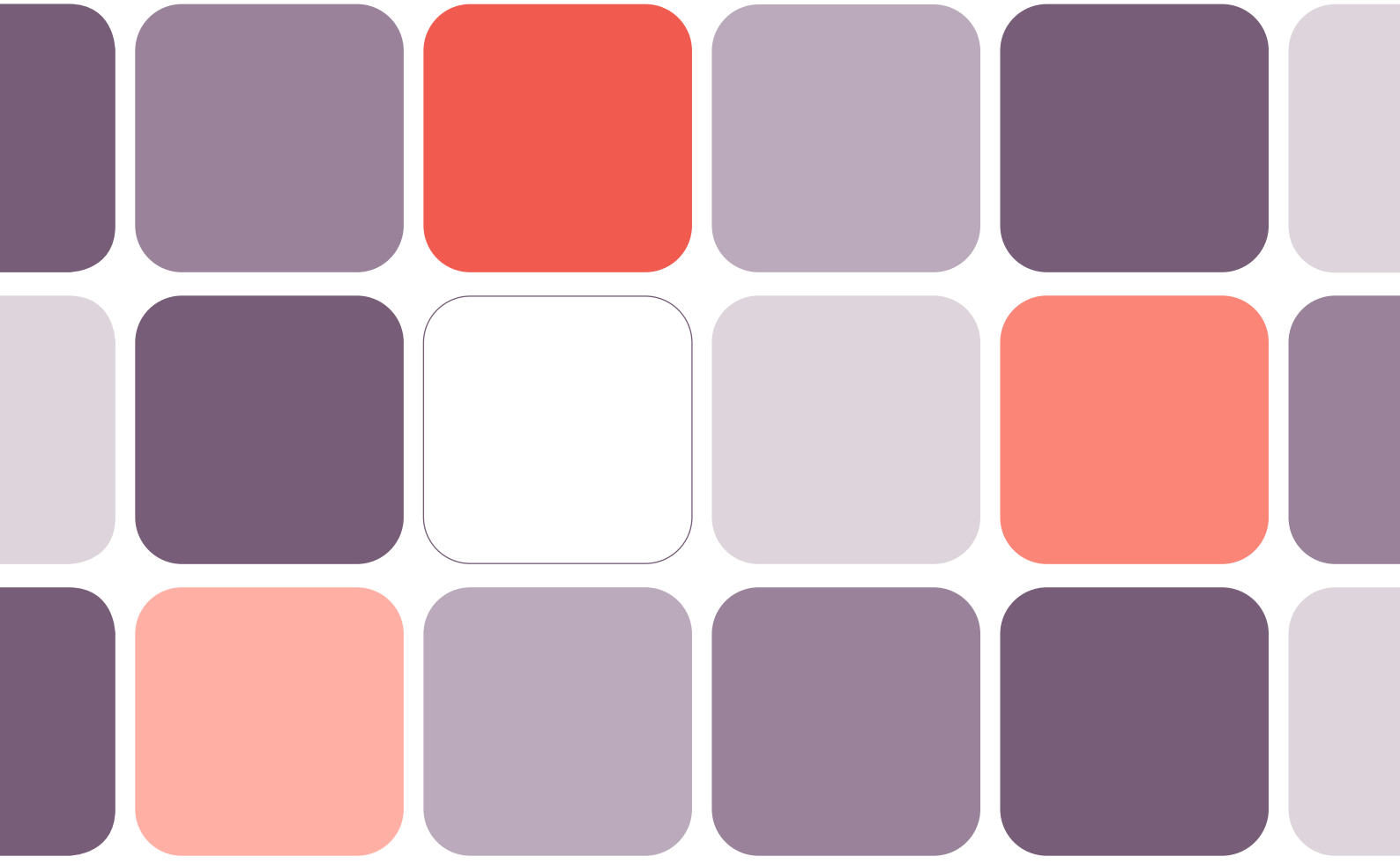
VOLUME FIVE
NUMBER THREE
WINTER 2022–23

ISSN: 2398-1679

Journal of

Data Protection & Privacy



Available online

HENRY STEWART PUBLICATIONS

ANONOS

Data without the drama™

Technische Kontrollen, welche Daten während der Verwendung schützen und Missbrauch verhindern

Zusammenfassung des Artikels mit Beiträgen von Magali Feys (Chefstratege von Ethischer Datenverwendung bei Anonos), sowie Gary LaFever (Co-CEO und General Counsel), der im Januar 2023 im "*The Journal of Data Protection & Privacy*" veröffentlicht wurde.

Zugriffskontrollen und Governance-Richtlinien verhindern den Missbrauch von Daten nicht, selbst wenn die Nutzung intern eingeschränkt wird. Wenn Daten außerhalb einer Organisation geteilt werden, werden sie normalerweise außerdem durch Verschlüsselung, Datenmaskierung und weitere Methoden geschützt, um die Sicherheit während der Übertragung und Speicherung sicherzustellen. Aber - wenn Daten bei einer Verarbeitung unverschlüsselt sind, sind diese gefährdet. Die Autoren des Artikels erklären darin, dass technische Kontrollen zum Schutz von Daten an sämtlichen Stellen an der Kette eingesetzt werden müssen – speziell während Datennutzung. Gesetzlich vorgeschriebene Pseudonymisierung ist eine hochmoderne und rechtlich unterstützte Methode zum Schutz von Daten während ihrer Nutzung, um negative Auswirkungen durch Datenmissbrauch, Sicherheitsverletzungen und Ransomware-Angriffe zu minimieren oder ganz zu verhindern. Die gesetzlich vorgeschriebene Pseudonymisierung ermöglicht es Organisationen, Daten weiterhin für Analyse-, Forschungs- oder andere Zwecke zu verwenden und gleichzeitig sicherzustellen, dass die sensiblen Daten einer bestimmten identifizierbaren natürlichen Person geschützt bleiben.

Wie im kompletten Artikel erläutert, ermöglicht die gesetzlich vorgeschriebene Pseudonymisierung die Datennutzung durch Organisationen für zwei ihrer Hauptziele:

- **Skaleneffekte:** Skaleneffekte nutzen zu können, die durch Cloud-basierte Infrastructure-as-a-Service (IaaS)- und Platform-as-a-Service (PaaS)-Angebote bereitgestellt werden; und
- **Datenaustausch und Sekundärverarbeitung:** Künstliche Intelligenz (KI), maschinelles Lernen (ML), erweiterte Analysefunktionen und andere Möglichkeiten durch den Einsatz von Diensten, die von Drittanbietern als Cloud-basierte Software-as-a-Service (SaaS)-Angebote erhältlich sind.

Die Bedeutung technischer Kontrollen

Aufsichtsbehörden und andere Gruppen erkennen zunehmend die Bedeutung des Einsatzes technischer Kontrollen zum Schutz von Daten vor Missbrauch und Datenschutzverstößen. Diese Gruppen sind sich zum Beispiel zunehmend der Bedeutung technischer Kontrollen zum Schutz von Daten während der Nutzung bewusst:

- **EU und US-Regierungen:** Zahlreiche Probleme zwischen den Regierungen der USA und der EU betreffend die korrekte Art und Weise, grenzüberschreitende Unterschiede in den Datenschutzgesetzen auszugleichen, haben dazu geführt, dass mehrere Datenschutzabkommen zwischen der EU und den USA außer Kraft gesetzt wurden. Beiden Seiten wird immer deutlicher, dass technische Kontrollen notwendig sind und rechtliche Vereinbarungen und Verträge für diese Aufgabe nicht ausreichen.
- **Gerichte:** Grundlegende Unterschiede zwischen US- und EU-Gerichten können nicht ignoriert werden. Technische Kontrollen erlauben es, diese Unterschiede zu überbrücken und auszugleichen; während Datenübermittlungen und die grenzüberschreitende Verarbeitung personenbezogener Daten möglich sind.
- **Strafverfolgungsbehörden:** Während die EU-Aufsichtsbehörden die DSGVO-Anforderungen in Europa nur langsam durchsetzen, ergreifen Strafverfolgungsbehörden zunehmend Durchsetzungsmaßnahmen gegen Unternehmen aller Größen und Nationalitäten. In ähnlicher Weise führen US-Strafverfolgungsbehörden, insbesondere die einzelnen Bundesstaaten, die Durchsetzung nach neuen, strengeren Datenschutzgesetzen durch. Diese Maßnahmen legen dar, wie wichtig technologisch erzwungene Kontrollen sind, um Organisationen vor Strafen, einstweiligen Verfügungen und Ansehensverlust zu schützen.
- **Nichtstaatliche Organisationen (NGOs):** Diese Gruppen haben zunehmend eine höhere Sichtbarkeit und mehr Einfluss, wie etwa die Organisation NOYB von Max Schrems und deren Gerichtsverfahren, welches dazu führte, dass das "EU-US Privacy Shield" und dessen Vorgänger, das Safe-Harbor-Abkommen, gekippt wurden. Diese Handlungen unterstreichen die Rolle von technischen Kontrollen bei Datenschutz- und Datensicherheitsbemühungen.

© 2023 Anonos. All rights reserved.

