Smart Data Privacy Laws

Achieving the Right Outcomes for the Digital Age

June 2019

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com and public policy website at www.gsma.com/publicpolicy

To view the GSMA's related resources online, visit www.gsma.com/mobileprivacy

Follow the GSMA on Twitter: @GSMA and @GSMAPolicy

CONTENTS

Introduction

Sensing the huge opportunity of digital transformation, governments are keen to establish a regulatory environment that supports data-driven economic growth while strengthening trust in technology. Many countries are therefore considering data privacy laws for the first time, while others are reappraising their existing approaches.

In today's global economy, organisations' use of personal data can no longer be contained or regulated in isolation within a single country. The future frameworks that will allow governments, businesses and, most importantly, individuals to benefit from the data revolution must respect national laws, traditions and cultures. However, they must also coalesce around an emerging consensus that data privacy laws should protect the privacy of individuals while enabling innovation and data flows critical to the digital economy.

This paper provides a resource for those involved in drafting and reviewing data privacy rules or legislation — distilling what has been learned from data privacy law implementation to date into guiding principles by which a proposal can be measured.

In brief, for a data privacy law to be successful, it must provide effective protection for individuals while allowing organisations the freedom to operate, innovate and comply in a way that makes sense for their businesses and can secure positive outcomes for society. The law should be guided by principles that put the responsibility on organisations to identify and mitigate risks while remaining flexible, technology- and sector-neutral and allowing data to move across borders easily.

Without these guiding principles, there is a serious risk that the resulting law or regulations will end up being too prescriptive, too rigid and too rapidly outdated. Conversely, if these guiding principles are adhered to, all stakeholders can win: organisations can prioritise their resources to achieve effective privacy outcomes while operating and innovating responsibly; supervisory authorities[1] can target their resources to focus on prevention of harm; and governments and individuals can enjoy the economic and societal benefits of digital transformation safely.

An individual's privacy should be at the heart of any smart data strategy. People must be able to trust the data-driven businesses, governments and digital ecosystem that they engage with on a daily basis. If individuals trust the organisations that use their data, then governments and industries, including the mobile industry, can benefit through greater uptake of new technology and business ideas, increased economic activity and a thriving, digitally enabled population.

To achieve this, a smart approach to data privacy is needed, comprising four key areas:

- **A data privacy law** that empowers and protects individuals and encourages innovation to benefit society
- **Organisations with privacy practices** that focus on the minimisation of risk of harm to individuals
- **Supervisory authorities** that are able to prioritise their functions and resources to target the most pressing risks of harm — educating individuals and businesses, encouraging good practice and enforcing appropriately
- **Individuals** who are equipped with the information and tools they need to make informed choices about how their data may be used and to understand the value exchange they are engaged in

This paper focuses on the first of those areas and is intended as an aid to those who are involved in drafting or reviewing proposed rules relating to data privacy. It considers the drivers for and advantages of general data privacy laws and then sets out some guiding principles aimed at ensuring effective privacy outcomes for governments, organisations, society and, most important, individuals.

1. In this paper 'supervisory authority' is used to refer to any data protection authority or other authority with a supervisory function that covers the privacy implications of using data.

Drivers for the Adoption of Horizontal Data Privacy Laws

In the digital age, successful businesses rely on advanced analytics to obtain actionable insights from data. Much of this data is personal data that relates to identifiable individuals. New business models, technologies and capabilities such as the Internet of Things (IoT), big data analytics and artificial intelligence (AI) often rely on a large volume of personal data and therefore have the potential to impact people's privacy. To realise the benefits of data-driven innovation for society and the economy, individuals need to be empowered and trust that their data is being used fairly and securely.

The rules that govern the use of personal data vary significantly, however — from sector to sector, from technology to technology and from country to country. This can be confusing for people who rightly expect the same protection regardless of who is using their data and how it is processed.

In addition, laws can quickly become outdated in the dynamic, rapidly changing digital ecosystem, and the traditional sectoral approach is becoming less relevant.

Organisations can find it challenging to navigate this complex regulatory landscape. For example, a company that sells smart home devices such as internet-enabled lightbulbs, televisions or washing machines is forced to distinguish between rules that cover the internet and e-commerce, rules that cover electronic communications and rules that cover data privacy more generally. This is particularly relevant for the mobile industry as it diversifies into new areas and increasingly provides the platform on which new, data-driven business models and technologies can thrive.

It has also become clear that enabling cross-border data flows in a way that protects privacy can be mutually beneficial for the economy and society. Countries are therefore aligning their approaches and cooperating more on enforcement.

Against this backdrop, many countries and regional bodies around the world are considering the adoption of a general data privacy law for the first time or are overhauling their existing frameworks. Whether economies are less developed or more developed, less digital or more digital, the high intensity of legislative activity on data privacy is likely to continue over the next few years.

Set out below are some of the advantages policymakers and legislators should take into consideration.

Horizontal data privacy laws cater to fundamental interests and economic considerations

General data privacy laws have always had a dual focus. Primarily, their goal is to protect the fundamental rights of individuals to privacy, particularly as the volume of personal data and the quality of insights have increased so rapidly in recent decades. However, it has always been recognised that the ability to use and move personal data in a responsible way is important for economies and society. Many innovations that benefit individuals owe something to insights gained from personal data. For example, the ability of expectant mothers to seek medical advice through their mobile phone in remote areas of poor countries can improve individual as well as public health outcomes. A general data privacy law can therefore help governments seize opportunities for sustainable and inclusive development arising from increased connectivity, mobile broadband penetration and digital transformation.

