CONTRACTS FOR DATA COLLABORATION

COVID-19 DATA AND DATA SHARING AGREEMENTS

THE POTENTIAL OF SUNSET CLAUSES AND SUNSET PROVISIONS

A report by SDSN TReNDS and
DataReady Limited on behalf of C4DC

TRENDS
Thematic Research Network on Data and Statistics

DataREADY
Use data confidently.

TABLE OF CONTENTS

INTRODUCTION AND OVERVIEW

The COVID-19 pandemic is currently ravaging societies and economies around the world. Its reach is unprecedented in modern times. As digital technologies have become more embedded in our lives, COVID-19 related data on incidence rates; the availability of medical supplies; and the location of vulnerable people, among others – are informing policymakers' responses around the world. Within this context, much of the data needed to track and trace patients and vulnerable people or monitor compliance with quarantines, curfews, and lockdowns is highly sensitive. This data is often derived from individuals' mobile phones or via remote sensors of various kinds.

This situation creates challenges for policymakers concerned with ensuring that any sensitive data they use effectively balances the public interest against individuals' fundamental rights. This dilemma is at the heart of data use within the context of COVID-19 – at what point does a country's need to tackle the pandemic outweigh an individual's rights over their sensitive data? Different approaches are being taken around the world. Where the political calculus results in policies that prioritize sensitive data over individual rights to tackle the pandemic, a host of further questions are then raised about how data should or should not be used; intellectual property rights; limitations on data re-use; how long data should be used for; and ultimately what should happen to collected data once the pandemic is over. There are no concrete answers to these questions; it is all a matter of degree. Policymakers worldwide face a series of stark choices on how to tackle these big issues. In this regard, mutual learning and the sharing of experiences will be crucial to help inform good practices as they emerge.

As part of its Contracts for Data Collaboration (C4DC) initiative,[1] the Thematic Research Network on Data and Statistics (TReNDS) is documenting the ways cross-sector data sharing agreements are formed and identifying issues that help strengthen the responsible and lawful processing of personal data. As part of this effort, the C4DC project is endeavoring to pull together data sharing agreements[2] and other best practice examples relating to how data should be responsibly disposed of at the end of a data sharing agreement.

There are many considerations that determine what happens to data at the end of a data sharing agreement or arrangement. The specific jurisdiction, sector, and resulting legal obligations that may govern data play a large part in determining what happens to data at the end of an agreement. From an analytical point of view, this creates limitations on what can be done in a short brief such as this one. Providing specific examples of contractual clauses, for instance, becomes hard as they are entirely jurisdiction-specific and may be misleading to policymakers in different jurisdictions. Moreover, given the unprecedented use of digital technology to respond to the COVID-19 pandemic, many countries are taking drastically different approaches, again making direct comparisons difficult.

In light of the above, this brief examines the potential of sunset clauses or sunset provisions to be a legally binding, enforceable, and hence accountable way of ensuring COVID-19 related data sharing agreements are wound down responsibly at the end of the pandemic. Sunset clauses stipulate how a piece of emergency legislation should come to an end. Sunset provisions are clauses in data

1 Contracts for Data Collaboration. (2020). https://contractsfordatacollaboration.org

2 Examples can be found in the C4DC online repository. https://contractsfordatacollaboration.org/library/

sharing agreements that determine what will happen to the data at the end of the agreement. This is a term that was not commonly used before the COVID-19 pandemic. This brief builds on C4DC's work to date, including the recently published "Laying the Foundation for Effective Partnerships: An Examination of Data Sharing Agreements"[3] report, and aims to clarify some of the issues that emerge when policymakers consider the potential of sunset clauses to help them responsibly use and eventually wind down the use of sensitive data as part of their COVID-19 responses.