Sichere und effektive Datenverarbeitung, unterstützt durch technische Kontrollen

Die Autoren halten fest, dass die gesetzlich vorgeschriebene Pseudonymisierung vier Aspekte einer qualitativ hochwertigen und hochgradig vertretbaren Datenverarbeitung ermöglicht und Organisationen dabei unterstützt, ihre Dateninnovations- und Datennutzungsziele ohne regulatorische und Compliance-Probleme oder Durchsetzungsmaßnahmen zu erreichen. Gesetzliche Pseudonymisierung ermöglicht Folgendes:

- **Überwachungssichere Verarbeitung:** Einer der größten globalen Konflikte war die Möglichkeit der Überwachung von EU-Daten durch Nicht-EU-Länder, insbesondere durch die USA. Einige Länder, beispielsweise Südkorea, haben strenge Anforderungen an die gesetzliche Pseudonymisierung verabschiedet, die es ihnen ermöglichten, eine Angemessenheitsentscheidung herbeizuführen. Die Anforderungen von Schrems II (der Fall, der den "EU-US-Privacy Shield" für ungültig erklärt hat), welche vom Gerichtshof der Europäischen Union (EuGH) und dem Europäischen Datenschutzausschuss (EDPB) festgelegt worden sind, weisen darauf hin, dass technische Kontrollen als ergänzende Maßnahmen eingesetzt werden können, um eine Überwachung durch Regierungen von Drittstaaten zu verhindern. Maßnahmen wie die gesetzlich vorgeschriebene Pseudonymisierung können rechtmäßige internationale Datenübermittlungen und -verarbeitungen ermöglichen, die dennoch die Identität der betroffenen Personen in der EU schützen, auch wenn Daten in „nicht vertrauenswürdigen" Umgebungen wie denen eines Unterauftragsverarbeiters, Cloud-Verarbeiters oder anderer Organisationen und Unternehmen verarbeitet werden.
- **Rechtmäßige Verarbeitung:** Ein weiteres zentrales Thema das der Artikel aufzeigt, ist die Sicherung der Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Rahmen der DSGVO. Die gesetzlich vorgeschriebene Pseudonymisierung spielt in der DSGVO eine einzigartige Rolle. Es ermöglicht die Verarbeitung pseudonymisierter Daten, wenn Organisationen keine Einwilligung oder vertragliche Mittel zur Datenverarbeitung einholen können, indem die Verarbeitung berechtigter Interessen als alternative rechtliche Grundlage ermöglicht wird. Dafür müssen Organisationen (a) einen legitimen Zweck für die Verarbeitung haben; (b) die Notwendigkeit der Verarbeitung personenbezogener Daten zur Erreichung dieses Zwecks muss vorliegen; und (c) es muss festgestellt werden, dass die Interessen des für die Datenverarbeitung Verantwortlichen gegen die Interessen oder Grundrechte und Grundfreiheiten des Datensubjekts abgewogen werden. Die Europäische Kommission hat festgestellt, dass der Einsatz technischer und anderer Maßnahmen, wie beispielsweise die gesetzlich vorgeschriebene Pseudonymisierung, dazu beitragen kann, Teil (c) dieses Tests durch geeignete Sicherungsmaßnahmen zu erfüllen. Zusätzlich kann es der Einsatz geeigneter Sicherungsmaßnahmen (z. B. Pseudonymisierung) möglich machen, dass die weitere Datenverarbeitung entsprechend den Leitlinien der Europäischen Kommission rechtmäßig ist. Schließlich kann der Einsatz von Datenschutztechnologien wie Pseudonymisierung sicherstellen, dass Datenverantwortliche die Anforderungen für die Prinzipien "Privacy by Design" und "Privacy by Default" erfüllen, die erfordern, dass der Datenschutz in der Verarbeitung so früh wie möglich angewendet wird.
- **Verletzungssichere Verarbeitung:** Gesetzlich vorgeschriebene Pseudonymisierung kann das Risiko von Datenschutzverletzungen und -missbrauch reduzieren, indem identifizierende Elemente unkenntlich gemacht werden, während die geschützte Form der Daten für eine Verarbeitung mit hohem Nutzwert verfügbar gemacht wird. Pseudonymisierte Daten können nur kontrolliert mit weiteren Informationen verknüpft werden, die vom Datenverantwortlichen gesondert verwahrt werden. Das erlaubt es Organisationen, vertrauliche Daten schützen, ohne sie unbrauchbar zu machen, während gleichzeitig der Aufwand und die Kosten von Datenverletzungen oder -missbrauch verringert werden. In der EU und den USA sind Organisationen durch verschiedene Gesetze und Vorschriften dazu verpflichtet, angemessene Sicherheitsmaßnahmen zum Schutz personenbezogener Daten anzuwenden. In vielen Fällen befreit dies Organisationen von der Verpflichtung zur Benachrichtigung betroffener Datensubjekten, wenn sie keine hinreichende Wahrscheinlichkeit eines Schadens für das betroffene Datensubjekt nachweisen können.
- **Daten-Lieferkettensicherheit:** Die gesamtschuldnerische Haftung wird im Rahmen der DSGVO vollstreckt, was bedeutet, dass Datenverantwortliche entlang der Daten-Lieferketten im Falle von Missbrauch oder Verletzung eventuellen Sanktionen ausgesetzt sind. Durch den Einsatz technischer Zusatzmaßnahmen wie Pseudonymisierung können Parteien entlang der Daten-Lieferketten ihr Risiko sowie ihre Gefährdung durch unsachgemäße Verarbeitung verringern.

Voraussetzungen für die gesetzlich vorgeschriebene Pseudonymisierung

Die gesetzlich vorgeschriebene Pseudonymisierung erfordert fünf Schlüsselelemente, wie in der vom EDSA endgültigen Fassung von Schrems II angegeben:

1. **Schutz aller Datenelemente:** Der Status der EU-DSGVO-Pseudonymisierung muss für einen Datensatz als Ganzes bewertet werden, nicht nur für bestimmte Bereiche. Das erfordert die Bewertung des Schutzniveaus für alle personenbezogenen Daten in einem Datensatz, einschließlich mehr als direkter Identifikatoren, und erstreckt sich auf indirekte Identifikatoren und Attribute.
2. **Schutz vor Singling-Out-Attacken ("Herausgreifen"):** Die endgültige Fassung von Schrems II der EDPB verlangt einen Schutz gegen das "Herausgreifen" eines Datensubjekts in einer größeren Gruppe, was die Verwendung von entweder k-Anonymität oder Aggregation obligatorisch macht.
3. **Dynamik:** Die gesetzlich vorgeschriebene Pseudonymisierung muss vor der Nutzung von Informationen aus verschiedenen Datensätzen zur erneuten Identifizierung von Datensubjekten schützen; dies erfordert die Verwendung unterschiedlicher Ersetzungstoken für unterschiedliche Zwecke zu unterschiedlichen Zeiten (d. h. Dynamik), um eine erneute Identifizierung durch den Einsatz von Korrelationen zwischen Datensätzen zu verhindern.
4. **Nicht-algorithmische Look-up-Tabellen:** Datenverantwortliche müssen die Vulnerabilität kryptografischer Techniken (insbesondere im Laufe der Zeit) für Brute-Force-Angriffe und das Risiko von Quantencomputing berücksichtigen, was die Verwendung von nicht-algorithmisch abgeleiteten Look-up-Tabellen erfordert; und
5. **Kontrollierte Wiederverknüpfbarkeit:** Die endgültige Fassung von Schrems II der EDPB stellt fest, dass neben anderen Anforderungen der Standard der EU-DSGVO-Pseudonymisierung nur dann erfüllt werden kann, wenn "ein Datenexporteur personenbezogene Daten so verarbeitet übermittelt, dass die personenbezogenen Daten nicht mehr einem bestimmten betroffenen Datensubjekt zugeordnet werden können, oder dazu verwendet werden können, um das betroffene Datensubjekt aus einer größeren Gruppe herausgreifen, ohne Verwendung zusätzlicher Informationen."

Schlussfolgerung

Die globale Datenverarbeitung erhöht die Risiken von Datenschutzverletzungen und -missbrauch. Gesetzlich vorgeschriebene Pseudonymisierung, die in immer mehr internationalen und US-amerikanischen Datenschutzgesetzen aufgenommen wird, hilft dabei, Datenschutzverletzungen zu verhindern, noch bevor diese auftreten. Darüber hinaus bietet es zahlreiche rechtliche und Geschäftskontinuitäts-Vorteile, Schutz vor Datenschutzverletzungen und reduzierte Meldepflichten bei ebensolchen. Aber - Unternehmen, Regierungen, nichtstaatliche Organisationen (NGOs) und andere Einrichtungen sollten die Anwendung technischer Kontrollen, welche die in der DSGVO definierten erhöhten Anforderungen an die gesetzliche Pseudonymisierung erfüllen können, sorgfältig prüfen.

© 2023 Anonos. All rights reserved.