Horizontal data privacy laws foster trust

Higher levels of trust in digital technology can encourage people to engage more with new technologies and innovations which, in turn, will boost the economic and societal prospects of a country. A horizontal data privacy law typically provides individuals with the protection they need to trust in digital technology without distinguishing between different technologies or sectors. Individuals should feel assured that they are simply protected whenever their data is processed. This can act as a valuable tool for fostering trust.

Horizontal data privacy laws adopted in other countries can facilitate cross-border data flows and local data-driven economic activity

With so many countries[2] now having or adopting data privacy laws, there is potential for some level of international alignment that allows governments to cooperate and trust each other's regulatory framework. In particular, supervisory authorities from countries that have general data protection laws are more likely to cooperate effectively to protect individuals' privacy. This makes it more likely that data can flow to where it is needed, stimulating local data-driven economic activity and societal gains.

Horizontal data privacy laws provide a platform for enhancing business reputation

Businesses also gain from operating under general data privacy laws. Where companies hold themselves to a high standard of data governance and privacy, they can gain a competitive advantage. When operating across multiple jurisdictions, companies often choose to adopt a high global standard, even when it means they go beyond what is strictly required in some of those countries, because it is more effective to embed a consistent culture of privacy across the organisation, and because it helps to demonstrate their commitment to responsible data management externally, fostering trust and brand loyalty.

2. According to UNCTAD (Data Protection and Privacy Worldwide 01 April 2018) as of 01 April 2018 there were 107 countries that have data privacy laws in place. According to Professor Graham Greenleaf (Global Tables of Data Privacy Laws and Bills (5th Ed 2017)) as of 01 June 2017 there were 120 countries that have data privacy laws in place.

Horizontal data privacy laws reduce the need for sector-specific privacy rules

General data privacy laws apply to the processing of all personal data, regardless of the technology used or the sector in which the processing takes place. When governments introduce a data privacy law that applies in this horizontal way, they also create an opportunity to review legacy sectoral rules.

This is highly relevant to the communications sector, which has always sought to protect the confidentiality of communications and the privacy of its users. Without a high standard of privacy and confidentiality, consumers would find it hard to trust in the communications networks they use. In many countries, this concern for privacy and confidentiality has become encoded in sectoral laws or within the conditions of the licences under which networks are obliged to operate.

With communications now proliferating over the internet and, increasingly, between objects connected to a variety of networks, a general data privacy law can provide the common rules that everyone must follow and an opportunity to eliminate redundant sectoral requirements.

For example, the adoption of the General Data Protection Regulation (GDPR)[3] in the European Union sparked a review of the so-called 'e-Privacy Directive' that regulates communications and traffic data.[4] Similarly, in India, certain conditions of the operating licence that applies to mobile network operators deal with the confidentiality and privacy aspects of traffic data.[5] These could be rendered superfluous if the proposed Indian data privacy law is adopted.

3. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DA
4. When a mobile network operator provides a communication service (including browsing the internet or connecting to devices via the cellular network), the network generates data about the time, duration, origin, destination and location of the communication. This is often referred to as traffic data, but is also known as metadata or call detail records (CDRs).
5. See India Unified Licence Conditions sections 37.1 (privacy of communication and no unauthorised interception), 37.2 (privacy & confidentiality of information relating to a third party), 37.2 a) (non-disclosure), 37.3 (confidentiality of information relating to the customer), 37.4 (parties acting on operator's behalf), 39.20 (retention of data), 39.23 (viii) (prohibition of transfers of subscriber accounting information or user information).

Guiding Principles for Smart Data Privacy Laws

This section sets out a number of principles to guide the construction of any data privacy framework suited to the data-driven age. It is intended particularly for those engaged in the proposal and scrutiny of new data privacy laws (or substantial revisions to existing data privacy laws) around the world.

The local context

For those considering a new data privacy framework, the starting point should always be the national or regional context:

- How important is privacy as a concept in local culture?
- How will individual behaviours and approaches to privacy be affected by digital transformation?
- What does the country's constitution say about privacy or related topics?
- What laws have already been adopted in this space to reflect local concerns?
- How do the local economic circumstances and data flows intersect with data privacy?

These are all questions that should be considered before drafting proposals for new data privacy laws or frameworks.

However, subject to such national considerations, it should also be the objective of policymakers to find as much alignment as possible with international data privacy frameworks to aid interoperability and cross-border data flows that are critical to economies at a national, regional and global scale.

Existing data privacy frameworks

Existing frameworks adopted by other countries, regions, multilateral organisations and supervisory authorities[6] can be extremely useful reference points for countries developing data privacy laws for the first time. However, there is no one-size-fits-all solution. While the EU's updated general data privacy law, the GDPR, has gained significant attention in recent years, it is by no means the only framework and may not suit the context of, or state of, privacy awareness in a particular country. An investigation of existing frameworks should therefore avoid a 'copy and paste' approach and instead be a genuine attempt to find the most appropriate inspiration from a broad range of existing frameworks. Appendix 1 sets out a non-exhaustive list of such frameworks and where to find them.

Accountability

A data privacy law should incentivise and/or require accountability mechanisms, drawing on good practice that exists in other legal instruments.

Rather than thinking about data privacy in terms of mere compliance with specific rules or adherence to administrative formalities, the concept of accountability suggests organisations should adopt 'effective mechanisms that deliver real protection'.[7]

Placing accountability at the heart of a general data privacy law brings with it benefits for all stakeholders:

Individuals benefit because organisations are required to think beyond mere compliance and instead implement effective measures to identify risks and prevent harm from occurring. This produces much better privacy outcomes for individuals, as organisations can focus their energy where it really matters.

