Flexible Data Protection Regulation: Ensuring safe use of new technological opportunities

Telenor exists to connect our customers to what matters most, always striving to empower societies. We believe in the promise of emerging technologies and work to provide new and innovative services while maintaining a firm dedication to fair processing, data protection and empowerment of individuals.

Privacy is important to us. We take pride in protecting our customers' privacy and are committed to earning their trust. We do this by keeping information safe and secure, and by being transparent about how we handle data.

As the value of data grows in the digital economy, privacy and data protection issues become a more and more important subject not just for us and our customers but also for regulators and governments. States have a responsibility to define and enforce an adequate level of data protection[1]. Legal frameworks that encourage trust will enable consumers and companies to meet and grow relationships that lead to opportunities for innovation.

We believe that future policies in the area of privacy and data protection should be built on four basic principles:

1. *International core principles and flexibility: The law should be built on international core principles of data protection and with an application that is flexible enough not to inhibit the adoption of new technologies.*
2. *Consistency and equal treatment: States should ensure a level playing field by adopting a comprehensive data protection regulation enforced by a single and independent regulator.*
3. *International interoperability: Data protection regimes in different countries should be interoperable to minimise barriers to transfer of data.*
4. *Checks and balances: Authority requests should be made only with a valid legal basis and subject to strong oversight. Service providers should be free to be transparent towards civil society and media regarding authority requests.*

We explain and justify these principles in greater detail in the following.

---

[1] Article 12 Universal Declaration of Human Rights; and Article 17 UN Covenant on Civil and Political Rights

Principle 1: International core principles and flexibility

The international core principles of data protection[2], including lawfulness, fairness, purpose-specification and –limitation - should be the cornerstone in any data protection regulation.

The purpose of data protection is to ensure that personal data is protected and it should avoid obstructing the development of new services. Therefore, the international core principles should be applied flexibly. News reports may have highlighted cases where the principles have not been satisfactorily followed by specific businesses or instances where consumers have had bad experiences. While it is tempting to introduce more specific rules when confronted with such cases, policy making should be based on solid evidence, identifying a minimum and proportionate level of protection, and avoiding rules that undermine the potential of existing and future technologies.

A legal framework must be flexible enough to fit low- and high-trust relationships. It should also allow the market to reward companies that innovate and give consumers the treatment they desire. For example, companies with ambitions to offer high value added services based on artificial intelligence will need to build trust by being very transparent and relying on specific consent to process data. Over time, consumers will want the trusted companies to rely more on 'legitimate interest' as a legal basis where they are not unnecessarily asked for permission to process data. This means the purposes in this instance should be 'compatible' with the purposes for which data has been collected. Accordingly, a framework should have flexibility to use both consent and legitimate interest as the legal basis.

Three elements are important to develop a future proof framework that will unleash the potential value of big data analytics:

1. It should in principle be lawful to process personal data where it is necessary for the purpose of the legitimate interests pursued, except where such interests are overridden by the interests or fundamental rights and freedoms of the consumer which require protection of personal data, in particular where the consumer is a child.

2. No rule should exist to prevent personal data collected for a specific purpose from being processed for a different but compatible purpose. Drawing a distinction between learning correlations in data and applying learned correlations to impact individuals, identifying correlations should in general, with appropriate measures in place, be considered a processing for a compatible purpose[3].

3. Lawfulness should be based on facts of the case, and the analysis should consider the reasonable expectations of the consumer, the context in which the personal data has been collected, nature of the personal data, consequences of the processing for the data subject, and the existence of appropriate safeguards such as encryption.

---

[2] Though the principles are not always called by the same name, nor separated from each other in the same fashion, a set of core principles can according to UNCTAD be identified. These principles are the principles of openness, collection limitation, purpose specification, use limitation, security, data quality, access and correction, and accountability. See UNCTAD, 2016, Data Protection Regulation and International Data Flows: Implications for Trade and Development, p. 56. See also Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), 1981; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; UN Guidelines for the Regulation of Computerized Personal Data Files, Resolution 45/95, 14 December 1990; APEC Privacy Principles.

[3] EU Working Party 29 Opinion 3/2013 On Purpose Limitation, p. 46.