The brief is divided into four substantive parts and is rounded-off with concluding thoughts. Part I introduces sunset clauses as legislative tools, highlighting a number of examples of how they have been used in both COVID-19 related and other contexts. It also shows their potential value as a tool to eventually wind down the use of sensitive data to trace and track individuals. Part II discusses sunset provisions in the context of data sharing agreements and attempts to explain the complex interrelationship between data ownership, intellectual property, and sunset provisions. Building on this, Part III identifies some key issues policymakers should consider when assessing the utility and viability of sunset provisions within their data sharing agreements and arrangements. Finally, Part IV highlights the value of a memorandum of understanding (MoU) as a viable vehicle for sunset provisions in contexts where data sharing agreements are either non-existent or not regularly used.

In this document, data that can identify an individual shall be referred to as personal data. In the context of COVID-19, personal data might include data points that can be used to ascertain an individual's location. Data that cannot identify an individual shall be referred to as non-personal data. These types of data might include privately held administrative records that indicate the availability of personal protective equipment (PPE) public health officials use to tackle the virus. Non-personal data does not include personal data that has been anonymized.

Summary of Findings

The research that underpins this brief used a combination of desk review and informal interviews. It has resulted in three findings (elaborated on in this brief) that highlight issues that merit further exploration and research:

- Sunset clauses could be effectively used in existing emergency power legislation to limit the risk of governments using sensitive data beyond the end of the pandemic.
- There is an opportunity to introduce sunset provisions into legally binding agreements around data sharing as part of the COVID-19 response to help safeguard rights and limit the future use of personal data.
- In contexts where data sharing agreements are not routinely used to set terms for data sharing, a memorandum of understanding between parties engaged in data sharing during the COVID-19 pandemic could be used to stipulate how sharing can be wound down.

3 Dahmm, H. (2020). UN Sustainable Development Solutions Network's Thematic Research Network on Data and Statistics (SDSN TReNDS). Laying the Foundation for Effective Partnerships: An Examination of Data Sharing Agreements. https://static1.squarespace.com/static/5b4f63e14eddec374f416232/t/5ee3e249b07a7d49fa6da34e/1591992905052/Laying+the+Foundation+for+Effective+Partnerships-+An+Examination+of+Data+Sharing+Agreements.pdf

PART I: GOVERNMENT LEGISLATION

In the context of government legislation, a sunset clause sets a time limit on a piece of legislation, or part of the legislation, whereby after a certain period of time it will no longer apply. A government must enact new legislation or provide for future parliamentary assessment and approval if it wishes the legislation to continue to apply after the time period expires. Sunset clauses are often used in exceptional situations, for example where emergency powers have been granted to deal with a crisis, including the COVID-19 pandemic.

Prior to the COVID-19 pandemic, sunset clauses have been applied to legislation adopted after terrorist attacks in Section 21 of the *Terrorism Prevention and Investigation Measures Act 2011* in the United Kingdom (U.K.); the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* in Australia; and in surveillance provisions in Section 215 of the *USA Patriot Act*. They may also be introduced where there is an element of experimentation or novelty, which may require a short period of application to assess whether it would be desirable to make the provision permanent. The European Union's Action Plan against Disinformation included a code of practice[4] that was subject to a 12-month sunset clause so its effectiveness could be explored, rather than committing to strict regulatory requirements at the outset.

Sunset clauses are now being incorporated into some countries' COVID-19 related emergency legislation. In the U.K., the *Coronavirus Act 2020* emergency legislation was enacted to deal with the pandemic. Its provisions are designed to expire after two years.[5] Similarly, in other jurisdictions, emergency legislation enacted to deal with the pandemic has been created only to take effect for a specific period of time. For example, Singapore's *COVID-19 (Temporary Measures) Act 2020*[6] and Canada's *COVID-19 Emergency Response Act 2020*[7] set out different time periods for the various sections in the acts to apply. In Israel, the *Emergency Regulations (Novel Corona Virus – Restrictions on Activities), 5780-2020,*[8] which imposed strict restrictions on movement, lasted only seven days.