Technical controls that protect data when in use and prevent misuse

Received: 3rd September, 2022

Magali (Maggie) Feys

Founder, AContrario.law, IP, IT & Data Protection Lawyer, Belgium

Magali (Maggie) Feys is founder of AContrario.Law, a boutique law firm based in Belgium, specialising in IP, IT, data protection and cybersecurity. In addition, Magali acts as a legal advisor to the Belgian Ministry of Health where she advises on privacy matters (such as e-health network, COVID-19 contact tracing and digital EU-COVID-certificate and the Covid Safe Ticket) and is a member of the legal working party e-Health of the Belgian Minister for Public Healthcare. Maggie also represents Anonos (www.anonos.com) as chief strategist of ethical data use.

AContrario.law, IP, IT & Data Protection Lawyer, Stapelplein 70, bus 104 — B.9000, Gent, Belgium
Tel: (+32) 474 29 61 25; E-mail: magali@acontrario.law

Joseph W. Swanson

Attorney at Law, Carlton Fields, USA

Joseph (Joe) Swanson chairs the cybersecurity and privacy practice at Carlton Fields, a full-service law firm with offices throughout the United States. Joe counsels clients on privacy compliance matters, breach investigation and response, and related litigation. Prior to joining Carlton Fields, Joe served as a federal cyber-prosecutor.

Carlton Fields, 4221 W. Boy Scout Blvd., Ste. 1000, Tampa, FL, 33607-5780, USA
Tel: (+1) 813 229.4335, Fax: 1.813.229.4133; E-mail: jswanson@carltonfields.com

Patricia M. Carreiro

Attorney at Law, Carlton Fields, USA

Patricia (Trish) Carreiro (CIPP/US, CIPM) is a privacy and cybersecurity attorney at Carlton Fields and co-chair of the International Association of Privacy Professional's South Florida chapter. She counsels clients of all sizes on privacy and cybersecurity compliance with an emphasis on retail and highly regulated industries.

Carlton Fields, 2 Miami Central, 700 NW 1st Avenue, Ste. 1200, Miami, FL 33136-4118, USA
Tel: (+1) 305 539 7314, Fax: 1.305.530.0055; E-mail: pcarreiro@carltonfields.com

Gary LaFever

Co-CEO and General Counsel, Anonos, USA

Gary LaFever is Co-CEO and General Counsel at Anonos, Global Innovator at the World Economic Forum, former partner at the law firm Hogan Lovells, and former Management Information Consultant at Accenture. Gary's 35+ years of technical and legal expertise enables him to approach data protection and utility issues from both perspectives. He is a co-inventor of 35+ granted patents and 80+ additional patent assets internationally.

Anonos Inc., 9450 SW Gemini Drive, Suite 96049, Beaverton, OR 97008, USA
Tel: (+1) 303 389 5759; E-mail: gary.lafever@anonos.com

Abstract Global data processing flowing across geographic borders and increasing risks of external data breach and misuse beyond lawful purposes requires careful evaluation of technical controls that prevent privacy violations before they occur. This paper details the specific requirements for, and certain benefits from, implementing technical controls satisfying the heightened requirements for statutory pseudonymisation as defined in the General Data Protection Regulation (GDPR) in the context of (i) surveillance-proof processing, (ii) lawfulness of processing, (iii) more secure processing and (iv) data supply chain defensibility. The interconnectedness of these issues is presented within the confluence of conflicting interests among four different groups: governments, courts, enforcement agencies and non-governmental organisations (NGOs).

KEYWORDS: pseudonymisation, international data transfer, cloud, data breach, analytics, artificial intelligence (AI), machine learning (ML)

INTRODUCTION

Companies, organisations and governments desiring to lawfully and ethically process global data that includes EU[1] personal data should evaluate the merits and benefits of implementing 'statutory pseudonymisation'[2] as a safeguard for protecting data when in use and preventing misuse. As outlined in this paper, effective technologically enforced controls like EU General Data Protection Regulation (GDPR)-compliant pseudonymisation help companies, organisations and governments to leverage:

a) economies of scale provided by cloud-based Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings delivered via networks of global subcontractors and cloud processors; and
b) artificial intelligence (AI), machine learning (ML), advanced analytics and other capabilities outside the scope of what they can accomplish using internal resources alone by leveraging services offered by third parties as cloud-based Software as a Service (SaaS) offerings.

EU GDPR-compliant pseudonymisation technology is:

a) recommended by the European Data Protection Board (EDPB)[3] for Schrems II[4]-compliant lawful cloud AI, ML and analytics of EU personal data;
b) highlighted as an EU GDPR-compliant safeguard for helping to ensure the compatibility and lawfulness of AI, ML and analytics beyond the scope of processing authorised by Consent and Contract;[5] and
c) recognised as 'tipping the balance in favour of the controller' to help support 'Legitimate Interest processing' under the EU GDPR.[6]

OBJECTIVES AND PERSPECTIVES

Companies, organisations and governments should implement safeguards such as the following to help ensure that IaaS, PaaS and SaaS processing are secure in environments which are beyond the exclusive control of the data controller — ie 'untrusted environments':[7]

- *Surveillance-proof processing* to enable lawful international data transfers and processing leveraging technical supplementary measures to protect the identity of EU data subjects without access to additional information held separately by the data controller.[8]
- *Lawfulness of processing* to support desired processing without violating the rights of data subjects.[9]

- *Breach-resistant processing* to reduce the risk from external attacks or internal misuse of data by obscuring identifying elements of personal data (while making the protected form of data available for processing capable of achieving data processing purposes) without access to additional information held separately by the data controller.[10]
- *Data supply chain defensibility* to ensure that parties up and down data supply chains are not subject to joint and several liability for the failure of other participants to process personal data in compliance with the preceding safeguards.[11]

The demand for technical controls that help to protect EU personal data when in use and prevent misuse does not originate from any one group. Rather, the growing demand comes from at least four groups, and the confluence of the interests of these different groups makes the current situation irreversible. *The common theme across the interests and perspectives of these groups is that technological controls are now critically important*. These groups comprise the following:

- *EU and US governments*: In recognition of the significant changes involved, when the EU GDPR was initially passed, all parties were given two years to comply (the EU GDPR was passed in May 2016 with an effective date in May 2018). It was a surprise to legislators (and regulators) that so much work had to be done for organisations even to begin to start to comply (eg doing inventories of their data — where it came from, where it was being stored vs processed, what rights they had and how they were documented, etc). As a result, six years after the initial passage of the EU GDPR, many companies are just now arriving at the point where they have completed the groundwork required to start implementing technology that reconciles data utility and compliance. As much as both EU and US governments would like to put a new treaty in place to ensure ongoing trans-Atlantic commerce, governments will not abandon surveillance activities they deem critical for national security. The complexity of the situation and the disparity of stakeholder interests mean that the current situation is not reconcilable by 'words alone' — regardless of whether the words are contained in contracts, policies, procedures or treaties — and requires effective technologically enforced controls.[12]
- *Courts*: The fundamentally different approaches to privacy between the EU and the USA are increasingly evident in decisions by the most senior courts in each jurisdiction (ie the Court of Justice of the European Union [CJEU] and the US Supreme Court). These decisions cannot be ignored or (easily) reversed by the other stakeholder groups. For example, the Schrems II decision by the CJEU[13] that EU personal data cannot be processed in cleartext in US-operated clouds without an assessment of whether there is adequate protection and whether Standard Contractual Clauses (SCC) require technical supplemental measures to prevent likely surveillance by third-country governments, as well as the CJEU ruling that protections must exist against the revelation of EU Special Category Data via analysis and deduction and not just immediate disclosure,[14] are binding on all parties on both sides of the Atlantic. By contrast, recent decisions by the US Supreme Court (eg related to FBI surveillance[15] and, more recently, the privacy rights of women in reproduction-related situations[16]) highlight the fundamental differences in philosophy and law when it comes to privacy between Europe and the USA. Technical controls can help to bridge these otherwise irreconcilable differences; words in a treaty are completely inadequate.

- *Enforcement agencies*: EU regulators were slow to enforce many EU GDPR requirements because of the widespread lack of fundamentals necessary to comply. Enforcement action across the EU has taken time to gather pace and for the authorities to exercise the full range of their powers. More recently, EU enforcement actions against companies of all sizes and nationalities are increasing. Examples include, enforcement actions related to the use of Google Analytics[17] by entities of various sizes and the use of customer prospecting lists.[18] Additionally, in the USA, enforcement under new, more stringent state privacy laws has begun.[19] These enforcement actions also highlight the increasing importance of technologically enforced controls.
- *Non-governmental organisations (NGOs)*: these groups have increasingly greater visibility and impact. For example, Max Schrems and his organisation NOYB successfully initiated the legal actions that invalidated the Privacy Shield trans-Atlantic treaty and its predecessor Safe Harbor treaty and more recently are behind the 101 complaints filed against the use of Google Analytics.[20] Note that this is before the effectiveness of changes in 2023 that authorise class action lawsuits or collective redress across Europe.[21] Moreover, coordinated actions against global companies involving NGOs teaming up across the Atlantic are also on the rise.[22] Activities by these NGOs again highlight the increasing importance of technologically enforced controls.

