Organisation for Economic Co-operation and Development

DSTI/CDEP/DGP(2023)8

For Official Use English - Or. English

20 March 2023

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Working Party on Data Governance and Privacy in the Digital Economy

Use Cases for Privacy-Enhancing Technologies

Proposal for (hybrid) Expert Workshop

8th Session of the WPDGP Meeting, 17-18 April 2023

This document outlines five use cases for privacy-enhancing technologies (PETs) that could be discussed at a possible (hybrid) expert workshop in the second half of 2023. These include using PETs for: (i) pandemic response through contact tracing and scientific research; (ii) collaboration across financial institutions and authorities for crime detection; (iii) privacy-preserving digital identity management; (iv) co-ordination across distributed global value chains for Industry 4.0; and (v) data collection and sharing for official statistics and evidence-based policies.

The goal is to provide policy makers and regulators with a more comprehensive understanding of the practical benefits and limitations of PETs and to identify current and emerging needs for possible regulatory and policy actions.

The proposed workshop would contribute to Output Result 1.3.1.5.4 of the Committee on Digital Economy Policy (CDEP)'s Program of Work and Budget (PWB) for 2023-2024 on "Follow on Work from the EASD Recommendation" [DSTI/CDEP(2021)15/FINAL].

Action requested: WPDGP Delegates are invited to consider the list of use cases to be discussed at the possible expert workshop and indicate the order of priority they wish to assign to theses use cases under Item 14 of the draft agenda of the 8th Session of the WPDGP Meeting.

Christian Reimsbach-Kounatze: christian.reimsbach-kounatze@oecd.org; +33 1 45 24 76 16
Clarisse Girot: clarisse.girot@oecd.org; +33 1 45 24 10 19
Marion Barberis: marion.barberis@oecd.org; +33 1 45 24 89 40

JT03514690

Use Cases for Privacy-Enhancing Technologies: Proposal for Expert Workshop

1. This document outlines five concrete use cases for privacy-enhancing technologies (PETs) that the Working Party on Data Governance and Privacy in the Digital Economy (WPDGP) is invited to consider as part of follow-up work on the OECD (2023[1]) report on "Emerging Privacy-Enhancing Technologies". To support the work, an expert workshop is proposed that would focus on a selection of these use cases. The goal is to provide policy makers and regulators, including but not limited to privacy enforcement authorities (PEAs), with a more comprehensive understanding of the practical benefits and limitations of PETs and to identify current and emerging needs for possible regulatory and policy actions based on the specific use cases to be discussed.

1. Background and rationale

2. PETs refer to a range of digital technologies and techniques that enable the collection, processing, analysis, and sharing of information while safeguarding data confidentiality and privacy. (OECD, 2023[1]) They are increasingly recognised as a practical solution that can provide a relatively high level of data utility in privacy-preserving ways. (OECD, 2021[2]; G7, 2022[3]; 2022[4])[1]

3. Although many emerging PETs are still in their early stages of development, they hold immense potential to advance privacy-by-design principles and foster trust in data sharing and re-use across organisations, sectors, and jurisdictions. As a result, policymakers and regulators are exploring ways to better align the potential and risks of PETs with their policy and regulatory frameworks. (OECD, 2023[1])

4. The technical complexity and rapid evolution of PETs, however, pose challenges not only for policymakers and regulators but also for organisations seeking to implement PETs into their existing business processes and data governance frameworks. These challenges are compounded by the fact that many PETs are limited to specific use cases. This raises questions about possible case-specific challenges that need to be addressed as policymakers and regulators seek to achieve wider, more effective and appropriate adoption of PETs, in line with their regulatory and policy frameworks.

[1] The G7 (2022[3]) Communiqué "Promoting Data Free Flow with Trust and Knowledge Sharing about the Prospects for International Data Spaces" for example recognises that "[t]he use of PETs can facilitate safe, lawful and economically valuable data sharing that may otherwise not be possible, unlocking significant benefits to innovators, governments and the wider public. In recognition of these benefits … the G7 data protection and privacy authorities … will seek to promote the responsible and innovative use of PETs to facilitate data sharing …".