Contact Tracking and Tracing Data

Globally, there is particular concern about data collected and its future use for contact tracking and tracing mobile phone applications, or apps.[9] Contact tracing involves the use of a type of surveillance

4 European Commission's Code of Practice on Disinformation. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

5 See Section 89(1) of the *Coronavirus Act 2020*. The period for expiry for different parts of the Act may be shortened or lengthened by further regulations according to Section 90 of the Act. https://www.legislation.gov.uk/ukpga/2020/7/contents/enacted

6 *Covid-19 (Temporary Measures) Act 2020.* https://sso.agc.gov.sg/Act/COVID19TMA2020/Historical/20200407?DocDate=20200407#pr3-

7 *Covid-19 Emergency Response Act 2020*. https://laws-lois.justice.gc.ca/PDF/2020_5.pdf

8 *Emergency Regulations (Novel Corona Virus – Restrictions on Activities), 5780-2020*. https://www.hfn.co.il/files/33644eb87c7b31fec816c438bc737c55/Emergency%20Regulations%20-%20Corona%202020%20%28update%29.pdf

9 Open Rights Group. (2020). Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights. 2 April 2020. here: https://www.openrightsgroup.org/publications/joint-civil-society-statement-states-use-of-digital-surveillance-technologies-to-fight-pandemic-must-respect-human-rights/

data. National governments are creating apps that utilize Bluetooth Low Energy technology on mobile phones to monitor the proximity of infected individuals with other individuals. The use of technology in this way is unprecedented and will connect people who are unknown to each other to particular locations and times, creating the potential for mass surveillance. Potential further uses of data have highlighted many issues that could lead to discrimination in employment, immigration, policing, and access to services.[10]

To resolve these issues, politicians, researchers, and non-governmental organizations have suggested governments introduce legislation that includes sunset clauses to avoid future use of surveillance data and possible future infringement on individuals' rights. In the context of contact tracing, the European Data Protection Board, an independent body comprised of representatives from the EU's national data protection authorities, has recommended that "personal data should be kept only for the duration of the COVID-19 crisis. Afterwards, as a general rule, all personal data should be erased or anonymized."[11]

The European Commission made recommendations to "develop a common approach for the use of technology and data to combat and exit from the COVID-19 crisis," known as the Toolbox, for the use of data collected through mobile applications and anonymized mobility data.[12] The European Commission recommends limiting the use of personal data to tackling COVID-19 and ensuring it is not used for law enforcement or for commercial purposes by "set[ting] appropriate sunset clauses, so as to ensure the processing does not extend beyond what is strictly necessary for those purposes."[13] A further recommendation is that personal data is "irreversibly destroyed, unless, on the advice of ethics boards and data protection authorities, their scientific value in serving the public interest outweighs the impact on the rights concerned, subject to appropriate safeguards."[14] Further data sharing with third parties is excluded. The European Commission has also suggested deleting data after 90 days or, at the latest, when the pandemic is declared under control.

Some countries have adopted this approach. France's StopCovid contact tracing app has integrated deletion provisions to remove information about an infected user once their contacts are notified. France plans to phase out the app six months after it declares the end of the health emergency. France's data protection authority, Commission Nationale de L'Informatique et des Libertés, has also recommended that users have a right to erase pseudonymized data (personal data that is de-

10 *Covid-19 (Temporary Measures) Act 2020.* https://sso.agc.gov.sg/Act/COVID19TMA2020/Historical/20200407?DocDate=20200407#pr3-

11 See paragraph 35 of the Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak. Adopted on 21 April 2020. European Data Protection Board. here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

12 European Commission's Toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.here: https://ec.europa.eu/futurium/en/european-ai-alliance/toolbox-use-technology-and-data-combat-and-exit-covid-19-crisis-particular

13 See (10)(1)&(10)(2) of the European Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020H0518

14 See (10)(3) of the European Commission Recommendation (EU) 2020/518 of 8 April 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020H0518

identified).

The Australian government approved legislation specific to data protection in the context of its COVID-19 app on 15 May 2020. *The Privacy Amendment (Public Health Contact Information) Act 2020*[15] includes provisions that data from the COVIDSafe app must not be retained on a communication device for more than 21 days, and that data will be deleted from the national data store once it is no longer required to prevent or control COVID-19.

