September 9, 2019

Parliament & Government Affairs
Information Commissioner's Office
Wycliffe House
Water Lane, Wilmslow
Cheshire SK9 5AF
United Kingdom

Re: ICO Consultation on the Draft Data Sharing Code of Practice

Dear Commissioner Denham,

Inpher appreciates the opportunity to advise the Information Commissioner's Office ("ICO") on the updated Data Sharing Code of Practice,[1] prepared under Section 121 of the Data Protection Act of 2018 ("DPA"). We support the ICO's leadership on best practices guidelines that reflect advances in privacy-enhancing technologies ("PETs") and promote organizational accountability in data processing and sharing. This consultation will be critical to clarifying the overarching policy goals of the DPA and the EU General Data Protection Regulation ("GDPR") to support their successful implementation in letter and in spirit.

The Draft Code exemplifies modern applications of data- and knowledge- sharing that can bring significant benefits to individuals and societal welfare, while emphasizing critical privacy and governance safeguards for data analytics. We strongly support this approach to responsible data sharing. Privacy is foundational to the future of computing, and should foreground the technologies that facilitate data processing and sharing. Regulators must guide organizations to harness the valuable utilities of cross-border, cross-industry, and cooperative data sharing with effective designs for privacy and security.

Therefore, Inpher makes the following recommendations for the ICO to include in the Draft Code: (1) to elaborate on data sharing use cases in the financial services sector, particularly in detecting fraud and trading anomalies; (2) to acknowledge the limitations of data stewardship in data sharing agreements; (3) to require data protection impact assessments ("DPIAs") to consider implementing PETs in data sharing operations, and (4) to educate on Secure Multi-Party Computation ("MPC") and Fully Homomorphic Encryption ("FHE") as methods that can facilitate cooperative computing without disclosing or sharing personal information.

Inpher Background

[1] UK Information Commissioner's Office, *ICO consultation on the draft data sharing code of practice* (Jul. 16, 2019), https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-data-sharing-code-of-practice/

We are a US-based cryptography and machine-learning company with the conviction that encryption and privacy are foundational to the future of computing and commerce. Inpher applies years of academic research on FHE and MPC into commercially-ready applications that financial institutions are using in production today.[2]

Inpher's customers include some of the world's largest multinational financial institutions that use our software platform for privacy-preserving analytics and computation with mathematical guarantees of data security and sovereignty. This 'secret computing' technology enables compliant data processing across siloed departments, cross-jurisdictional and cross-industry information sharing, and zero-knowledge cloud computing, as the host never 'sees' the data nor has access to the keys. Our legal and public policy department facilitates public education on privacy-preserving technologies and advocates for data protection by design, global privacy, and algorithmic accountability.

Recommendation 1: Add Use Cases on Beneficial Data Sharing

From pages 13 to 15 in the Draft Code, the section on 'Benefits of Data Sharing' only provides examples related to patient health records and medical care. The scope of this guidance is limited and does not reflect the diversity of industries that actively engage in data sharing for various commercial or regulatory benefits. Adding the following use cases will expand the Code's application to industries where data sharing is already prevalent.

- Financial institutions could benefit from data sharing to detect outliers that indicate fraudulent transactions, money laundering, or trade anomalies. However, banks are often prevented from pooling data for global transactions-monitoring due to privacy and confidentiality concerns in revealing customer data to competing institutions. Applying encryption-based PETs can enable knowledge sharing without data sharing—for example, MPC facilitates high precision, privacy-preserving computing methods in detecting financial fraud.[3]

- Financial regulators such as the UK Financial Conduct Authority ("FCA") could benefit from inter-agency data sharing and collaborative computing to monitor global financial crimes.[4] The FCA has recently hosted a regulatory sandbox, TechSprint, for cryptographic PETs that can resolve inherent privacy concerns in cross-border data sharing with international regulators. MPC and FHE demonstrated applications to secure data-sharing for financial enforcement.[5]

- Autonomous vehicles could benefit from industry-wide data sharing for safety testing and validation, but are often prevented due to competitive concerns that reinforce data silos across companies.[6] Cryptographic PETs that enable secure collaboration with multiple parties to

[2] Inpher, *Case Studies*, https://www.inpher.io/case-studies-1#case-studies
[3] Christina Boura, Ilaria Chillotti, Nicolas Gama, Dimitar Jetchev, Stanislav Peceny & Alexander Petric, "High-Precision Privacy-Preserving Real-Valued Function Evaluation." IACR Cryptology ePrint Archive (2017). https://eprint.iacr.org/2017/1234.pdf
[4] UK Financial Conduct Authority, *2019 Global AML and Financial Crime TechSprint* (Held on Jul. 29, 2019 to Aug. 2, 2019), https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint
[5] Inpher, *Inpher Wins People's Choice Award at FCA TechSprint* (Aug. 9, 2019), https://www.inpher.io/news/2019/8/9/inpher-wins-peoples-choice-award-at-financial-conduct-authoritys-2019-tech-sprint.
[6] Jesse Krompier, *SAFETY FIRST: THE CASE FOR MANDATORY DATA SHARING AS A FEDERAL SAFETY STANDARD FOR SELF-DRIVING CARS,* U. Ill. J.L. Tech. & Pol'y 439 (2017)

perform a function without revealing the underlying data can equally address the critical lapse of data sharing in this industry.