2. Objective and logistics

5. Against above backdrop, the OECD (2023[1]) report on "Emerging Privacy-Enhancing Technologies" concluded that:

> an analysis of concrete use cases of PETs, including but not limited to the use of PETs for facilitating cross-border data flows, may help inform policy discussions, including in respect to the privacy and economic outcomes PETs promise to help achieve.

6. To help advance policy discussions on PETs in line with the above conclusion, it is proposed to hold an (hybrid) expert workshop that would focus on concrete use cases for PETs. More specifically, the objective of the expert workshop would be to:

- Analyse the opportunities and challenges of PETs based on a selection of concrete use cases;
- Identify current and emerging needs for possible regulatory and policy actions that would help promote the appropriate adoption of PETs; and
- Build an international community of experts on the policy and regulatory aspects related to PETs that would assist the Secretariat in developing policy recommendations as needed and appropriate.

7. Depending on the number of use cases that the WPDGP would wish to address (see Section 3), the proposed expert workshop could be held on one or two days in Q3 or Q4 2023. The proposed venue of the event would be the OECD Headquarters, but WPDGP delegates are strongly encouraged to consider hosting the proposed event, in which case voluntary contributions would be required.

3. Potential use cases for PETs for consideration

8. The following sections present an open list of potential use cases for PETs that could be discussed at the proposed expert workshop. They are listed in the order of priority as proposed by the Secretariat.

9. For each proposed use case, experts would examine how PETs can foster trust for collaboration when e.g.: (i) identifying commonalities across multiple datasets; (ii) enabling artificial intelligence (AI), for instance, by deriving common AI models across multiple datasets; and/or (iii) supporting cross-border data flows in combination with existing privacy and other legal requirements. Additionally, experts would discuss the privacy risks and limitations related to the (inappropriate) use of PETs and how to address these risks in the specific use cases. They would also explore how to address possible legal, organisational and skills-related barriers that may have hindered the appropriate adoption of PETs so far.

3.1. Pandemic response through contact tracing and scientific research

10. At the early stages of the COVID-19 pandemic, governments sought new tools to inform their policies and tackle the crisis. (OECD, 2020[5]) This included mobile applications (apps) designed to track the spread of the virus through contact tracing. However, these apps raised serious privacy concerns due to the collection of a wide range of personal data, including geo-location data, the scale and scope of which was challenging for most users to understand, in particular as changes were continuously introduced (OECD, 2020[5]). Moreover, some apps continued to run in the background and share data with other apps through application programming interfaces (APIs), fuelling existing privacy concerns.

11. The collection and processing of sensitive health-related data also played a crucial role in expediting scientific research for the development of effective COVID-19 vaccines. Evidence indicates that global collaboration enabled by data sharing across organisations and jurisdictions enabled the rapid development of some of these vaccines in less than a year. (OECD, 2021[6]) However, several challenges such as poor data quality and trust issues regarding privacy and confidentiality between organisations and countries hindered effective data sharing between key stakeholders in some instances. (OECD, 2020[7])

12. PETs have been recognised and used to address the above challenges during the COVID-19 pandemic. For example, some contact tracing apps used private set intersection (PSI) techniques to notify users of potential exposure to the virus, without the need to share personal data. (OECD, 2023[1]) PETs have also facilitated cross-border health research by enabling healthcare providers across multiple countries to share encrypted data sets with researchers more securely. (OECD, 2020[7]) This has allowed for instance for reliable calculations of correlations between certain chronic or genetic conditions and COVID-19 mortality rates while preserving individual patient privacy. (Blatt et al., 2020[8])

13. This use case would focus on lessons learned from the deployment of PETs to minimise privacy risks when addressing the COVID-19 pandemic through data and digital technologies. It would benefit from promising solutions presented at innovation contests such as the UK-US PETs Challenge Prize (n.d.[9])[2], which focusses on privacy-preserving solutions that can forecast individuals' risk of infection with the aim to bolster pandemic response capabilities and strengthen global readiness for ongoing and future public health emergencies.[3]

