you news of the important but not much talked about UK-US Bilateral Data Sharing Agreement, which has been seen as a possible problem for the UK's post-Brexit adequacy decision.

See p.28 for a comprehensive analysis of the current requirements for Records of Processing Activities (RoPA) - a GDPR requirement which relates to the old registration duty.

As this is the last issue for 2020, I wish you a safe and happy end of the year, and Merry Christmas.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 165+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

> "*Privacy Laws & Business* is my go-to for the latest international thought leadership on hot topics in data protection law and policy."
>
> **Giles Pratt, Partner, Freshfields Bruckhaus Deringer LLP**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.