Organisations benefit because operational priorities can be set according to where the risk to individuals lies, fostering trust and enabling a degree of flexibility to innovate.

Supervisory authorities benefit because they can differentiate between organisations that demonstrate compliance and organisations that do not. This also means that the authorities are no longer burdened with an unrealistic expectation that they have checked everything. Instead, they can direct their resources strategically and efficiently in pursuit of privacy protection for individuals.

To implement the idea of accountability effectively, three key elements[8] are required:

- Accountability in law
- Accountability in practice
- Accountability incentives

6. |Supervisory authorities can coordinate their actions through memoranda of understanding, through bodies such as the International Conference of Data Protection and Privacy Commissioners or through dedicated networks such as the Global Privacy Enforcement Network. In this context, the Madrid Resolution issued by data protection authorities under the ICDPPC (see Appendix 1) can be considered a relevant framework.
7. WP168 - Article 29 Working Party Opinion on The Future of Privacy adopted 01 December 2009 (The Article 29 Working Party was the forum in which the supervisory authority from each EU Member State met. This has been superseded by the European Data Protection Board established under the GDPR).
8. WP173 - Article 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010.

Accountability in law is achieved when the law requires organisations to implement appropriate and effective measures, as a duty, and to be able to demonstrate compliance to the supervisory authority.

Accountability in Law

1. Duty to implement appropriate and effective measures to ensure compliance
2. Duty to be able to demonstrate implementation of effective compliance measures

Accountability in practice is achieved when an organisation implements effective measures to comply with the requirements of data privacy law. Such measures can range from the appointment of a data protection officer to adoption of risk assessment procedures and are usually aimed at embedding a culture of good data privacy practices throughout the organisation. For simplicity, these are often organised into certain functional categories.[9]

Accountability in practice

Category	Examples of Measures
Leadership	Board-level buy-in, adoption of strategy Appointment of a data protection officer
Policies and procedures	Policy for staff Data inventory Procedure for assessing new processing Privacy-by-design
Risk assessment	Data privacy impact assessment
Transparency	Template notices for regular use cases
Training and awareness	Staff training Website guidance
Response and enforcement	Data breach reporting Subject access and other rights request Complaints Staff disciplinary process
Monitoring and verification	Periodic review of programme Internal and/or third-party audit

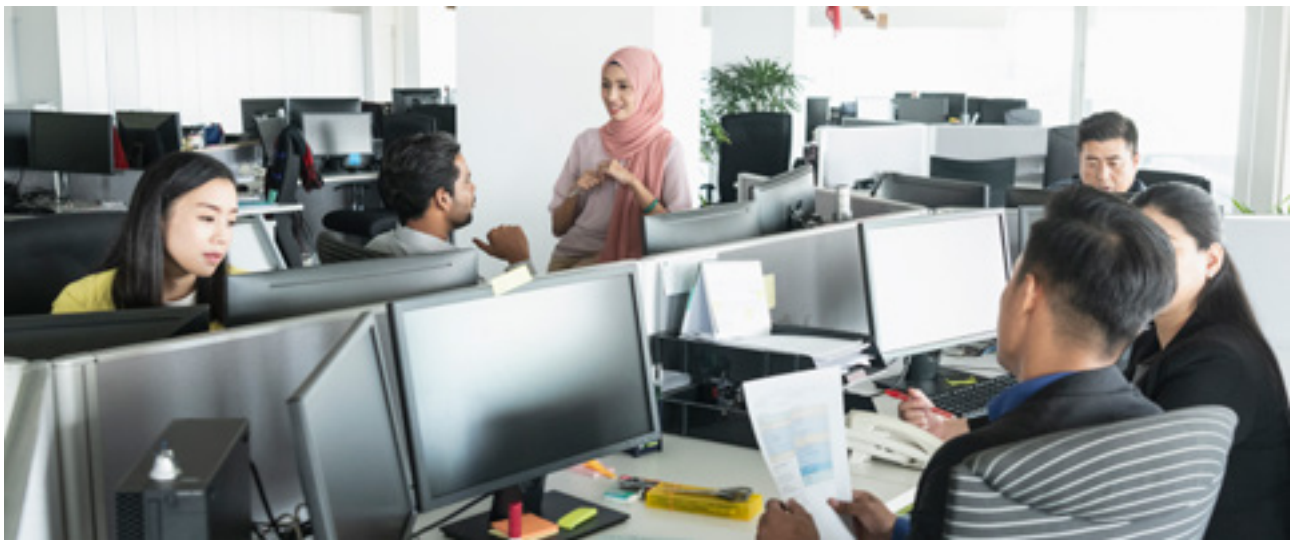
9. For example, leadership, risk assessment, policies and procedures, transparency, training and awareness, monitoring and verification, response and enforcement. See for example the privacy management approach proposed by Nymity (Privacy Management Accountability Framework – A Practical and Operational Structure for Complying with the World's Privacy Requirements) or the concept of 'Organisational Accountability' promoted by CIPL (The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, Centre for Information Policy Leadership, 23 July 2013).

Accountability incentives come in different forms. Although organisations already have an incentive to be accountable due to the enhanced reputation and trust they can foster among their customers, there is also a net gain to supervisory authorities and individuals as more organisations embrace an effective approach to privacy. Cutting-edge data privacy laws should, therefore, also incentivise accountable practices. This may be in the form of reduced administrative requirements such as the removal of detailed registration requirements, the provision of mechanisms to demonstrate accountability (as mentioned above) or for supervisory authorities to take an organisation's good practices into account when determining sanctions.