Recommendation 2: Acknowledge Limitations of Data Sharing Agreements

Contractual safeguards do not offer effective privacy protections in data transfers. Privacy "self-management"[7] tools—privacy policies and service agreements—can be easily overridden by bad or negligent actors. Consequently, unauthorized access to data often goes undetected until it is too late to contain the information leak. The ICO should address these shortcomings in the Draft Code and contrast with *ex ante* privacy-by-design safeguards which could be more appropriate in routine data sharing arrangements.

The validity of standard contractual clauses ("SCC") for cross-border data transfers is currently being challenged at the European Court of Justice.[8] Contractual arrangements offer virtually no protection against foreign legal systems that provide limited judicial redress for data that has been transferred into that jurisdiction. This was highlighted by the *Schrems I* decision of the Court of Justice of the European Union ("CJEU") in 2015 that invalidated EU to U.S. data transfers under the Safe Harbor scheme.

Moreover, data sharing agreements do not protect against liability for a third party's data breach—whereas rapidly evolving cryptographic PETs such as FHE and MPC offer incorruptible *ex ante* privacy safeguards against unauthorized access by intermediaries and employees of third parties.[9] The regulatory focus on data transfers should shift to implementing PETs that can keep data securely encrypted in storage, transit, and *in-use* (while being processed), so that sensitive plaintext information is not exposed to those who may violate their data sharing agreement or fiduciary obligations to engage in misconduct.

Cryptographic technologies can protect data with mathematical certainty, whereas mere operational policies to monitor use and authorizations cannot ensure absolute privacy firewalls.

Recommendations 3 & 4: Require DPIAs to Consider Adopting Cryptographic PETs

GDPR article 35(4) empowers the ICO to publish a list of processing operations that are likely to cause a high risk and thus mandate a DPIA. GDPR Article 36 requires the data controller to immediately suspend processing when DPIAs point to a high risk for individuals. Accordingly, GDPR Article 36(1) mandates the data controller to submit DPIAs to the ICO and consult the ICO on whether the proposed processing is permissible under the law. The data controller is prohibited from proceeding without satisfying these safeguards under the supervision of the ICO.

---

[7] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013)
[8] Data Protection Commissioner v Facebook Ireland and Maximillian Schrems ("Schrems II")
[9] Yehuda Lindell & Benny Pinkas, *Secure Multiparty Computation for Privacy-Preserving Data Mining*, The Journal of Privacy and Confidentiality (2009), http://jpc.cylab.cmu.edu; *ING Belgium Sees Opportunities for 'Secret' Sharing of Encrypted Data*, The Wall Street Journal (Jun. 1, 2017), https://blogs.wsj.com/cio/2017/06/01/ing-belgium-sees-opportunities-for-secret-sharing-of-encrypted-data/

Pages 21 - 23 of the Draft Code enumerate key factors that data controllers must consider in determining whether a DPIA is required before processing or sharing data. The ICO recommended the following assessment in page 22, supporting the use of cryptographic PETs to anonymize data for functions that require multi-party computing:[10]

> ***Could we achieve the objective without sharing the data or by anonymising it?***
>
> *If you can reasonably achieve the objective in another less intrusive way, you should not process the personal data. For example, where you could instead do this by sharing data that has been rendered anonymous (to which the GDPR doesn't apply) then you should do so, as it would be inappropriate to share the personal data itself in this context.*

The ICO should use its authority under the GDPR to recommend specific technology that enables anonymized computing as a best practice guideline. This section should educate on the application of Secure Multi-Party Computation and Fully Homomorphic Encryption to achieve knowledge-sharing without the transfer of personal data:

- MPC and FHE allow functions to be performed on encrypted data without revealing the underlying information. In particular, the additive secret sharing method in MPC transforms plaintext data into random auxiliary numbers in the computing process, so that collaborative analysis can be performed without disclosing or transferring any personal information from the original dataset. This auxiliary data is then deleted after each computing operation, virtually eliminating the possibility of re-identification.

- According to the Opinion of the Article 29 Working Party on Anonymization Techniques[11] and the Court of Justice of the European Union's ("CJEU") 'identifiability test' in case C-582/14 (October 19, 2016), data is effectively anonymized if re-identification of the data subject is practically impossible because it requires a disproportionate effort in terms of time, cost and manpower. The mathematical risk of re-identification in MPC through the reverse engineering of randomly generated, then deleted, numerical data is virtually nil, thereby satisfying the anonymization threshold of the GDPR. MPC thus computes on anonymized data that can no longer be attributed to a specific data subject, even through the use of additional data from any third party.

MPC and FHE can ensure that privacy will continue to be protected during the transfer, storage, and processing of data—whilst preserving the data's valuable utility. Application of such privacy-preserving technologies obviates traditional tradeoffs in privacy and analytical precision (for example, with differential privacy methods), and allow secure collaboration across data hosts.

Conclusion

[10] UK Information Commissioner's Office, *Data Sharing Code of Practice: Draft Code for Consultation,* https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

[11] Opinion 05/2014 on Anonymization Techniques of 10 April 2014, WP216, available on the European Commission's website at http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

The inclusion of MPC and FHE in ICO's Data Sharing Code of Practice would raise awareness of beneficial PETs that can facilitate privacy-preserving analytics. Regulatory support of PETs can instill organizational accountability by requiring businesses to implement better technological safeguards and protective measures for privacy.

Thank you for the opportunity to comment on this important consultation. If you have any questions regarding our comments, or if Inpher could be of any assistance, please do not hesitate to contact me at [redacted]

[redacted]
Inpher, Inc.