SURVEILLANCE-PROOF PROCESSING

Given the interconnected nature of international data flows, and the exposure represented by sub-processor and cloud processing, governments, organisations and companies should consider the merits and benefits of following South Korea (the Republic of Korea) in adopting strong requirements for statutory pseudonymisation that helped secure EU adequacy determination.[23]

The processing of EU personal data outside of the European Economic Area (EEA)[24] and adequacy countries requires compliance with Schrems II requirements promulgated by the CJEU and the EDPB,[25] including the use of technical controls as supplementary measures when an assessment of whether there is adequate protection reveals that SCCs together with organisational and contractual supplementary measures cannot prevent likely surveillance by third-country governments.[26] These obligations extend to onward transfers and processing by sub-processors, with respect to which the EDPB specifically highlights concerns since 'a large variety of computing solutions may imply the transfer of personal data to a third country (eg for storage or maintenance purposes)'.[27] A decision by the German Baden-Württemberg *Vergabekammer*, which judges compliance with the requirements for public tender dossiers, ruled on 13th July, 2022 that even the risk of onward processing by sub-processors using US-managed cloud infrastructure is equivalent to an actual transfer of personal data requiring compliance with the EU GDPR.[28] While the Karlsruhe Higher Regional Court later reversed the decision of the Baden-Württemberg procurement chamber, its ruling acknowledging contractual commitments by Amazon Web Services EMEA SARL to restrict processing to the EU, failed to address the impact of requests by the parent company Amazon Web Services, Inc. to provide data in response to FISA, EO 12333 or US Cloud Act requests. In addition, a 26th July, 2022 Dutch Ministry of Justice and Security (NCSC) legal memorandum stresses that the reach of government surveillance extends to data processed internationally by sub-contractors and cloud processors.[29] As a result, global enterprises that leverage

non-EEA (eg US) managed infrastructure (eg public cloud, multiparty data sharing and analytics) to process EU personal data will be subject to similar scrutiny.

It should be noted that in addition to the EDPB, the heightened EU GDPR requirements of pseudonymisation have been recognised by the European Data Protection Supervisor (EDPS)[30] as a viable means of enabling the lawful transfer of personal data to third countries not offering an equivalent level of protection. As noted by European Data Protection Supervisor, Wojciech Wiewiórowski, in an EDPS webinar titled *Pseudonymous Data: Processing Personal Data While Mitigating Risks*:

> Our legal data protection rules in the European Union and particularly GDPR itself considered pseudonymisation as a sort of model of all risk mitigating measures. This comes only after the first of all obligations, if you do not need the personal data do not process them. But if you need the personal data, then GDPR refers to pseudonymisation when it takes exemplifying the appropriate safeguards in many circumstances.[31]

LAWFULNESS OF PROCESSING

Legitimate Interest processing

Article 6 of the EU GDPR provides six legal grounds for processing personal data for which there is no statutory preference or sequence of application.[32] This is highly relevant because if Consent under Article 6(1)(a) was the only basis upon which information could be processed, controllers and processors would often face a 'Hobson's choice'[33] between: (a) securing 'uninformed consent'; and (b) not processing data for valuable complex research (health, scientific, marketing or otherwise) purposes because of the complexity of explaining what is happening behind the scenes so that data subjects can fully understand.

The difficulty of successfully using either Consent[34] or Contract[35] to enable EU GDPR-compliant AI, ML, and advanced analytics, was highlighted by (i) the near billion-dollar fine levied by the Luxembourg Data Protection Authority in July 2021 against Amazon[36] for improper processing of Amazon's own first-party data under the EU GDPR, and (ii) the ruling by the Belgian Data Protection Authority that IAB Europe's self-styled Transparency and Consent Framework (TCF) — relied upon by Google and many other advertisers for targeted advertising — violates the EU GDPR.[37]

The limitations of Consent and Contract in complex processing situations is one of the reasons that Legitimate Interests[38] exists as an alternate legal basis. The EDPB notes that the Legitimate Interests legal basis[39] requires a controller to satisfy all three conditions:[40]

1. *Legitimate purpose*: the identification and qualification of a legitimate purpose pursued by the controller or by a third party. This interest of the controller or third party may be broader than the purpose of the processing but must be present at the processing date.[41]
2. *Necessity*: the need to process the personal data must be established as a requirement for the legitimate interest pursued.[42]
3. *Balancing of interests*: the legitimate interest of the controller or third party must be balanced against the interests or fundamental rights and freedoms of the data subject, including the data subject's rights to data protection and privacy, considering the particular circumstances of the processing.[43]

The Purpose, Necessity and Balancing tests must *all* be satisfied, and 'high marks' in one or more tests does *not* overcome the failure to satisfy other tests.[44]

As a result, attempts to use Legitimate Interests processing for data uses that violate the EU GDPR, including Article 5 (Principles Relating to Processing of

Personal Data), such as discrimination against protected categories of individuals, illegally influencing the results of elections, etc will fail the first test. These data uses would not be lawful under Legitimate Interests grounds regardless of the outcomes of the Necessity and Balancing tests.

If a proposed data use satisfies both the Purpose and Necessity tests, then the Balancing test must be applied to assess the impact of the intended processing on the interests or fundamental rights and freedoms of data subjects. In performing the assessment of relevant 'impact', the Article 29 Working Party has stated that:

> The Working Party emphasises that it is crucial to understand that relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of the data processing. For the sake of clarity, we also emphasise that the concept is unrelated to the notion of data breach and is much broader than impacts that may result from a data breach. Instead, the notion of impact, as used here, encompasses the various ways in which an individual may be affected — positively or negatively — by the processing of his or her personal data.[45]

The need to assess the collective interests at stake on both sides of the balancing of interests test — ie the interest of the data controller (or a third party) and the interests of the data subject — are affirmed in opinions of the EDPB (including its predecessor Article 29 Working Party) and decisions of the CJEU. Citing the CJEU rulings in Google Spain and 'Schrems I',[46] Lokke Moerel and Corien Prins highlight in *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*, that 'the clear signal is that collective interests must also be involved in these considerations. Only then can full account be taken of the constitutional basis for personal data protection at the EU level.'

Under EU GDPR Article 6(4), personal data collected and processed for a stated purpose based on Legitimate Interests, a contract, or vital interests — ie *not based on consent — may be further processed* for another purpose if the new purpose is compatible with the original purpose. The European Commission in its guidance — *Can we use data for another purpose?* — highlights the following points (as stated in the EU GDPR) as being relevant for determining whether a new purpose is compatible with the original purpose:[47]

- the link between the original purpose and the new/upcoming purpose;
- the context in which the data was collected (what is the relationship between a data controller and the individual?);
- the type and nature of the data (is it sensitive?);
- the possible consequences of the intended further processing (how will it impact the individual?); and
- the existence of appropriate safeguards (such as encryption or *pseudonymisation*).

They also note that if a data controller wants to use the data for statistical or scientific research 'it is not necessary to run the compatibility test'.

Furthermore, the European Commission guidance[48] highlights that if a data controller has collected the data 'on the basis of consent or following a legal requirement, no further processing beyond what is covered by the original consent or the provisions of the law is possible'. In these instances, 'further processing would require obtaining new consent or a new legal basis'.

This underscores the 'Hobson's choice' noted above: if the processing is too complex to be explained simply (or too complicated to comprehend, but data

subjects consent anyway) then either the processing cannot be allowed at all (with the attendant loss of societal benefits) or a non-consent legal basis must, in practice, actually be available for use.

As described more fully below, the combination of EU GDPR-compliant Data Protection by Design and by Default and EU GDPR-compliant pseudonymisation can enable lawful and trusted personalisation leveraging complex data analysis, machine learning, AI, sharing, combining and enriching not otherwise supportable using consent or contract.

Data Protection by Design and by Default

Data Protection by Design and by Default, as newly defined under EU GDPR Article 25, goes beyond Privacy by Design.[49] The EU GDPR requires that Data Protection by Design and by Default be applied as far 'upstream' in processing as possible (eg by 'pseudonymising data at the earliest opportunity') to limit data use to the minimum extent and time necessary to support each specific product or service authorised by an individual data subject.[50] This is a more stringent standard than basic Privacy by Design, which can be satisfied by 'considering data protection and privacy issues upfront in everything you do'.

Encryption and traditional Privacy Enhancing Techniques (PETs) were developed long before the EU GDPR requirements were established. Because of their limitations in protecting data during computation and analysis ('protection in use'), when used alone, encryption and traditional PETs will likely fail to satisfy new EU GDPR Data Protection by Design and by Default requirements.

For example, persistent tokens and identifiers used for marketing purposes such as the Google Advertising ID (ADID) and the Apple Identifier for Advertising (IDFA) may fall short of requirements for Data Protection by Design and by Default because links between data subjects and identifying information are readily ascertainable.

As noted in the recent decisions regarding the unlawfulness of Google Analytics,[51] EU supervisory authorities are increasingly finding that persistent tokens and identifiers generally used in the industry fail to satisfy EU GDPR Data Protection by Design and by Default requirements because of the risk of unauthorised re-identification via the Mosaic Effect. The Mosaic Effect occurs when a person is indirectly identifiable via linkage attacks because information can be combined with other pieces of information, enabling the individual to be distinguished from others.[52] These static tokens and identifiers do not satisfy the requirements for EU GDPR-compliant pseudonymisation set forth below because personal data can be attributed to specific data subjects without the use of separately kept 'additional information'. This means that the benefits enumerated herein associated with properly EU GDPR-compliant pseudonymised data will not be available under the EU GDPR.