Mechanisms such as the EU Binding Corporate Rules, APEC's Cross Border Privacy Rules, codes of conduct or certification schemes under several international instruments[10] including the GDPR provide organisations with a clear way to demonstrate their accountable practices. These can also act as an incentive to organisations to adopt accountable practices.

Accountability Incentives

- Avoid detailed registration requirements to register processing activities with the supervisory authority
- Provide accountability-based mechanisms in a way that reduces administrative burden and can act as a stamp of approval, e.g.:
  - Binding corporate rules
  - Codes of conduct
  - Certification
- Law enables accountable practices to be taken into account when deciding:
  - Whether or not to initiate an investigation
  - The appropriate level of sanction in infringement cases
- Allow accountable practices or mechanisms to be relied upon in contractual contexts
- Provide mechanisms to allow cross-border data flows based on accountable practices



10. Certification is now recognised as a possibility under the GDPR. Other forms of certification also exist through bodies such as the International Standards Organisation which administers a set of standards for information security (ISO27000). Although these may not focus entirely on data privacy, they can support the demonstration of accountable practices by an organisation.

In addition, in the mobile context, different accountability mechanisms are emerging. For example, the GSMA's IoT Security Guidelines[11] are already achieving widespread recognition, while a certification for Mobile Money[12] has been developed to demonstrate to consumers and regulators how the system implements effective safeguards. Other industry initiatives that require some form of accountability or adherence to common principles include Mobile Connect.[13]

A smart data privacy law should:

- Embrace the concept of accountability by including explicit duties for responsible organisations to implement effective measures to comply and to be able to demonstrate that such measures are in place.
- Encourage organisations to adopt accountable practices (e.g., maintain a data privacy function or data protection officer, keep appropriate records, conduct data privacy impact assessments and implement Privacy-by-Design) to the extent that such duties support the idea of accountability.
- Insert provisions into the law to incentivise accountable practices:
  - Detailed requirements to register processing activities with the supervisory authority should be abandoned in favour of organisations keeping appropriate internal records
  - The need to obtain prior authorisations should be kept to a minimum, relying instead on the accountable practices
- Allow organisations that implement responsible data management practices to benefit from simplified mechanisms to allow them to transfer data across borders (such as Binding Corporate Rules, APEC Cross-Border Privacy Rules or certifications).
- Allow accountable practices implemented by an organisation to be a factor when assessing whether or not to initiate an investigation and what level of sanction is applied.

11. GSMA IoT Security Guidelines. www.gsma.com/iot/iot-security/iot-security-guidelines/.
12. GSMA Mobile Money Certification, April 2018: gsmamobilemoneycertification.com.
13. The GSMA's Mobile Connect solution: https://mobileconnect.io/ and Mobile Connect Privacy Principles.

Principles-based

Data privacy laws should not be too prescriptive. Instead, they should operate on the basis of principles[14], so as to ensure flexibility and accommodate changes in business practices and technology. In a similar way, laws should focus less on how compliance is achieved and more on the desired outcome. For example, mandating a specific encryption standard may not be the best way to achieve the desired outcome of keeping personal data secure. A specified technical standard in law may become outdated very quickly. A principles-based law would achieve the desired outcome by requiring the organisation to implement a level of security that is appropriate given the nature of the data, the context in which it is processed, the state of art of information security technology and practices, and the cost. A principles-based approach also helps countries to find essential equivalence between their respective frameworks which can support the establishment of cross-border data flow mechanisms.

At the heart of many data privacy frameworks are common principles that are generally accepted such as fairness and transparency, purpose limitation, necessity, proportionality, the legitimacy of data processing, limited retention period, keeping data secure, and ensuring data is accurate, sufficient and up to date. This paper does not go into these principles as they are reasonably well understood[15], and instead focuses on those key elements of modern data privacy laws that make them successful.

A smart data privacy law should:

- Be based on principles and avoid obligations that are too specific

14. Many of the frameworks listed in Appendix 1 are based on common principles that can be traced back to the earliest multilateral attempts to address privacy: the OECD Guidelines of 1980 and the Council of Europe's Convention 108 of 1981.
15. See for example the ICO guidance on privacy principles https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. Most of the frameworks listed in Appendix 1 include reference to such core principles.

Risk-based

General data privacy laws should focus on the risk of harm to individuals. Obligations or duties that do not focus on the risk of harm result in checkbox approaches to compliance that bring little value to individuals and undermine the credibility of the law. For example, a requirement to consult the supervisory authority whenever a certain type of data or technology is used does not take into account the context of the processing or the safeguards put in place by the organisation. It would therefore impose an unnecessary burden on organisations and it would swamp supervisory authorities with unnecessary consultations. A risk-based approach would require an organisation to carry out its own risk assessment; to the extent consultation with the authority is included in the framework, it would be obliged to consult the authority only in exceptional circumstances. The same philosophy should be applied throughout the data privacy law.

A risk-based approach would also include the concepts of privacy-by-design and data privacy impact assessments. Privacy-by-design requires organisations to identify and mitigate risks throughout the lifecycle of a product, service or process. Data privacy impact assessments are a mechanism used by organisations to evaluate the impact on individuals of certain high-risk processing activities. It may be desirable to have these practices mandated by law, as they enable tailored approaches to privacy protection rather than a one-size-fits-all approach. This prevents the need for more prescriptive provisions set out in law.

A smart data privacy law should:

- Adopt a risk-based approach throughout
- Ensure each provision targets the risk of harm to individuals
- Include privacy-by-design and privacy impact assessments

Horizontal (sector- and technology-neutral)

General data privacy laws usually apply to any processing of personal data, regardless of sector or the technologies used. This represents a positive for consumers, as it gives them a consistent level of protection without having to worry about what technology they are using, or whether the activity they are engaged in has specific rules or not.