3.2. Collaboration across financial institutions and authorities for crime detection

14. Collaboration based on data sharing across financial institutions as well as tax authorities and regulators is essential for detecting tax and financial crimes. (FATF, 2021[10]; 2022[11]) However, traditional methods for such detection often rely on analysing sensitive financial data, which puts the data at risk of being compromised and of violating clients' privacy and confidentiality. To address these concerns, some financial market and tax authorities have explored PETs such as secure multi-party computation (SMPC), homomorphic encryption (HE), and federated learning (FL) when searching for financial and tax crimes.

15. To enforce Estonia's 2016 law against Value Added Tax (VAT) fraud, for example, the Estonian Tax and Customs Board initially considered collecting all transactions of companies subject to VAT. This turned out to be impractical, and the authority decided to explore alternative solutions using SMPC to implement a distributed but confidential fraud detection system. The goal was to enable both the tax authority and organisations representing the companies paying VAT to perform the calculations needed, while preventing any other party from accessing sensitive information. (Bogdanov et al., 2016[12]; Archer et al., 2018[13])

16. The Financial Conduct Authority (FCA) in the United Kingdom, as another example, held the 2019 TechSprint event on "Global Anti-Money Laundering and Financial Crime," with the objective to create a network of financial institutions to investigate financial transactions, codify typologies of financial crimes, develop a process for data verification during due diligence, and identify the Ultimate Beneficiary Owner (UBO) across a network of financial institutions. (FCA, 2023[31]; see also ACPR, 2022[32]) The event inspired various follow-up activities, including the UK-US PETs Challenge Prize (n.d.[9]) and its first track on using PETs for privacy-preserving financial information sharing and collaborative analytics to address international money laundering.[4]

17. This use case would focus on PET-based solutions that have shown to successfully enable collaboration across financial institutions and/or tax and financial market regulators for crime detection, building on possible solutions presented at innovation contests such as those mentioned above.

---

[2] Initiated in July 2022, this initiative by the United Kingdom and the United States governments aims to encourage innovators to develop PETs that can combat global societal challenges. (United Kingdom, 2022[34])

[3] This second track of the UK-US PETs Challenge Prize is based on synthetic dataset created by the University of Virginia's Biocomplexity Institute, a dataset representing the digital twin of a regional population.

[4] This track of the UK-US PETs Challenge Prize challenges is based on synthetic global transaction data created by SWIFT, the global provider of secure financial messaging services. (United Kingdom, 2022[34])

3.3. Privacy-preserving digital identity management

18. The rapid expansion of online services, and the corresponding increase in sensitive information collected by these services, including e.g. biometric information, have made the need for reliable and secure digital identity management more pressing than ever. (OECD, 2011[14]; 2021[15]; FATF, 2020[16])[5] However, some existing digital identity management approaches have limitations in ensuring privacy and digital security (Solomon, 2018[17]; Liyanage et al., 2021[18]), resulting in possible severe violations of individuals' privacy and identity theft. This is particularly critical in respect to children online, who may need to have their age established to be given or denied access to certain online services, but can easily be subject to invasive age verification and assurance systems (Livingstone et al., 2021[19]).

19. There is thus a pressing need for robust solutions that can help verify or assure a user's identity or key attributes (e.g. age) remotely, and in a privacy-preserving and secure manner. To address this need, some governments and privacy enforcement authorities (PEAs) together with researchers and industry practitioners are exploring the use of PETs such as zero-knowledge proofs (ZKP) and SMPC. (Liyanage et al., 2021[18]) The innovation lab of the French data protection authority ("Laboratoire d'Innovation Numérique de la CNIL", LINC), for example, presented a demonstrator of an "ideal" digital solution for age-verification that relies on ZKP. This demonstrator was used to prove that an age verification system is feasible, through a third-party system, that protects the privacy of individuals.