Requirements for EU GDPR-compliant pseudonymisation

The EU GDPR provides incentives to use technical and organisational measures, including pseudonymisation, to enable the flow, commercial use and value maximisation of data in a way that recognises, respects and enforces the fundamental rights of individuals while allowing for the benefits to society from the commercial use of data. The heightened standards for EU GDPR-compliant pseudonymisation (relative to the narrower historical use of the term) were most recently affirmed by the EDPB[53] and the European Commission (EC)[54] in the context of the Schrems II ruling by the CJEU.

Pseudonymisation was previously understood to generally refer to replacing direct identifiers with tokens for individual fields independently within a dataset. Under the EDPB Final Schrems II Guidance and the Final SCCs, it is clear that EU GDPR-compliant pseudonymisation requires all of the following:

- *Protecting all data elements*: Footnotes 83 and 84 of the EDPB Final Schrems II Guidance highlight that achieving EU GDPR pseudonymisation status must be evaluated for a dataset as a whole, not just particular fields. This requires assessing the degree of protection for all data elements in a dataset, including more than direct identifiers, and extending to indirect identifiers and attributes. This is underscored by the definition of 'Personal Data' under EU GDPR Article 4(1) as more than immediately identifying information and extending to any information relating to an identified or identifiable natural person ('data subject'); 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.
- *Protecting against singling out attacks*: Paragraph 85 of the EDPB Final Schrems II Guidance requires protection against 'singling out' of a data subject in a larger group effectively making the use of either k-anonymity or aggregation mandatory.
- *Dynamism*: complying with the requirements in Paragraphs 79, 85, 86, 87 and 88 of the EDPB Final Schrems II Guidance to protect against the use of information from different datasets to re-identify data subjects necessitates the use of different replacement tokens for differing purposes at different times (ie dynamism) to prevent re-identification by leveraging correlations among datasets without needing access to the 'additional information held separately' by the EU data controller (see https://www.MosaicEffect.com);
- *Non-algorithmic lookup tables*: the requirement of Paragraph 89 of the EDPB Final Schrems II Guidance to consider the vulnerability of cryptographic techniques (particularly over time) to brute force attacks and quantum computing risk will necessitate the use of non-algorithmic derived look-up tables in many instances; and
- *Controlled re-linkability*: The combination of the four preceding items are necessary to meet the requirement in Paragraph 85(1) of the EDPB Final Schrems II Guidance that, along with other requirements, the standard of EU GDPR pseudonymisation can be met only if 'a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information'.

Contract vs Consent vs Anonymisation vs Legitimate Interest processing

The following graphic and accompanying narrative highlight the differences in the capability of contract, consent and anonymisation versus EU GDPR pseudonymisation-enabled Legitimate Interest processing to support repurposing of data for secondary processing, including personalisation, in the context of the sale of a trip via a website. While a controller could initially decide to rely on legitimate interests, the diagram highlights that contract, consent and anonymisation face severe limitations in their ability to support the desired use case (Figure 1).

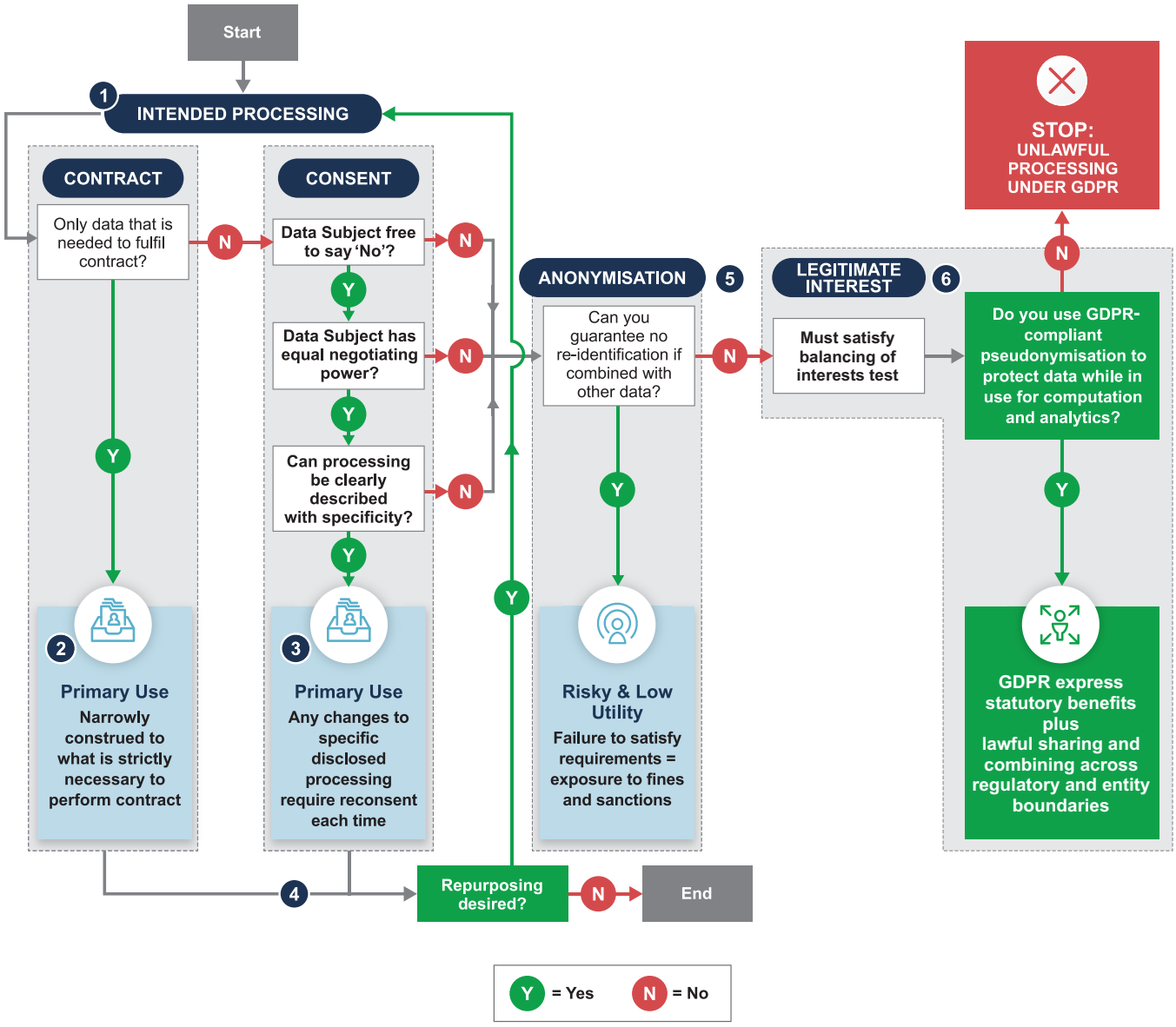


Figure 1: EU GDPR pseudonymisation enables Legitimate Interest-based personalisation

Marketing example

Number references below correspond to number references in Figure 1.

1. Examples of Intended Purposes
   - Sell a trip via website (flight, hotel, etc)
   - Save preferences for future bookings
   - Market analytics to offer personalised future trips via email
2. Under Contract
   - Can sell initial trip, but cannot (a) save for future bookings or (b) market for future trips
3. Under Consent
   - Can save preferences for future bookings
   - Works only for marketing analytics disclosed with specificity at time of initial data collection

4. New marketing is (a) secondary repurposing under Contract and (b) fails requirements of advanced specificity for Consent and thus '[f]urther processing would require obtaining new consent or a new legal basis'.
5. Due to the details of the data collected and the need to retain indirect identifiers and attributes unprotected for desired analytics, the requirements for anonymisation under the EU GDPR are not satisfied.[55]
6. Legitimate Interest is the remaining applicable option for a legal basis for marketing analytics. EU GDPR pseudonymisation provides protection for data while in-use for computation and analytics to help tip the balance in favour of processing by the data controller.[56]

BENEFITS OF PSEUDONYMISATION FROM A SECURITY COMPLIANCE STANDPOINT

In addition to the foregoing benefits, pseudonymisation can both be a tool in a company's data protection toolkit, while also potentially reducing a company's reporting obligations and liability if the personal data they hold is compromised.

The EU GDPR repeatedly endorses pseudonymisation. EU GDPR Article 25(1) obligates parties to 'implement appropriate technical and organisational measures, such as pseudonymisation', and Article 25(2) obligates parties to 'implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed'.[57] EU GDPR Recital 78 uses 'pseudonymising data as soon as possible' as an example of such a measure. EU GDPR Article 32 explicitly recognises pseudonymisation and encryption as measures to be considered when:

> taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.[58]

Likewise, in the US, state and federal laws and regulations, both comprehensive and industry-specific, require organisations to implement reasonable security measures to safeguard personal data. Examples include:

- New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act);[59]
- Massachusetts's 201 CMR 17.00; and
- HIPAA's Security Rule.[60]

California even provides consumers with a private right of action and statutory damages of between $100 and $750 'per consumer per incident or actual damages, whichever is greater' if their personal information is subject to 'unauthorized access and exfiltration, theft, or disclosure' resulting from a business's failure to 'implement and maintain reasonable security procedures and practices appropriate to the nature of the information'.[61]

Pseudonymisation can be a powerful tool for satisfying these requirements because it can allow companies to protect personal data without rendering that data unusable. Further, pseudonymisation may even allow organisations to exempt certain data from the reach of various privacy laws. For example, pseudonymisation could potentially be used as a means of statutory deidentification, which would largely remove an organisation's HIPAA obligations related to that data.