A horizontal approach benefits all organisations that make use of personal data and defines a common baseline in the data economy, providing clarity and facilitating competition for all participants.

The introduction of a horizontal general data privacy law provides a useful opportunity for governments to review legacy sectoral rules. This is of particular relevance in the communications sector, which has always had a concern for privacy at its core. With communications now being possible over the internet and, increasingly, between objects connected to a variety of networks, a general data privacy law can provide the common rules that everyone must follow. A beneficial consequence of this is that redundant legacy rules concerning privacy in sectoral laws, guidance or telecom licence conditions can be reviewed and removed to avoid confusion.

In a modern, digital world, personal data should be subject to the same protections, regardless of whether it is collected via a website, a mobile application, a connected device, a retail establishment or a communications provider.

A successful data privacy law should:

- Apply horizontally to any processing of personal data regardless of the sector or the technology used
- Provide a common baseline for all actors in the digital ecosystem and data-driven economy
- Provide an opportunity for governments to review legacy privacy rules in sectoral laws, guidance or telecom licence conditions and, where possible, to remove them

Balancing *ex ante* and *ex post*

In a fast-paced digital world, it is impossible for supervisory authorities to scrutinise all data processing activities in advance ('*ex ante*'). It makes more sense to set clear rules and give organisations a duty to implement effective measures and be able to demonstrate compliance (see Accountability section) while retaining the power for supervisory authorities to intervene after the event if something goes wrong ('*ex post*'). For example, the GDPR moved the EU's data protection regime firmly away from an *ex ante* approach towards an *ex post* approach, rejecting complex registration requirements in each EU member state in favour of accountability and internal recordkeeping.

The benefits of such an approach are far-reaching. It enables supervisory authorities to request information from organisations, to investigate or to impose sanctions or seek other corrective measures if needed. Importantly, it also allows supervisory authorities to be strategic in how they set their priorities and manage their limited resources with the result that they can focus their energy on the risk of harm to individuals rather than administrative burdens.

This approach represents a significant burden on organisations to keep good internal records and implement comprehensive programmes, but it also means that they can focus their energy where the risk lies rather than being tied up in administrative tasks that, ultimately, do not serve the individual.

While it is important to move from an *ex ante* approach to an *ex post* approach, this does not mean that all *ex ante* activity should cease. In order to facilitate a more accountability-based system of oversight, supervisory authorities, third-party verification agents and industry will still need to engage positively before processing starts for certain mechanisms. For example, certifications and codes of conduct that enable companies or industry sectors to demonstrate their compliance may need prior scrutiny before they can be relied upon.

If the law focuses on *ex ante* for accountability-related mechanisms, it can leave day-to-day responsibility for assessing and avoiding risk to organisations rather than creating unrealistic expectations that supervisory authorities can check a piece of processing in advance.

A smart data privacy law should:

- Avoid or minimise unnecessary prior approval requirements
- Replace any existing duties to register details of data processing activities with a duty to keep internal records
- Ensure that internal record-keeping duties are not too prescriptive
- If a registration duty is kept, require only the minimum essential pieces of information to keep in contact with organisations
- Focus *ex ante* activity on accountability mechanisms such as certifications or codes of conduct that provide more general permissions to process data

Personal data

The definition of personal data should be broad enough to capture any information from which a living individual can reasonably be identified. This avoids multiple rule sets and definitions of personal data that compete or even contradict each other, which would be contrary to the 'horizontal' principle.

The law should recognise that whether some types of data are to be considered personal depends on factors such as the ease with which data can be linked to an individual and any commitments organisations have made with regard to linking data.

For example, a mobile phone number or IMEI[16] on its own may not seem like personal data at all, but when combined with account data or other information held by the recipient, the identity of the phone user could be discovered.

A smart data privacy law might also recognise that data can fall on a spectrum of identifiability.[17] Anonymised data is, by definition, not personal data. Pseudonymised data from which individuals can be potentially identified, for example, where the same organisation holds a data set that enables re-identification of the data, may be considered to be personal data. Given that analytics activity may often rely on the use of pseudonymised data, modern data privacy laws have begun to define pseudonymisation and recognise that it can be an effective safeguard to mitigate privacy risk.

If the law seeks to prohibit re-identification, special care should be taken to target only those actors with malicious intent and to have a high threshold for legal liability. For the sake of legal certainty, it would also be desirable to clarify exceptions, for example, for research, for day-to-day business operations or where the vital interests of the individual are at stake.

A smart data privacy law should:

- Include a sufficiently broad definition of personal data to give the law horizontal effect
- Make the definition of personal data subject to a test of likelihood of identifiability
- Acknowledge that certain obligations do not apply to pseudonymous data
- Avoid or set a high threshold for legal liability in regard to re-identification

16. International Mobile Equipment Identity Number used to identify valid mobile phones and those that have been reported as stolen
17. The Future of Privacy Forum has developed useful material on the subject of de-identification and how identifiable data is. https://fpf.org/issues/deid/.

Consent and lawful grounds for processing

A general data privacy law should provide organisations with a range of lawful grounds on which they can process personal data. While consent can be appropriate in many instances, overreliance on consent can lead to 'consent fatigue', thus rendering poor privacy outcomes for individuals. Smartphone users, for example, have become accustomed to a barrage of requests from apps and other service providers to consent to collection of data from their devices. Although these can be controlled through systems preferences or dashboards, it is unreasonable to think that every user has the time to fully consider what they are agreeing to. The individual's withdrawal of consent can also represent an unreasonable burden, for example if consent can be withdrawn for activities related to the prevention of fraud or the improvement of products and services.