20. National digital identity initiatives can also help promote PET adoption. Finland, for example, is developing national legislation to enable citizens and foreigners to use digital identification based on a state-issued core identity that follows self-sovereign identity principles[6] (Ministry of Finance, Finland, n.d.[20]). This new digital identification is planned to be tracking-resistant thanks to PETs, preventing the issuer from tracking its use. The new digital ID solution also aims to serve as the foundation for the upcoming natural person EU Digital Identity wallet, based on the revised electronic identification, authentication and trust services (eIDAS) regulation of the European Union, which regulates cross-border use of digital ID (European Union, 2014[21]).

21. This use case aims to explore the use of PETs in current and emerging digital identity management approaches, in areas such as health, travel, and e-government. The use case would also address how PETs can help implement self-sovereign identities (OPC, 2017[22]; Consensys, n.d.[23]), and enable individuals to gain more control over their 'digital footprints' which have become a significant additional element of today's digital identity (Wilton, 2008[24]; Davison, 2012[25]; Adjei, 2019[26]).

3.4. Co-ordination across distributed global value chains for Industry 4.0

22. Industrial production increasingly relies on a confluence of technologies, including in particular data analytics, AI, cloud computing and the Internet-of-Things (IoT), a trend often referred to as Industry 4.0. (OECD, 2017[27]; 2020[28]) In conjunction with data, these digital technologies can help enhance global value chains (GVCs) along the different stages of the production process, which are typically spread across various countries. (OECD, 2022[29]) This involves: facilitating collaboration for research and development (R&D); optimising the flow of goods and services from suppliers to customers; improving risk management across GVCs and enhancing their resilience; increasing productivity through process optimisation and automation; and enabling new business models, including the "servicification"[7] of manufacturing.

---

[5] See also the OECD draft Recommendation on the governance of digital identity [GOV/PGC/EGOV(2022)4/REV2].

[6] Self-sovereign identity is a concept whereby users are given complete control over their digital identity by allowing them to manage it across multiple locations with their consent. (OPC, 2017[22]).

[7] Rolls-Royce, for example, shifted their business from a product and service solution to a service model, trademarked as "Power by the Hour" (PBH), where customers only pay for the time they use Rolls-Royce engines. (OECD, 2017[27])

23. In this context, protecting non-personal data, often generated by machines, has become a significant concern for organisations involved in GVCs. This raises questions beyond privacy protection on the need for practical solutions to better control access and use rights to non-personal data, while enabling their sharing and re-use along GVCs, in line with regulatory, intellectual property (IP), digital security and business requirements. To address this challenge, PETs are being increasingly considered, and in some cases, tested and implemented.

24. For example, Thales, a French aerospace, defence, transportation and security company, tested the use of PETs to enable secure predictive maintenance services for distributed fleets. (Inpher, n.d.[30]). This allowed Thales to provide customers with comprehensive, accurate, and cryptographically secure predictive maintenance that can train prediction models on distributed data sources without moving or exposing any confidential and proprietary data between the owners and the operators of the equipment.

25. BMW, a German automobile manufacturing company, as another example, has explored how PETs can improve automotive value chains, with a focus on reducing maintenance costs and enabling personalised services in confidential and privacy-preserving manners (Garrido et al., 2022[31]). In this context, PETs such as SMPC have proven to be necessary for secured data sharing for instance when reconciling stock levels while avoiding the leakage of business critical information.

26. This use case aims to address the potential and challenges of using PETs for enhancing GVCs, with a particular emphasis on non-personal data. It would involve businesses and academic researchers prototyping, testing, and/or deploying PETs for industrial production applications, in order to discuss the feasibility and effectiveness of PETs in this use case.

3.5. Data collection and sharing for official statistics and evidence-based policies

27. Accurate statistical information is essential for governments, businesses, researchers, and the general public to make informed decisions, develop evidence-based policies, and monitor progress towards national and international societal and policy objectives. National statistical offices (NSOs) have traditionally been the primary sources of such statistical information, but their production requires the collection and processing of significant amounts of personal and/or confidential data, creating potential risks for privacy and confidentiality violations.