Pseudonymisation may also significantly reduce the burden and costs stemming from incidents that involve the compromise of personal data. In the EU, pseudonymisation

may mean that a data incident is 'unlikely to result in a risk to the rights and freedoms of natural persons', and thus not a data breach which would otherwise require notification to a supervisory authority under GDPR Article 33 and data subjects under Article 34.

Similarly in the US, many federal and state breach notification laws exempt victim organisations from notification requirements when there is no reasonable likelihood of harm to the affected individuals or where the compromised data is unusable. HIPAA, for example, requires covered entities to notify patients when their unsecured protected health information ('PHI') is impermissibly used or disclosed *unless* the covered entity demonstrates that there is a 'low probability' that the PHI has been compromised.[62] As part of any risk assessment performed pursuant to HIPAA, pseudonymisation could help establish this 'low probability'.

Likewise, state breach notification laws often define encrypted or 'otherwise unusable' data as not requiring breach notification to either regulators or affected individuals. Florida's data breach statute, for example, mandates notification in instances of a breach of personal information, but explicitly excludes information that is 'encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable'.[63] Pseudonymisation can thus significantly reduce the breach notification obligations of organisations.

Finally, in the event of a regulatory investigation or litigation filed in the wake of a data security incident, the fact that the personal data was pseudonymised would be an important fact against liability but also could stem any claimed damages from that incident.

DATA SUPPLY CHAIN DEFENSIBILITY

Articles 28 and 29 of the GDPR obligate data controllers to ensure the lawful processing of personal data throughout their data supply chain. Article 28(1) specifically requires that:

> the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

GDPR Articles 26 and 82 set forth the principle of joint and several liability, pursuant to which any division of liability among parties in a data supply chain is unenforceable against claims by data subjects. As a result, each participant in a data supply chain, regardless of whether they are a controller, joint controller or processor, is obligated to indemnify data subjects for damages as a whole; only after providing full relief to data subjects are they then entitled to seek relief from other actors in the data supply chain who contributed to the damage.

As a result, companies, organisations and governments are increasingly demanding Schrems II compliant technical supplementary measures (like EU GDPR pseudonymisation) from fellow data supply chain participants to reduce the risk and exposure from improper processing by other parties with whom they share and process data. Data is an incredibly valuable resource for company performance and innovation, and without data flowing freely, critical opportunities for growth and revenue may be lost.

Business continuity risks arising from the inability to process data are more significant than the monetary risk from penalties or non-monetary risks from damaged reputation from privacy or security breaches. The CJEU Schrems II ruling notes five times the preference for injunctive relief for failing to comply with international data transfer requirements.[64] See the *National Law*

Review article discussing a 12-hour notice to terminate processing sent by the Portuguese data protection authority to a Portuguese agency relying on SCCs.[65] See also the PwC article highlighting that 52 per cent of Fortune 500 companies now include privacy risk disclosures in their annual reports due to auditing considerations regarding an entity's ability to continue as a going concern.[66] Most recently, the European Commission clarified the joint and several liability of data controllers and processors in Clauses 3 and 12 of its new SCCs.[67] These issues related to data supply chain risk and exposure highlight the need for technologically enforced controls that data when in use and prevent misuse.

CONCLUSION AND RECOMMENDATION

Global data processing flowing across geographic borders and increasing risks of external data breach and misuse beyond lawful purposes require careful evaluation of technical controls that prevent privacy violations before they occur. Statutory pseudonymisation, adopted under an increasing number of global (eg EU, UK, Japan and South Korea) and US state privacy laws (eg California, Virginia and Colorado), helps to prevent privacy violations before they happen. As a result, companies, governments, NGOs and other entities should carefully evaluate the merits and benefits of implementing technical controls satisfying the heightened requirements for statutory pseudonymisation defined in the GDPR.

References

1. The countries comprising the European Union (EU) are Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.
2. The term 'statutory pseudonymisation' refers to statutorily recognised heightened standards for de-identification as more fully described under the laws of *the EU and the UK*, Article 4(5) of the EU and UK GDPR:

> pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person,

and the data protection laws of *Brazil*, Article 13(4) of General Data Protection Law (LGPD):

> For purposes of this article, pseudonymization is the processing by means of which data can no longer be directly or indirectly associated with an individual, except by using additional information kept separately by the controller in a controlled and secure environment;

Japan, Article 2.9 of Act on the Protection of Personal Information (APPI):

> 'Anonymously processed information' in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information. (i) Personal information falling under paragraph (1), item (i); Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of descriptions etc. with other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.). (ii) Personal information falling under paragraph (1), item (ii); Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions etc. using a method with no regularity that can restore the said personal identification codes);

South Korea, Article 2(i-2) of Personal Information Protect Act (PIPA):

> Pseudonymisation is 'the processing of personal data in such a manner that a specific individual becomes not identifiable without the use of additional information, rendered by removing a part of the data, replacing all or a part of the data, etc.'

and five US states — *California*, Article 1798.140(r) of California Consumer Privacy Act (CCPA):

> 'Pseudonymize' or 'Pseudonymization' means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

Colorado, Article 6-1-1303(22) of Colorado Privacy Act (CPA):

> 'Pseudonymous Data' means personal data that can no longer be attributed to a specific individual without the use of additional information if the additional information is kept separately and is subject to technical and organizational measures to ensure that the person data are not attributed to a specific individual;

Virginia, Article 59.1–571 of Virginia Consumer Data Protection Act (VCDPA)

> 'Pseudonymous data' means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

Utah, Article 160.103.171(28) of Utah Consumer Privacy Act (UCPA):

> 'Pseudonymous data' means personal data that cannot be attributed to a specific individual without the use of additional information, if the additional information is: (a) kept separate from the consumer's personal data; and (b) subject to appropriate technical and organizational measures to ensure that the personal data are not attributable to an identified individual or an identifiable individual;

and *Connecticut*, Article 1(24) of Connecticut Data Privacy Act (CTDPA):

> 'Pseudonymous data' means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

See also *Is Canada's Proposed Consumer Privacy Protection Act Too High Risk Compared to E.U. Data Protection Law?*, available at https://www.linkedin.com/pulse/canadas-proposed-consumer-privacy-protection-act-too-high-magali-feys/ (accessed 20th November, 2022).

3. See 'Use Case 2: Transfer of Pseudonymised Data' at paragraphs 85 through 89 of EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data Version 2.0 on 18 July, 2021, available at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (accessed 20th November, 2022; hereinafter referred to as the 'EDPB Final Schrems II Guidance').
4. 'Schrems II' refers to the Judgment of the Court of Justice of 16th July, 2020, Data Protection Commissioner *v*. Facebook Ireland Limited and Maximillian Schrems, C-311/18, related to protection of EU personal data in the context of US national security intelligence gathering frameworks, including Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (EO 12333), available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en (accessed 20th November, 2022).
5. See EU GDPR Article 6(4)(e).
6. See pages 42 and 67 of *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller*, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (accessed 20th November, 2022).
7. Gartner refers to this as privacy-enhancing computation (PEC) — ie protecting data when in use in untrusted environments. Gartner highlights the use of public cloud, multiparty data sharing and analytics as untrusted environments, notwithstanding that such processing is increasingly foundational to the success of organisations. See *Gartner Identifies Top Five Trends in Privacy Through 2024*, available at https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024 (accessed 20th November, 2022).
8. See EDPB Final Schrems II Guidance, note 6 above; see also *Application of the CLOUD Act to EU Entities*, available at https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/augustus/16/memo-cloud-act/Cloud+Act+Memo+Final.pdf (accessed 20th November, 2022).
9. See 'Lawfulness of Processing' section and text accompanying Notes 32–56.
10. The same technical controls that enable surveillance-proof international data transfers reduce the surface area for attack by bad actors — both internal and external — behind an organisation's firewall. When breached, the majority of data that would otherwise be available for misuse or attack is protected by

cryptographic controls (encryption when at rest and in transit and statutory pseudonymisation when in use) and does not reveal identifying information. Access to the keys necessary to re-identify cryptographically protected data is sequestered to separately authorised personnel for limited secure processing for permitted purposes only. These additional technical and organisational supplementary measures increase the security of the data and reduce exposure and liability upon external breach or internal misuse. See EU GDPR Articles 25 and 32 (accessed 20th November, 2022).