In the U.K., the Joint Committee on Human Rights presented a report highlighting its deep concerns regarding the use of mass surveillance of personal data for a COVID-19 tracing app, where there has been no scrutiny by the public or by Parliament.[16] It has proposed a bill[17] to regulate the use of information for contact tracing and connected purposes, which includes the deletion of contact tracing data once it is no longer required for contact tracing, and upon request by an individual. The bill also proposes the anonymization of data as soon as possible after collection, defining anonymization as data that "can no longer be attributed to a specific individual either alone or in conjunction with other data."

Some are advocating that the technologies that are created, as well as the personal data collected, be deleted at the end of the pandemic, given the potential for misuse and possible future infringements on individual rights. The Ada Lovelace Institute recommends that "legal and technical sunset clauses must be built into the design of new powers and technologies" so technical and legal infrastructure built during the pandemic is also dismantled.[18] Google LLC and Apple Inc. have created specific application programming interfaces (API) for COVID-19 apps to work effectively on their phones. The APIs are limited in use and are not available to all app developers. Each nation is only permitted one app, which is developed by its national health authority. Google LLC is also planning to sunset the APIs once the health crisis is over. [19]

The Relevance for Data Sharing

The legislative introduction of sunset clauses to the use of data collected during the COVID-19 pandemic — most likely in relation to personal data — is highly relevant in the context of data sharing. Organizations process personal data on a particular legal basis, such as consent or public

15 *Privacy Amendment (Public Health Contact Information) Act 2020*. https://www.legislation.gov.au/Details/C2020A00044/Html/Text

16 Joint Committee on Human Rights. (2020). Human Rights and The Government's Response to Covid-19: Digital Contact Tracing. 6 May 2020. Accessed 1 July 2020. https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/343/34302.htm

17 U.K. parliamentary Joint Committee on Human Rights. Proposed Bill. https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/correspondence/Letter-to-Rt-Hon-Matt-Hancock-MP-Secretary-of-State-for-HSC-Draft-Bill.pdf

18 Ada Lovelace Institute. (2020). Exit through the App Store? Should the UK Government use technology to transition from the COVID-19 global public health crisis. 20 April 2020. Accessed 3 July 2020. https://www.adalovelaceinstitute.org/exit-through-the-app-store-how-the-uk-government-should-use-technology-to-transition-from-the-covid-19-global-public-health-crisis/

19 According to Google's Chief Privacy Officer, Keith Enright, speaking at Wirewheel's Spokes 2020 Privacy Technology Conference on 17 June 2020. https://wirewheel.io/spokes-2020-recap/

interest, depending on the laws of the relevant jurisdiction. Where personal data is lawfully shared on a basis provided by emergency legislation, the legality of the continued use of data will be affected once emergency legislation ends. Data sharing arrangements must comply with any introduction of specific legislation that includes sunset clauses regarding the use of COVID-19 data.

PART II: DATA SHARING AGREEMENTS

The terminology used to describe agreements and contracts that regulate data sharing between organizations is not applied consistently within and across different jurisdictions. For example, a data sharing agreement may sometimes be referred to as a data processing agreement or an intellectual property licensing agreement. In Europe, there is a distinction between a data sharing agreement and a data processing agreement in relation to personal data.[20] A data sharing agreement is where two organizations share personal data and have the authority to determine how they independently use data. A data processing agreement is where one organization has been instructed to use or do something to the personal data with specific requirements, but is not authorized to use the personal data in other ways.

Agreements may refer to personal data, non-personal data, or both. Where personal data is concerned, the agreement will contain stipulations relevant to the laws that govern such data in the particular jurisdiction. For example, in Europe, the *General Data Protection Regulation 2016/679* (GDPR) governs the use of personal data. Each Member State will have enacted legislation to supplement it. There may also be particular data sharing laws that apply to specific industries. For example, the *Council Directive 2004/82/EC* on the obligation of carriers to communicate passenger data and *Directive 2016/681* on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime apply to the aviation industry. In the United States, the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* contains data protection rules that apply to the health sector. In the U.K., the *Coronavirus Act 2020* legally requires food retailers to provide information to the government, if requested, about food supply disruption.[21]

Where data has been provided to another party on the basis of a license, there will usually be a data licensing agreement, rather than a data sharing agreement. A data licensing agreement specifies how data is to be used, the terms of the license, and the fees for the use of data. Most agreements — whether data licensing, data sharing, or data processing — will typically include clauses that outline the duration of the agreement, how the agreement may be terminated, and the parties' obligations when the agreement ends. There may be factors or events that trigger the early termination of an agreement. These factors will all be relevant in determining what happens to the data at the end of the agreement.