28. NSOs, and the statistical community more broadly, are increasingly exploring and promoting the adoption of PETs to better respond to the need for more timely statistical information, while ensuring confidentiality and privacy protection. For example, the United Nations Economic Commission for Europe (2022[32]) explored the use of PETs such as synthetic data as an alternative to the release of individual-level records. It concluded that synthetic data can be sufficiently practical to “maximise the amount of statistical information that data users can utilise, while keeping statistical disclosure risks at a minimal level”.

29. Moreover, in certain jurisdictions, frameworks governing the production and dissemination of official statistics are under review, with particular attention being given to the role of PETs. In its proposal for “European statistics on population and housing”, for instance, the European Commission (2023[33]) explicitly endorses the use of PETs to facilitate data sharing, while “strengthen[ing] the legal basis and encourag[ing] the development of innovative solutions to enable data sharing”, in line with privacy protection legislation in the European Union.

30. This use case aims to explore the potential and limitations of PETs when collecting, producing, and disseminating national statistics and other public sector information needed to inform public policies. It would benefit from collaboration with the statistical community, including NSOs and relevant international organisations, as well as with government bodies and researchers who have used PETs in their interactions with NSOs to help inform public policies.

References

ACPR (2022), *Tech Sprint 2022 : Call for applications*, Banque de France, https://acpr.banque-france.fr/en/tech-sprint-2022-call-applications (accessed on 13 March 2023). [35]

Adjei, J. (2019), "Monetization of Personal Digital Identity Information: Technological and Regulatory Framework", *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-7113-1.ch016*, pp. 283-293, https://doi.org/10.4018/978-1-5225-7113-1.CH016. [26]

Archer, D. et al. (2018), "From Keys to Databases-Real-World Applications of Secure Multi-Party Computation", *The Computer Journal*, Vol. 61/12, pp. 1749-1771, https://doi.org/10.1093/comjnl/bxy090. [13]

Blatt, M. et al. (2020), "Secure large-scale genome-wide association studies using homomorphic encryption", *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 117/21, pp. 11608-11613, https://doi.org/10.1073/PNAS.1918257117/SUPPL_FILE/PNAS.1918257117.SAPP.PDF. [8]

Bogdanov, D. et al. (2016), "How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation", *International Conference on Financial Cryptography and Data Security*, https://doi.org/10.1007/978-3-662-47854-7_14. [12]

Consensys (n.d.), *Blockchain for Digital Identity | Real World Blockchain Use Cases | ConsenSys*, https://consensys.net/blockchain-use-cases/digital-identity/ (accessed on 13 March 2023). [23]

Davison, C. (2012), *Presentation of digital self in everyday life: towards a theory of digital identity*, RMIT University, https://researchrepository.rmit.edu.au/esploro/outputs/doctoral/Presentation-of-digital-self-in-everyday/9921861557101341. [25]

European Commission (2023), *Proposal for a Regulation of the European Parliament and of the Council on European statistics on population and housing, amending Regulation (EC) No 862/2007 and repealing Regulations (EC) No 763/2008 and (EU) No 1260/2013*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2023:31:FIN (accessed on 9 February 2023). [33]

European Union (2014), "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", Document 32014R0910, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910. [21]

FATF (2022), *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html. [11]

FATF (2021), *Stocktake on Data Pooling, Collaborative Analytics and Data Protection*, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Digitaltransformation/Data-pooling-collaborative-analytics-data-protection.html. [10]

FATF (2020), *Guidance on Digital ID*, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html (accessed on 13 March 2023). [16]

G7 (2022), *Communiqué Roundtable of G7 Data Protection and Privacy Authorities: Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces*, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1 (accessed on 31 January 2023). [3]

G7 (2022), "G7 Digital Ministers' Track - Annex 1: G7 Action Plan for Promoting Data Free Flow with Trust", in *G7 Ministerial Declaration*, https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile (accessed on 7 March 2023). [4]

Garrido, G. et al. (2022), "Exploring privacy-enhancing technologies in the automotive value chain", *2021 IEEE International Conference on Big Data*, https://doi.org/10.1109/BigData52589.2021.9671528. [31]