11. See Clauses 3 and 12 of Final EU Commission SCCs, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN (accessed 20th November, 2022).
12. See *Why Words Alone Cannot Comply with Schrems II*, available at https://www.anonos.com/why-words-alone-cannot-comply-with-schremsii (accessed 20th November, 2022).
13. See *Assessing the Implications of Schrems II for EU–US Data Flow*, available at https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/assessing-the-implications-of-schrems-ii-for-euus-data-flow/71E5412185BA0AE59B9F1AE1CFB6B97B (accessed 20th November, 2022).
14. See Case 184/20 (OT v Vyriausioji tarnybinės etikos komisija), available at https://curia.europa.eu/juris/document/document.jsf;jsessionid=E7212ECF38E8EAB7DBC2AB443FD6B4C1?text=&docid=263721&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2255189 (accessed 20th November, 2022).
15. See *The Supreme Court Just Made a US-EU Privacy Shield Agreement Even Harder*, available at https://thehill.com/opinion/judiciary/598899-the-supreme-court-just-made-a-us-eu-privacy-shield-agreement-even-harder/ (accessed 20th November, 2022).
16. See *Roe v. Wade Reversal Sends Ripples through Privacy World*, available at https://iapp.org/news/a/roe-v-wade-reversal-sends-ripples-through-privacy-world/ (accessed 20th November, 2022).
17. See *French and Italian Data Protection Authorities Take Issue with Google Analytics: Analysis and Key Takeaways*, available at https://www.orrick.com/en/Insights/2022/07/French-and-Italian-Data-Protection-Authorities-Take-Issue-with-Google-Analytics (accessed 20th November, 2022).
18. See *Commercial Prospecting and Rights of Individuals: ACCOR Fined 600,000 Euros*, available at https://www.cnil.fr/en/commercial-prospecting-and-rights-individuals-accor-fined-600000-euros (accessed 20th November, 2022).
19. See *California Attorney General Announces First CCPA Enforcement Action*, available at https://iapp.org/news/a/california-attorney-general-announces-first-ccpa-enforcement-action/ (accessed 20th November, 2022).
20. See *101 Complaints on EU-US Transfers Filed* at https://noyb.eu/en/101-complaints-eu-us-transfers-filed, see also, *101 . . . Not Dalmatians, But Tracking Technologies Related Complaints: Highlights On Recent Case-Law*, available at https://www.lexology.com/library/detail.aspx?g=e3da9b72-2dd9-498d-8bd4-dc58b3221936 (accessed 20th November, 2022).
21. See *Class Actions to Reshape the Litigation Landscape in Europe in 2023*, available at https://www.gibsondunn.com/class-actions-to-reshape-the-litigation-landscape-in-europe-in-2023/ (accessed 20th November, 2022).
22. See *Oracle's 'Surveillance Machine' Targeted in US Privacy Class Action*, available at https://techcrunch.com/2022/08/22/oracle-us-privacy-class-action/ (accessed 20th November, 2022).
23. See §17, 27, 36, 42, 44, 45, 46, 47 and 48, as well as footnote 24 of the Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act, available at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf (accessed 20th November, 2022). See also *Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act")*, available at https://ag.ny.gov/internet/data-breach and 45 C.F.R. Parts 160 and 164, available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (accessed 20th November, 2022).
24. In addition to the EU member states, the EEA also includes Iceland, Liechtenstein and Norway.
25. See EDPB Final Schrems II Guidance, note 5 above.
26. *Ibid*. at paragraph 53.
27. See Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems Adopted on 23rd July, 2020, FAQ #11, available at https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf (accessed 20th November, 2022).
28. See *Baden-Württemberg Procurement Chamber Decides US Cloud Services are Not GDPR Compliant*, available at https://nextcloud.com/blog/baden-wurttemberg-procurement-chamber-decides-us-cloud-services-are-not-gdpr-compliant/ (accessed 20th November, 2022).
29. See the last paragraph of 26th July, 2022 NCSC legal memorandum (p. 15) highlighting that the reach of the CLOUD Act extends to data processed via sub-contractors and cloud processors, available at https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/augustus/16/memo-cloud-act/Cloud+Act+Memo+Final.pdf (accessed 20th November, 2022).
30. In a December 2021 EDPS webinar, Thomas Zerdick, Head of Technology and Privacy at the EDPS, stated that: 'After the Schrems II ruling, the debate on pseudonymisation has gained momentum as many consider it as the most viable "supplementary measure" to transfer personal data to third countries not offering an equivalent level of protection.' Available at https://edps.europa.eu/

press-publications/press-news/videos/ipen-2021-pseudonymous-data-introduction-thomas-zerdick_en (accessed 20th November, 2022).
31. See *IPEN 2021 on Pseudonymous Data*, available at https://edps.europa.eu/press-publications/press-news/videos/ipen-2021-pseudonymous-data-keynote-speech-wojciech_en at 4:06 (accessed 20th November, 2022).
32. Article 6(1) of the EU GDPR provides the following six lawful bases for processing EU personal data: (a) consent; (b) contract; (c) legal obligations; (d) vital interests of the data subject; (e) public interest; or (f) legitimate interests pursued by the data controller.
33. See https://www.merriam-webster.com/dictionary/Hobson%27s%20choice (accessed 20th November, 2022).
34. See GDPR Article 6(1)(a).
35. *Ibid*., Article 6(1)(b).
36. See *Amazon Gets Record $888 Million EU Fine Over Data Violations*, available at https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach#xj4y7vzkg (accessed 20th November, 2022).
37. See *Belgian DPA Fines IAB Europe Over Consent Framework GDPR Violations*, available at https://iapp.org/news/a/belgian-dpa-fines-iab-europe-250k-euros-over-consent-framework-gdpr-violations/ (accessed 20th November, 2022).
38. See GDPR Article 6(1)(f).
39. See Article 29 Working Party Opinion on the Notion of Legitimate Interest of the Data Controller Under Article 7 of Directive 95/46/EC, currently under revision by the EDPB (see the EDPB Work program 2021/2022 adopted on 16th March, 2021, available at https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf) (accessed 20th November, 2022).
40. See EDPB Recommendations 02/2021 on p. 3, citing the CJEU judgment of 4th May, 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme', Case C-13/16, ECLI:EU:C:2017:336.
41. *Ibid*., citing CJEU judgment of 11th December, 2019, TK v Asociația de Proprietari bloc M5A-ScaraA, Case C-708/18, ECLI:EU:C:2019:1064.
42. *Ibid*.
43. *Ibid*., citing CJEU judgment of 24th November, 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v, Administración del Estado, Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, points 47 and 48; CJEU judgment of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779.
44. See EDPB Recommendations 02/2021, note 40 above.
45. See *Article 29 Working Party 06/2014*, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf at 35 (accessed 20th November, 2022).
46. See Lokke Moerel and Corien Prins, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123, citing Case C-131/12 Google Spain and Google Inc. May 13, 2014, EU:C:2014:317; Case C-362/14, Schrems, October 6, 2014, EU:C:2015:650; Opinion WP29 06/2014 (accessed 20th November, 2022).
47. See European Commission *Can We Use Data for Another Purpose?*, available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en (accessed 20th November, 2022).
48. *Ibid*.
49. Privacy by Design is the approach championed by Ann Cavoukian, Ph.D., former Information and Privacy Commissioner of Ontario, for embedding privacy into the system design process. See https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (accessed 20th November, 2022).
50. See the quotation by the European Data Protection Supervisor, 'The first rule in data protection is: if you do not need personal data, do not collect it. The second rule is: if you really need personal data, then start by pseudonymising the personal data.' Available at https://edps.europa.eu/ipen-webinar-2021-pseudonymous-data-processing-personal-data-while-mitigating-risks_en. See also GDPR Article 25(1), GDPR Recital 78, and Articles 25(1) and (2).
51. See Commission Implementing Decision of 17.12.2021, note 23 above.
52. See https://MosaicEffect.com/ (accessed 20th November, 2022).
53. See EDPB Final Schrems II Guidance, note 7 above.
54. See EC Implementing Decision 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on 4 June 2021 (Final SCCs).
55. Anonymisation is not the state-of-the-art for protecting data when in use because of the availability of external datasets for augmenting purportedly anonymised data enabling unauthorised re-identification. If successful in making re-identification impossible, data subjects suffer from not having the flexibility to relink to identity for authorised processing. Recital (26) of the EU GDPR notes that even the data controller must not be able to reidentify a data subject, considering 'all the means reasonably likely to be used'. In practice, data controllers never delete source datasets used to create purportedly anonymous datasets, meaning that, apart from aggregated data, re-identification will almost always be trivial for the data controller. See footnote 2 in Annex II Commission Implementing Decision (EU) 2021/914, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN, which stipulates that anonymisation 'requires rendering the

data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible'. The EDPB highlights that the availability of external datasets enabling unauthorised re-identification must be considered. See paragraphs 79, 85, 86, 87, 88 of EDPB Final Schrems II Guidance, *Opinion 06/2014*, note 6 above.