20 Sometimes referred to as personally identifiable information (PII) in other jurisdictions.

21 See Sections 25 and 28 of the U.K. *Coronavirus Act 2020*. https://www.legislation.gov.uk/ukpga/2020/7/contents/enacted

Data Ownership, Intellectual Property, and Sunset Provisions

The intangible nature of data and the ease with which it can be replicated and shared makes it difficult from a legal point of view to define it as property. There is often misunderstanding in the use of the term ownership in the context of data, particularly in relation to personal data. Personal data is not owned by the person to whom it relates nor to the organization that uses it. Rather, the organization has rights and responsibilities in the use of that personal data. In some jurisdictions, there are laws that give individuals rights over their personal data, whether it be privacy, data protection, or consumer rights.

In the lifecycle of personal and non-personal data, the value created and extracted at various points usually involves multiple stakeholders. This further complicates the concept of ownership in relation to data, which is not compatible with exclusive rights for any one stakeholder. The only legal rights that come closest to ownership are intellectual property rights, trade secrets, and to some extent confidentiality.

This is important to understand in the context of data deletion, including COVID-19 related personal data. Globally, the question of data ownership is complex, with some legal uncertainty surrounding the ownership, re-use, access to, and liability arising from data use and data sharing. This problem has become particularly acute as organizations and governments across the world are pressured to find solutions to an unprecedented health and economic crisis as a result of COVID-19. The sensitive nature of health and location data makes sharing such data particularly challenging.

For this reason, privacy advocates suggest that clauses are inserted into data sharing agreements to specify that personal data be deleted or anonymized at the end of the contract or after a set period of time. As outlined in Part I of this document, organizations may be legally obliged to delete data as a consequence of emergency or COVID-19-specific legislation. However, in the absence of such legislation, they may choose to incorporate sunset provisions into agreements of their own volition. Where the basis for processing COVID-19 data is of public interest, once the pandemic is over, it may no longer be lawful or desirable to continue to use the data. Purpose and use limitations are key data protection principles and are paramount to good data governance, although their enforcement can be challenging. Where COVID-19 data is processed for purposes that are tangential to the pandemic, the legal basis for data processing will need to be carefully examined and documented prior to entering into any data sharing agreement.

PART III: VOLUNTARY SUNSET PROVISIONS: ISSUES TO CONSIDER

International organizations, governments, companies, or other stakeholders considering incorporating voluntary sunset provisions into data sharing agreements that result in the processing of personal data to tackle COVID-19 must address a number of issues across the following areas:

Intellectual Property Rights

In the context of intellectual property rights, it is necessary to consider the rights to data that may be created through the data sharing agreement to assess whether deletion is possible, and if so, what parameters can be set. Foreground intellectual property is intellectual property that is made, developed, or created in connection with an agreement. It may also be referred to as new, arising, resultant, or project-specific intellectual property. If the original data is processed or combined with other data to create derived, co-mingled, or resultant data, agreements usually define and specify intellectual property rights in relation to this data. Where data has been made open, there is usually a license upon which data can be used. Deletion will not be relevant in these circumstances, as the data is already openly available.

Mandatory Deletion

There are scenarios where, by law, data must be deleted at the conclusion of an agreement. Under Europe's GDPR, it is mandatory for data processing agreements to contain a clause that specifies that personal data must be deleted or returned at the end of the contract, unless Member State law requires it to be stored.[22] This means that further use of the data by the company processing the data[23] is not permitted. Under the GDPR, data sharing agreements do not have this strict requirement, giving organizations flexibility to determine what happens to personal data at the end of the contract. However, any further use of personal data must be compatible with the legal basis for the initial collection and must comply with the principles of the GDPR.