Inpher (n.d.), *Predictive Maintenance for Distributed Fleets*, https://inpher.io/solutions/by-use-case/defense-iot/ (accessed on 15 March 2023). [30]

Livingstone, S. et al. (2021), *Can the Internet be age appropriate, or at least not inappropriate and harmful? The promise of age verification and parental control tools*, https://euconsent.eu/can-the-internet-by-age-appropriate-or-at-least-not-inappropriate-or-harmful-the-promise-of-age-verification-and-parental-control-tools/. [19]

Liyanage, H. et al. (2021), "Privacy Enhancing Techniques for Digital Identity Management", https://doi.org/10.25394/PGS.14847567.V1. [18]

Ministry of Finance, Finland (n.d.), "Digital Identity", webpage, https://vm.fi/en/digital-identity (accessed on 1 March 2023). [20]

OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en. [1]

OECD (2022), "Fostering cross-border data flows with trust", *OECD Digital Economy Papers*, No. 343, OECD Publishing, Paris, https://doi.org/10.1787/139b32ad-en. [29]

OECD (2021), *G20 Collection of Digital Identity Practices: Report for the G20 Digital Economy Tak Force, Trieste, Italy, August 2021*, OECD Publishing, Paris, https://doi.org/10.1787/75223806-en. [15]

OECD (2021), *Recommendation of the Council on Enhancing Access to and Sharing of Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463. [2]

OECD (2021), "Resolving global challenges and crises through international collaboration", in *OECD Science, Technology and Innovation Outlook 2021: Times of Crisis and Opportunity*, OECD Publishing, Paris, https://doi.org/10.1787/e0643f52-en. [6]

OECD (2020), "Artificial intelligence, digital technology and advanced production", in *The Digitalisation of Science, Technology and Innovation: Key Developments and Policies*, OECD Publishing, Paris, https://doi.org/10.1787/629af843-en. [28]

OECD (2020), "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics"*, OECD Policy Responses to Coronavirus (Covid-19)*, No. Updated version 23 April 2020, OECD, http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/. [5]

OECD (2020), *Why open science is critical to combatting COVID-19*, https://www.oecd.org/coronavirus/policy-responses/why-open-science-is-critical-to-combatting-covid-19-cd6ab2f9/ (accessed on 13 March 2023). [7]

OECD (2017), "Benefits and challenges of digitalising production", in *The Next Production Revolution: Implications for Governments and Business*, OECD Publishing, Paris, https://doi.org/10.1787/9789264271036-6-en. [27]

OECD (2011), *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*, https://www.oecd.org/sti/ieconomy/49338380.pdf (accessed on 13 March 2023). [14]

OPC (2017), *Privacy Enhancing Technologies – A Review of Tools and Techniques*, Office of the Privacy Commissioner of Canada, Ottawa, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/. [22]

Solomon, B. (2018), "Digital IDs Are More Dangerous Than You Think", *WIRED*, https://www.wired.com/story/digital-ids-are-more-dangerous-than-you-think/ (accessed on 13 March 2023). [17]

UK-US Prize Challenges (n.d.), *Privacy Enhancing Technologies Prizes*, website, https://petsprizechallenges.com/ (accessed on 1 March 2023). [9]

United Kingdom (2022), *UK and US launch innovation prize challenges in privacy-enhancing technologies to tackle financial crime and public health emergencies*, https://www.gov.uk/government/news/uk-and-us-launch-innovation-prize-challenges-in-privacy-enhancing-technologies-to-tackle-financial-crime-and-public-health-emergencies (accessed on 30 January 2023). [34]

United Nations Economic Commission for Europe (2022), *Synthetic Data for Official Statistics: A Starter Guide*, United Nations, Geneva, https://unece.org/sites/default/files/2022-11/ECECESSTAT20226.pdf (accessed on 1 February 2023). [32]

Wilton, R. (2008), "Identity and privacy in the digital age", *International Journal of Intellectual Property Management*, Vol. 2/4, pp. 411-428, https://doi.org/10.1504/IJIPM.2008.021435. [24]