Responsible data analytics-based services will become increasingly important to achieve public policy goals and drive economic growth in the near future. Any consent collected from the consumer in this context could only be extremely general. More flexible grounds for processing are therefore needed to allow the private and public sectors to innovate while fully protecting consumers' privacy.

Such additional lawful grounds for processing can include processing that is necessary for compliance with legal obligations, for performance of a contract, to protect vital interests of the individual, and for legitimate interests of the controller which requires the organisation to balance competing interests and risks. Further processing of personal data should also be allowed, where it is compatible with the original purpose and, where consent is the most appropriate option, there should be a range of ways in which organisations can collect consent.

A smart data privacy law should:

- Recognise that consent can have serious shortcomings including 'consent fatigue' in certain circumstances
- Avoid exclusive reliance on consent
- Focus also on transparency and giving the individual the information and tools they need to understand how their data is processed
- Provide a range of lawful grounds for processing including 'legitimate interests'
- Allow processing where it is compatible with the original purpose for which the personal data was collected

Rights

Individuals need strong data privacy rights to be able to understand what data an organisation holds about them and to exert a reasonable level of influence over the use of that data. They also need to be able to seek redress if those rights are not respected. This is key to individuals having trust in new technologies and business models.

Such rights may include the right to:

- **Subject access** – It is important that individuals, or 'data subjects', are able to find out who is processing what personal data that identifies them. This right gives individuals the power to obtain a copy of any personally identified information an organisation holds about them.
- **Explanation** – Although organisations have traditionally had a duty to provide information to individuals about what data they are collecting and why, this sometimes appears as a right in law to have the process and methods of using data explained to the individual. This is potentially important in the fields of data analytics and artificial intelligence in which algorithms play a key role and may be difficult for people to understand.
- **Objection** – In the absence of a right to deletion, empowering individuals to object to processing can provide a useful tool for individuals to ask the organisation to stop processing data about them.
- **Correction** – Individuals may merely wish for inaccurate data to be corrected. However, where the organisation disputes the correction requested, such rights usually allow the organisation to continue with the original data as long as they record the difference of opinion.
- **Deletion** – More recently, data privacy laws have gone further, allowing the individual to ask for data about them to be deleted. This kind of right is also sometimes dubbed a 'right to be forgotten'.
- **Data portability** – The GDPR has introduced a new right for individuals to require organisations to transmit data directly to another organisation. The implications of data portability for individuals and for the economy are not yet fully understood. Any proposals to include such a right would therefore have to be considered very carefully.

The above list is neither exhaustive nor a minimum. Each of these rights should be considered on its own merits, and carefully crafted exceptions should guard against unintended consequences. For example, organisations should not be required to re-identify data that is not maintained in personally identifiable form or to build data systems for the sole purpose of fulfilling access requests. There should also be a limit as to how far an organisation has to go to unearth and redact data and organisations should be protected from repeated, frivolous or vexatious requests. A right to deletion may need to be balanced with exceptions for the public interest such as fraud protection or journalistic freedom. Data portability may provide an exciting foundation for the evolution of the digital and data economies, but implementation of such a right must also be cognisant of the impact on competition and investment.

A smart data privacy law should:

- Include strong rights for individuals so that they can understand and influence data processing and seek redress when things go wrong
- Understand the impact of proposed rights on all stakeholders, the economy and society
- Include appropriate exceptions and qualifications to guard against unintended consequences

Data breach notification

In the EU, mobile operators have long since been under a duty to report data breaches to the authorities. Data breach notification duties are a useful tool for raising awareness generally, and they can encourage organisations to keep improving their data security arrangements due to the reputational damage that such disclosures cause.

However, over-notification to individuals can be counterproductive, as it leads to fatigue and undermines trust generally. Therefore, if a rule is proposed to notify individuals of breaches, it should only apply where the breach is likely to cause a high risk of harm to the affected individuals. For example, a public disclosure on the internet of one million bank account details and passwords would certainly merit notification to the affected individuals, whereas it may be counterproductive to report the loss of a document containing the names of attendees of a business meeting.

The timing of the notification to the supervisory authority can also be an issue. Organisations need time to establish whether a breach has occurred and take remedial action. A sensible approach is therefore to set a general standard (e.g., 'promptly' rather than a specified number of hours or days) for the time in which a data breach needs to be reported and for the clock to start only once the organisation has (or should have) established that an incident does amount to a data breach.

A smart data privacy law should:

- Express the time limit for reporting data breaches as a general standard such as 'promptly' or 'without undue delay' rather than a specified number of hours
- Set a threshold for reporting data breaches to individuals based on a high risk of harm to the affected individuals
- Include exceptions for encrypted data, applications, files or hardware

Cross-border data flows

General data privacy laws should allow personal data to flow across borders. Data privacy frameworks such as the OECD Privacy Guidelines[18], the Council of Europe's Convention 108[19], the APEC Privacy Framework[20] and the EU data protection rules have always recognised that protecting personal data goes hand in hand with allowing data to flow. As set out in the GSMA report *Cross-Border Data Flows: Realising Benefits and Removing Barriers*, the GSMA believes that allowing data to flow while protecting privacy has beneficial consequences for society and the economy.[21] If more and more countries see themselves and each other as 'data-connected', interoperable markets with broadly similar rules and the ability to enforce reciprocally, everyone will benefit. Conversely, the more countries impose localisation (also known as data sovereignty) requirements, the more the internet and data flows will become fragmented and isolated. Such restrictive measures could have a devastating effect on the roll-out of new business models such as in the IoT or connected car markets where centralised processing of data collected from remote and often mobile sensors is critical to their viability. They also represent an impediment to cloud computing services which mobile operators both purchase — as they look to leverage the efficiency of the cloud for their own purposes — and provide, taking advantage of the cloud as a business-to-business opportunity. For this reason, the GSMA believes such measures should be avoided.[22]