56. See Article 29 Working Party Opinion on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, currently under revision by the EDPB (see the EDPB Work program 2021/2022 adopted on 16th March, 2021).
57. It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that pseudonymisation is a non-elective precondition under PIPA for certain processing activities pertaining to statistics, scientific research and archiving in the public interest (such as to be able to process the data without consent, repurposing, sharing and combining datasets). See paragraphs 36 and 42, available at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf (accessed 20th November, 2022) and PIPA Sections 15(1), 28(2) and 28(3).
58. It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that parties have an affirmative obligation under PIPA to 'endeavour to process personal data in anonymity or in pseudonymised form, if possible'. See paragraph 62, available at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf (accessed 20th November, 2022) and PIPA Sections 3(6) and 3(7).
59. See *SHIELD Act*, note 23 above.
60. See 45 C.F.R Parts 160 and 164, note 23 above.
61. Cal. Civ. Code § 1798.150(a)(1).
62. See *Breach Notification Rule*, available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
63. Fla. Stat. § 501.171(g)(2).
64. See *CJEU Schrems II* ruling at paragraphs 121, 135, 146, 154, and 203(3), available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404 (accessed 20th November, 2022).
65. See *Portuguese DPA Orders Suspension of U.S. Data Transfers by Agency that Relied on SCCs*, available at https://www.natlawreview.com/article/portuguese-dpa-orders-suspension-us-data-transfers-agency-relied-sccs (accessed 20th November, 2022).
66. See *52% of Fortune 500 Now Include Privacy Risk in 10-K Reports*, available at https://www.linkedin.com/pulse/52-fortune-500-now-include-privacy-risk-10-k-reports-jay-cline/?trk=eml-email_series_follow_newsletter_01-hero-1-title_link&midToken=AQEuYwjcC6-W7A&fromEmail=fromEmail&ut=3RK9saM2F069M1 (accessed 20th November, 2022).
67. See clauses 3 and 12 of Commission Implementing Decision (EU) 2021/914, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN (accessed 20th November, 2022).

Journal of
Data Protection & Privacy
Volume 5 Number 3

Contents

Editorial

Elon Musk's cost-cutting at Twitter raises fresh data protection concerns and puts the social media platform on a collision course with regulators on both sides of the Atlantic 205
Ardi Kolah, BA (Hons), LL.M, MBCS, MSyI, CIPP/E, CIPM, FIP, FRSA, Doctorate Researcher, Queen's University Belfast and Founding Editor-in-Chief, Journal of Data Protection & Privacy

Comment

Who are you on Web 3.0? 207
Lothar Determann, Baker McKenzie

Practice papers

African Union's Data Policy Framework and Data Protection in Africa 209
Kinfe Yilma, Addis Ababa University

The AI Act in light of the EU Digital Agenda: A critical approach 216
Konstantinos Kouroupis, Frederick University

Deconstructing the regulatory impact of the US CLOUD Act: An optimal regulatory approach to ensuring access to data in the cloud? 230
Nick Roudev, Linklaters and Lori Baker, Dubai International Financial Center

UK data protection and digital information bill explained 242
Steve Wilkinson, Freelance Data Protection Officer

Observing 2021–2 data breach decisions of the Irish Data Protection Commission 254
Marie C. Daly, Covington & Burling

Privacy nutrition labels, app store and the GDPR: Unintended consequences? 267
Miloš Novović, BI Norwegian Business School

Technical controls that protect data when in use and prevent misuse 281
Magali Feys, AContrario.law, et al

Right to be forgotten in case of search engines: Emerging trends in India as compared to the EU 297
Indranath Gupta and Paarth Naithani, Jindal Global Law School

Book review

Taming the Algorithm. The Right Not to Be Subject to an Automated Decision in the General Data Protection Regulation 310
Prof Dr Chris Bellamy, Member, Editorial Board Journal of Data Protection & Privacy

Henry Stewart Publications
Ruskin House,
40-41 Museum Street,
London, WC1A 1LT, UK
www.henrystewartpublications.com

Journal of
Data Protection & Privacy

Editorial Board

Founding Editor-in-Chief: Ardi Kolah LL.M, FCIM, MBCS, CIPP/E, CIPM, FIP, Founding Editor-in-Chief, Journal of Data Protection & Privacy and global privacy advisor

Professor Rajesh Babu, *Indian Institute of Management Calcutta*

Lori Baker, VP Legal Affairs and Director of Data Protection, *DIFC (Dubai International Financial Centre Authority)*

Robert Baldock, MD, *Clustre – The Innovation Brokers*

Aurélie Banck, Group DPO, *Europcar*

Christopher Bellamy, Professor Emeritus of Maritime Security, *University of Greenwich*, former Director of Security Studies and the Resilience Centre the *UK Defence Academy*

Joanne Bennett, Commercial Lawyer and Data Protection Consultant, UK

Nora Boukadid, Head of Chief Data Officer Services, *Deloitte*

Alexander Brown, Partner, Head of Data Protection and Privacy Group, *Simmons & Simmons LLP*

Cameron S D Brown, Director Cyber Security and Data Risk, *Deloitte*

Ann Cavoukian, PhD, Executive Director of The Privacy and Big Data Institute, *Ryerson University*

Abhik Chaudhuri, Chevening Fellow and Domain Consultant in Cyber Security, Privacy and Policy, *TATA Consultancy Services*

Roberto Colizzi, Executive Director, Privacy Legal, EMEA, *Sony Pictures Entertainment*

Philip Coppel QC, Barrister, *Cornerstone Barristers*

Lothar Determann, Partner, *Baker & McKenzie,* Professor, *Free University of Berlin,* and Lecturer, *University of California, Berkeley School of Law*

Fabio Di Resta, Attorney at law, *Di Resta Lawyers*

Abigail Dubiniecki, Founder, Strategic Compliance Consulting

Andrew Dyson, Partner, *DLA Piper UK LLP*

Khaled El Emam, Professor, Faculty of Medicine, *University of Ottawa*

Dr Detlev Gabel, Partner, Chair of the Global Data, Privacy and Cyber Security Group, *White & Case LLP*

Dennis Garcia, Assistant General Counsel, *Microsoft Corporation*

Ben Gerber, Chief Information Security Officer, *Coupang*

Dr Aris Gkoulalas-Divanis, Technical Lead on Data Protection and Privacy, *IBM Watson Health*

Eduard Goodman, International Privacy Lead Counsel, *TransUnion*

Dr Jaap Henk Hoepman, Privacy & identity Lab, *Radboud University*

Mark D Hughes, Executive Director, *Institute for the Study of Privacy Issues (ISPI)*

Denis Kelleher, Head of Privacy (EMEA), *LinkedIn*

Dr Kouroupis Konstantinos, Assistant Professor of European and Data Rights Law, Department of Law, *Frederick University*, Cyprus — MC Member of COST ACTION CA19143 (Global Digital Human Rights Network — GDHRN)

Jacob Kornbeck, Youth Unit, *European Commission*

Paul Lanois, Director, *Fieldfisher*

Michael Lester, Director, M&A Risk Analysis, *Cognizant*

Michael Lewis, Group Data Protection & Privacy Officer, *The Admiral Group plc*

David Melnick, CEO, *Ledger Works*

The Honourable Mr Justice, **Graeme Mew**

Simon Morrissey, Legal Director, *BBC Information Rights*

Dr Phil Nobles, Lecturer, *Cranfield University at the Defence Academy*

Rocco Panetta, Managing Partner, *Panetta Law Firm* and Chair, *Strand PTP Privacy & Technology Professionals*

Antonis Patrikios, Partner, *Dentons*

Alexandre Pinheiro, *Universidade Federal do Estado do Rio de Janeiro (UNIRIO)*

Richard Preece, Hybrid consultant and GCHQ Certified Trainer

Chiara Rustici, Independent GDPR Analyst

Nick Taylor, UKI Strategy Lead, *Accenture*

Martijn ten Bloemendal, Global Privacy Counsel, *AbbVie*

Roslyn Vadala, Chief Privacy Officer, *Cochlear Limited*

Fokke Jan van der Tol, Data Governance Expert

Steven Wilkinson, Data Privacy Consultant

Steve Wright, DPO, CEO, Privacy Culture

Order Form

Journal of

Data Protection & Privacy

ISSN 2398-1679

◯ Please enter my subscription to the current volume, Volume 5 (consisting of 4 issues), at:
☐ £210 UK and Europe ☐ US$295 N. America* ☐ £225 Rest of World

◯ Please enter my subscription to the current volume, Volume 4 (consisting of 4 issues), at:
☐ £210 UK and Europe ☐ US$295 N. America* ☐ £225 Rest of World

◯ I enclose a cheque made payable to: Henry Stewart Publications

◯ Please invoice me/my company

◯ Please charge £_____/US$_____to my Mastercard/Amex/Visa (Please delete accordingly)

*Only subscribers in North America may pay the Dollar rate. All other subscribers will be charged in Sterling

Card No: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Expiry date: ☐☐/☐☐

◯ CVC Number* ☐☐☐

(*the last 3 digits on the reverse of card — please note this data will be destroyed after your payment has been processed)

Name of Cardholder:_____Signature of Cardholder:_____

Please provide card billing address if different from the firm/organisation address.

_____

_____

Postcode

Mr/Mrs/Miss/Ms First Name Last Name

Position/Department

Organisation

Address

_____

Country Zip/Postcode

Tel: Fax: E-mail:

Type of Organisation

PLEASE PHOTOCOPY AND SEND THE COMPLETED FORM TO:

Henry Stewart Publications, Ruskin House, 40-41 Museum St, London, WC1A 1LT, UK
Tel: +44 (0)20 7092 3469, +1 646 895 6129; Fax: +44 (0)20 7404 2081; E-mail: gweny@henrystewart.co.uk