There may be other deletion obligations that arise within the legal framework of a particular jurisdiction. In Europe, the GDPR gives data subjects the right to request the erasure of their personal data under certain conditions.[24] Whilst there is an exemption to erasure in the GDPR for reasons of "public interest in the area of public health"[25] and for "archiving and research purposes,"[26] it is necessary to carefully assess whether the exemptions apply to the parties and their specific use of COVID-19 data. It may be that a valid erasure request would require data to be deleted in advance of any sunset provision date.

Retention Obligations

In certain jurisdictions, there may also be legal obligations to retain data, which impact an organization's ability to make sunset provisions in their contracts. In some countries, communications service providers must retain some types of electronic telecommunications data and keep records of financial

22 GDPR Article 28(3)(g). https://eur-lex.europa.eu/eli/reg/2016/679/oj

23 Defined as a data processor in the GDPR.

24 GDPR Article 17.

25 GDPR Article 17(3)(c).

26 GDPR Article 17(3)(d).

transactions, so law enforcement agencies can have access to data for future investigations.[27] *European Union Directive 2016/681/EU* makes it mandatory for airlines to retain passenger flight records to prevent and investigate terrorist offences and other serious crimes.

Anonymization and Further Use of the Data

An important question for organizations considering sunset provisions is whether or not it will apply to data that has been anonymized or de-identified. This does not include non-personal data, which will not identify an individual. It is also important to make the distinction between anonymized data and de-identified data. The latter is referred to as pseudonymized data in European data protection law.[28] The process of anonymization removes identifiers so data can no longer be linked back to an individual. However, true anonymization, where it is not at all possible to re-identify an individual, is especially difficult to achieve in practice. Given the advances in big data analytics and the availability of data on the Internet, it is becoming easier to link anonymized data to openly-available data, or other available data, to individuals to re-identify them.[29] It may also be possible to infer sensitive personal data by linking together different datasets. An assessment of the risk of re-identification is usually undertaken to determine how close to true anonymization a de-identification technique has come.[30]

Anonymization and de-identification often reduce the usefulness of data to the organizations using it, and may therefore not be desirable or achievable for data sharing. In some scenarios when applied to health data, anonymization may make it difficult to return a diagnosis or link it back to an individual to whom the data relates. If a sunset provision is included in a data sharing agreement where anonymization or de-identification is being applied, the parties will need to decide whether the anonymized or de-identified COVID-19 data will also be subject to deletion.

Artificial Intelligence and Machine Learning

Organizations are seeking to further develop machine learning, artificial intelligence, and data analytics in the healthcare sector for screenings, diagnosis, analysis of clinical findings, genomics, and the development of treatments and medicines. Large quantities of data are required to train and develop such systems, and for the functioning of some systems. Even once data has been used to create such a system, it may still be necessary to maintain data in a form where individuals can be re-identified to test the veracity of the model or system at a later date, or to respond to any challenges to its results.[31] Therefore, where COVID-19 data is being used in this context, it is unlikely that the voluntary adoption of sunset provisions in data sharing agreements will be possible. However, this

27 Note that joined cases *C-293/12* and *C-594/12 Digital Rights Ireland and Seitlinger and Others, EU:C:2014:238* invalidated the EU Data Retention Directive 2006/24/EC that permitted the blanket retention of data, but Article 15(1) of Directive 2002/58/EC (e-Privacy Directive) still allows Member States to enact data retention legislation, although this is currently under judicial scrutiny in a number of European countries.

28 See Article 4(5) of the GDPR for the definition of pseudonymized data.

29 Sweeney, L. (2015). Only You, Your Doctor, and Many Others May Know. *Technology Science*. 2015092903. 28 September 2015. Accessed 1 July 2020. https://techscience.org/a/2015092903/

30 See Recital 26 to the GDPR, which sets out the factors that should be taken into account to determine the likelihood or re-identification. https://www.privacy-regulation.eu/en/recital-26-GDPR.htm

31 Salami, E. (2019). Artificial Intelligence (AI), Big Data and The Protection of Personal Data in Medical Practice. *European Pharmaceutical Law Review*, Volume 3, Issue 4, pp. 165–175.

does raise ethical questions about how such data should be used to train algorithms, and how access to any commercial or other benefits derived from data should be distributed equitably in future.