A general data privacy law should provide an array of mechanisms to allow data to flow[23] while ensuring an adequate level of protection for personal data. The first is that accountable organisations (see Accountability) should be allowed to transfer personal data to other organisations wherever they are located, provided that the accountable organisation is satisfied with the level of safeguards in place. Alternatively, accountable organisations should be given the opportunity to demonstrate the effectiveness of their measures through mechanisms similar to the

18. OECD Guidelines (1980, as amended 2013), Guidelines governing the protection of privacy and transborder flows of personal data, OECD Guidelines
19. 'Convention for the protection of individuals with regard to automatic processing of personal data' adopted first in 1981 and modernised in 2018. There are 54 signatories comprising 47 member states of the Council of Europe and Uruguay, Mauritius, Senegal, Tunisia, Capo Verde, Mexico and Argentina. A protocol strengthening the convention was signed in 2018 and is in the process of being ratified.
20. APEC Privacy Framework (2005): https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework
21. See the GSMA's report from 2018 Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers
22. GSMA Mobile Policy Handbook position on Cross-Border Flows of Data https://www.gsma.com/publicpolicy/mobilepolicyhandbook/consumer-protection#cross-border-flows-of-data
23. For a useful guide to the range of possible data transfer mechanisms, please see Cross-Border Data Transfer Mechanisms, Centre for Information Policy Leadership, September 2017.

European Union's Binding Corporate Rules, the APEC Cross Border Privacy Rules, certifications or codes of conduct. Where such mechanisms are established, administrative processes must be quick and straightforward to improve chances of success.

Another mechanism is to allow data flows to countries that provide an essentially equivalent level of protection. The EU and Japan, for example, have recently agreed to recognise each other's legal framework as providing adequate safeguards. Similar adequacy findings have been reached in relation to a growing list of countries and in relation to the EU-US Privacy Shield.[24] While such mechanisms are a good catalyst for gradual approximation of data privacy laws around the world, it will take a long time before the majority of countries reach mutual findings of adequacy and, in the meantime, it creates considerable complexity for organisations with operations in multiple countries.

In a similar vein, the Council of Europe's Convention 108 promotes the adoption of data privacy laws based on a common high standard set out in the convention. Consequently, and as a matter of law, countries that have ratified the convention can benefit from a free flow of data between them. Indeed, the EU takes Convention 108 status into account when assessing its own adequacy findings and the UN Special Rapporteur on Data Privacy encourages UN member states to sign and ratify the convention.

The law can also enable transfers through contractual commitments, used by organisations, which meet a certain standard or contain specific provisions.

Finally, flows of data can also be allowed on the basis of consent, although this produces significant challenges for organisations, for example when one individual withdraws consent. This should therefore be made available for exceptional circumstances or as a last resort.

A smart data privacy law should:

- Provide a range of cross-border data flow mechanisms
- Allow accountable organisations to transfer data across borders or provide mechanisms for accountable companies to demonstrate they have adequate safeguards in place (approval, certification, code of conduct)
- Provide clarity regarding which countries are considered to have an adequate level of protection
- Allow cross-border data flows on the basis of contractual clauses or consent
- Ensure that administrative processes are minimised, quick and straight-forward
- Avoid or prohibit localisation (data sovereignty) requirements

24. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

Supervisory Authority

Supervisory authorities are an essential part of administering a general data privacy law. They can raise awareness, educate individuals and businesses, encourage good practice, deal with complaints, investigate and take enforcement action and are therefore pivotal in building trust. According to a discussion paper drafted by an ex-Information Commissioner[25], the role of a supervisory authority can be divided between four distinct types of function: 'leader', 'police officer', 'complaint handler' and 'authoriser'. In order to fulfil these functions effectively, the supervisory authority must be independent from direct interference from other parts of government and needs the appropriate powers in law to act, as well as sufficient resources.[26]

Supervisory authorities can be funded in a variety of ways. For example, a supervisory authority might be allocated budget from central government, or may be permitted to keep any fees it collects. In some exceptional countries, supervisory authorities have been funded from fines they impose, but this leads to the obvious danger of skewing the authority's priorities away from its leadership role.

Supervisory authorities are also critical intermediaries when it comes to cross-border data flows, as they need to be able to cooperate in order to carry out functions on each other's behalf in the destination country. Indeed, the APEC Cross-Border Privacy Rules system places great emphasis on 'privacy enforcement authorities' being endowed with sufficient powers and resources to cooperate effectively. The modernised Convention 108 reinforces the power of the supervisory authorities requiring them to provide mutual assistance, coordinate on investigations and conduct joint actions. On a wider scale, other networks such as GPEN[27] have been taking a lead on coordinated enforcement 'sweeps' across multiple jurisdictions. Without such coordinated enforcement activity, the freedom to share data across borders would undoubtedly suffer.

A smart data privacy law should:

- Empower an independent supervisory authority for data privacy
- Grant sufficient powers for the supervisory authority to carry out its core functions
- Mandate that the supervisory authority receives or is able to raise sufficient funds to conduct its functions
- Avoid raising funds from fines
- Encourage the supervisory authority's participation in cross-border enforcement activity

25. Regulating for Results - Strategies and Priorities for Leadership and Engagement, Centre for Information Policy Leadership, 10 October 2017.
26. Before the GDPR, the paper estimates, data protection authority budgets in the EU averaged less than €0.41 per citizen or about €8 per business with low staffing levels. Since the GDPR, budgets and staffing levels have increased.
27. Global Privacy Enforcement Network formed in response to a recommendation of the OECD.