Collectively, these elements embody a risk-based approach and allow companies flexibility to introduce and adapt relevant and sufficient data protection measures. For example, it may be possible to reach an acceptable level of risk if a safeguard such as pseudonymisation is introduced to conceal the identity of the individual to the people analysing the data.

Principle 2: Consistency and equal treatment

If a state has adopted a flexible legislation built on international core principles of data protection, there is no need for sector specific regulations of data protection and data protection provisions in licence requirements. In fact, having a single legal instrument equally applicable to all businesses increases the predictability for the consumers; ensures more clarity for businesses, promotes efficient allocation of capital, and prevents inconsistencies in the interpretations of different legal instruments.

In cases where a state finds that sector-specific rules or data protection provisions in licence agreements are necessary, contrary to our view, it is important that the same authority is tasked with the enforcement of all data protection instruments. Having a single, independent regulator improves consistency, increases clarity and promotes efficient use of resources in the public sector. Japan, which has been able to move from more than 30 regulators to only one, is an example to follow for other countries.

As the cross-border nature of business increases, it is important that companies offering services to consumers in different markets are held to the same standards. Where there are differences in legislative and regulatory levels among countries, it is difficult for consumers to feel safe about the use of their personal information. In this respect it is important that laws from different countries are comparable and that privacy authorities engage in international cooperation, establishing lines of communication and tools for cooperation for the benefit of their citizens.

Principle 3: International interoperability

Cross border data transfers are essential to benefit from economies of scale and to drive affordability. In cases where data transfers are either not required or where they are not legally possible, it may be desirable to deploy similar IT solutions locally in different countries. In such instances, data protection regulation can be a barrier to IT deployment if they are not sufficiently harmonised.

Data protection regulations in different countries should not vary more than necessary. From our point of view, states should strive for international interoperability, by:

- Avoiding unnecessary discrepancies between national data protection requirements and requirements in other countries;
- Avoiding unnecessary deviations in issue-specific guidance provided by data protection authorities in other countries; and
- Introducing alternative legal mechanisms for transfer of data.

For example, if data protection legislation in a country offers an 'adequate level of protection essentially equivalent to that within the EU', then the EU Commission may issue an 'adequacy decision'[4]. An 'adequacy decision' makes it possible to treat transfers from an EU country to a non-EU country as an intra-EU transfer, thereby lowering barriers to trade.

[4] EU General Data Protection Regulation, Art. 45.

It should be noted that an 'adequacy decision' can be issued even if the legislation in the non-EU country is not similar; the legislation only needs to ensure an equivalent level of protection. Therefore, states with the desire to strengthen international trade should consider an EU 'adequacy decision'. In particular, states should consider acceding to Convention 108 on Automatic Processing of Personal Data and its Additional Protocol which is a key step towards reaching an 'adequacy decision'[5]. Convention 108 is open to accession by non-European countries.

Principle 4: Checks and balances

Authorities may have legitimate reasons to want to intercept electronic communication. However, checks and balances should be in place. A request for access to personal data should always be proportionate and justified by a valid legal basis. Access should be subject to strong legal oversight and public scrutiny. Providers of electronic communications services should therefore be free to be completely transparent about the access requests received, keeping in mind the need to protect the privacy of the individual whose data will or have been accessed.

How to move forward

Taken together, the four principles of data protection create the case for governments, businesses and organisations to collaborate and support a balanced privacy and data protection regime that will create opportunities to deliver new services and innovation. The use of data will only become more critical over time. It is imperative that we act now to ensure a future-proof framework is in place and can deliver the benefits that citizens and businesses desire.

Telenor is committed to cooperating with global stakeholders to achieve this objective as part of our strategy to be a trusted and secure provider in all markets. This is also an integral part of the process as we have embarked on a digital transformation, and will provide global digital services through the effective use of digital infrastructure and the smart use of data. Our customers want greater control of their digital lives, as well as an open, secure and safe digital experience. In turn, consumer confidence and trust are critical to enable a thriving digital economy.

Telenor and our peers in the telecoms industry can step up and work with governments and partners to protect and respect consumers' data privacy, and enable them to make informed choices about their personal data. Together, we can play an important role in establishing a sound and transparent regulatory framework for privacy and data protection that will serve as a driver for innovation, economic growth and social development.

[5] EU General Data Protection Regulation, recital 105.