Timing of Deletion

When should COVID-19 data be deleted? In the absence of legislation-specific sunset clauses in relation to the use of COVID-19 data, this is a difficult question to answer. The long-term impact of the pandemic is not yet known, and further outbreaks, or waves, of COVID-19 are likely to occur. For this reason, it may be that COVID-19 data will need to be held for a long period of time until there is certainty that the crisis is truly over or an effective vaccine is found. Some organizations may choose the deletion date as fixed against government measures of the crisis, so that once the national emergency status is downgraded to the lowest level, it will be appropriate to delete the data. The factors to consider will depend upon the specific purpose of the data sharing agreement, its context, and the sensitivity of data being shared.

PART IV: INFORMAL AGREEMENTS

In contexts where data sharing agreements are not mandatory or where legislation is weak or non-existent, some organizations may opt to enter into a partnership on the basis of common understanding and purpose rather than formalizing their arrangements in a contract or agreement.

Within the context of COVID-19, a number of data partnerships aimed at providing data to help tackle the pandemic are emerging across the world. In Africa, for instance, the United Nations Economic Commission for Africa (UNECA) and the Global Partnership for Sustainable Development Data (GPSDD)[32] are brokering and supporting many of these partnerships. Interviews with GPSDD's Director of Programs, Davis Adieno, and Victor Ohuruogu, Senior Africa Regional Manager,[33] undertaken as part of the research for this brief shed light on some of the mechanisms that are being used in lieu of formalized contracts.

While it is not the only informal mechanism used to establish a data sharing arrangement, an MoU[34] is a document that outlines arrangements between parties without the legal formalities of a binding legal contract. It is one of the more common informal agreements used to set out the terms of data sharing in the absence of a binding contract. Generally, MoUs are not legally binding in their entirety, but rather a statement of the parties' intentions in relation to their specific relationship. However, an MoU, or parts of it, may become legally binding if the formalities required to form a legal contract exist within the content of the MoU. How and when this might happen depends entirely on the jurisdiction in which the MoU is formed.

MoUs have emerged as one of the preferred modes of establishing the terms of COVID-19-related data sharing arrangements in countries where more formalized structures are absent. Interviews with Mr.

32 https://www.uneca.org/stories/covid-19-data-resilient-africa

33 Interview with Davis Adieno and Victor Ohuruogu, 26 June 2020.

34 Sometimes also referred to as 'heads of terms' or 'letters of intent.'

Adieno and Mr. Ohuruogu highlight that although these documents are informal in terms of their legal enforceability, they are often the result of protracted processes of negotiation and rely largely on trust built over time between the stakeholders involved to mitigate risks and harms. These arrangements, which may include MoUs, do not currently appear to contain provisions setting out terms for how personal data sharing will be wound down at the end of the pandemic. There are a number of reasons for this, including the fact that many of the arrangements between governments and data providers, such as telecommunications companies and data processing and analytics firms, do not actually share personal data, but rather aggregated statistical data. Moreover, the intention at the point of exchange is often to establish a lasting partnership, as opposed to a temporary partnership focused solely on addressing the pandemic.

Typically, MoUs will describe the partnership, the common aims or objectives, each party's use of resources, and performance dates. They may also contain a process for any disputes to be resolved or termination provisions. MoUs are flexible and can be adapted to reflect the parties' interests and motivations. They can also include terms that address privacy and confidentiality. Notwithstanding their informality, it is also possible for MoUs to incorporate sunset provisions in a similar way to data sharing agreements. Should the organizations choose to adopt a sunset provision for the use of certain data within their arrangement, this can be outlined in the MoU in similar terms to those found in formal data sharing agreements.

For the MoU to be effective in relation to a sunset provision, it should clearly describe the data that is subject to the provision, the timing for deletion, and how the parties will give effect to it. The parties should consider the circumstances where incorporating sunset provisions within MoUs might be beneficial and explore how such provisions could help mitigate data misuse. There are multiple factors to consider, and the same issues outlined in Part III of this document will also be relevant where an informal agreement is reached.