Remedies, enforcement and sanctions

Where the law has been infringed, it is common for the supervisory authority or the courts to consider sanctions (ordering the organisation to do or cease doing something) or remedies (helping the individual to get back to the situation they were in before the infringement took place).

Sanctions and remedies may include non-monetary measures, such as orders to stop processing or to delete data, and in some countries damages can be sought through the courts. Whatever the precise remedies made available under the law, the objective of a smart data privacy law should always be to encourage good practice in the first place and, in case of infringement, to provide genuine and proportionate redress for individuals who have suffered a significant level of harm. This avoids individuals having to resort to private rights of action and protects organisations from frivolous claims. Without the idea of proportionality or a threshold of significant harm, supervisory authorities may waste resources and individuals will not be effectively protected.

If fines are proposed, they should be capped at a reasonable level and supervisory authorities should be required to take responsible data management practices of accountable organisations into account when setting the level of fines or imposing other forms of sanction in order to incentivise the widespread adoption of good practices.

A smart data privacy law should:

- Ensure that any remedies provided in the law aim to achieve effective redress for individuals and are proportionate to the risk of harm
- Set an appropriate harm threshold below which certain remedies are not available
- Include a reasonable cap on the overall level at which a fine can be imposed
- Require supervisory authorities to take responsible data management practices of accountable organisations into consideration when setting fines or other forms of sanction

Conclusion

The opportunities of digital transformation and data-driven strategies are significant. New technologies and business models leverage personal data to deliver real benefits to society and the economy. Those benefits can only be realised if individuals whose data is collected and used can trust in the ecosystem that is emerging around them. Many countries are therefore passing new data privacy laws to protect and empower individuals.

This paper has explored the core principles that should guide those who are involved in the creation of new data privacy laws. For such data privacy laws to be successful, they have to provide genuine, effective protection for individuals while allowing organisations the freedom to operate, innovate and comply in a way that makes sense to them. To achieve this, they need to avoid unnecessary administrative requirements that ultimately do not serve the individual well, and they should avoid being too rigid and prescriptive. Instead, data privacy laws should put the responsibility on organisations to identify and mitigate risks and, in return, be flexible, technology- and sector-neutral and allow data to move across borders easily.

Without these guiding principles, there is a serious risk that the resulting law or regulations will end up being too prescriptive, too rigid and rapidly outdated. Conversely, if these guiding principles are adhered to, all stakeholders can benefit: organisations can prioritise their resources to achieve effective privacy outcomes while operating and innovating responsibly; supervisory authorities can target their resources to focus on the prevention of harm; and governments and individuals can enjoy the economic and societal benefits of digital transformation safely.

A smart data privacy law is one that:

- Takes the local national law, traditions and culture as its starting point
- Finds alignment with existing international norms and data privacy frameworks
- Is underpinned by the concept of accountability
- Is based on flexible principles rather than excessively prescriptive requirements
- Is based on preventing or limiting the risk of harm
- Applies horizontally without reference to a specific sector or technology
- Achieves the right balance between *ex ante* and *ex post*
- Has a definition of personal data that is in line with international definitions
- Provides a range of flexible lawful grounds for processing and recognises the shortcomings of consent
- Includes a range of rights to empower individuals
- Has a pragmatic approach to data breach notifications
- Promotes cross-border data flows
- Establishes an independent supervisory authority for data privacy
- Provides a range of remedies, enforcement measures and sanctions that are proportionate to the harm and take an organisation's good practices into account

Appendix 1: Useful References for Data Privacy Frameworks

Organisation	Title	Link
Asia-Pacific Economic Cooperation	**APEC Privacy Framework (2005)**	APEC Privacy Framework https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework
African Union	**African Union Convention on Cyber Security and Personal Data Protection (2014)**	African Union Convention on Cyber Security and Personal Data Protection https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
Association of Southeast Asian Nations	**ASEAN Framework on Personal Data Protection (2016)**	ASEAN Framework on Personal Data Protection https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf
Council of Europe	**Convention 108+ (1981, amended 2013-2016)** Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223	Convention 108+ https://rm.coe.int/16808ade9d
European Union	**GDPR (2016)** General Data Protection Regulation Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	GDPR https://eur-lex.europa.eu/eli/reg/2016/679/oj
Organisation for Economic Cooperation and Development	**OECD Guidelines (1980, as amended 2013)** Guidelines governing the protection of privacy and transborder flows of personal data	OECD Guidelines https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
Southern African Development Community	**SADC Model Law (2013)** Data Protection: SADC Model Law	SADC Model Law https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf
Red Iberoamericana de Protección de Datos	**Ibero-American Standards for Personal Data Protection (2017)** Standards for Personal Data Protection for Ibero-American States	Ibero-American Standards for Personal Data Protection http://www.redipd.es/noticias_todas/2017/novedades/common/Estandares_eng_Con_logo_RIPD.pdf#Texto%20en%20inglés
Economic Community of West African States	**ECOWAS Supplementary Act (2010)** Supplementary Act A/SA.1/01/10 On Personal Data Protection Within ECOWAS	ECOWAS Supplementary Act https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf
GSMA	**The GSMA Mobile Privacy Principles (2011)** Promoting consumer privacy in the mobile ecosystem	The GSMA Mobile Privacy Principles https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf
International Conference of Data Protection and Privacy Commissioners	**The Madrid Resolution (2009)** Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data	The Madrid Privacy Resolution https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London, EC4N 8AF,
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601