CONCLUSION

The COVID-19 pandemic has led to an unprecedented global public health crisis, requiring governments to act quickly to prevent loss of life and address the resulting economic and social consequences. Globally, there is particular concern about data that is being collected and the future use of that data once the emergency is over. The introduction of sunset clauses in government legislation to require the deletion of COVID-19 data has been proposed as a possible solution to allay these concerns. As highlighted above, in some countries, emergency powers are now already subject to sunset clauses. Organizations sharing COVID-19 data may want to consider the impact on their arrangements if such legislation is introduced, or adopt sunset provisions within their data sharing agreements or MoUs.

Finally, the research that underpins this brief has resulted in three findings that highlight issues that merit further exploration and research:

- **Sunset clauses in existing emergency power legislation could be an effective way of limiting the risk that governments will use sensitive data beyond the end of the pandemic.** Any sunset clause in emergency legislation must be subject to democratic oversight mechanisms and frequent review by legislative decisionmakers. The example of contact tracking and tracing data suggests that to ensure that individuals' rights are upheld during the crisis, personal data collected to tackle COVID-19 should only be used for epidemiological purposes, and not for law enforcement or commercial purposes.

- **Legally binding data sharing agreements are valuable tools that create enforceable rights and duties over how data should be used as part of the COVID-19 response. Notwithstanding this, based on data sharing agreements that practitioners have shared with the C4DC project to date, voluntary sunset provisions do not appear to be used currently in response to the COVID-19 crisis.** All data sharing agreements should contain provisions that stipulate how data sharing should end and what should happen to any data at the end of the agreement. Further research is needed to better understand how practitioners would view the value of sunset clauses and provisions, the issues that could arise in their inclusion, and the reasons that may lie behind the absence of explicit sunset provisions or deletion requirements within contracts involving COVID-19 related data. It is also crucial that stakeholders considering entering into data sharing agreements that involve sensitive COVID-19 related data consider the complexities and particularities of how many laws around the world treat data, and in particular, the data ownership and intellectual property implications of any agreement they seek to enter. These issues are especially important as they go to the heart of debates about how various parties to an agreement reuse and recombine data. In the context of the COVID-19 pandemic, given the sensitivity of data that is often involved, it is important that each party's legal rights to (re)use and (re)combine sensitive data for purposes other than epidemiological and related uses is limited contractually, to uphold fundamental human rights and data governance standards.

- **Where data sharing agreements are not routinely used to set terms for data sharing in the context of a COVID-19 response, a memoranda of understanding (MoU) between parties engaged in data sharing can be used to stipulate how sharing can be wound down. Voluntary sunset provisions can also be used within MoUs.** Whether within a data sharing agreement or an MoU, parties should consider issues, including:
    - The purpose of the agreement.
    - The legal basis for using COVID-19 data (e.g., whether it is based on specific legislation that might later be amended to include a sunset clause, a public interest basis arising from a legal source other than legislation, data subjects' consent, or merely a contractual obligation or provision within an existing MoU).
    - The duration of the agreement.
    - Whether an agreement can be terminated early, and if so, under what conditions.
    - Intellectual property rights and the creation of new intellectual property, including issues pertaining to reusing and recombining data.
    - Any existing legal obligations to delete or retain COVID-19 data.
    - Anonymization or de-identification and further use of COVID-19 data.
    - The use of COVID-19 data in machine learning or training of AI systems, including for future commercial gain.

ABOUT THE AUTHORS

This brief was produced by DataReady on behalf of the Thematic Research Network on Data and Statistics (TReNDS).

The lead author, Melissa Stock, is DataReady's legal consultant and a practising barrister at Normanton Chambers in London. She specializes in information and privacy law and advises organizations, public authorities, and individuals in all aspects of data use.

Tom Orrell is DataReady's Founder and Managing Director, as well as a TReNDS' expert member. Tom is a non-practising barrister whose work bridges digital and data policy, human rights, and sustainable development.

CONTRACTS
FOR DATA
COLLABORATION