Europe

GSMA Europe and ETNO briefing papers on the proposed General Data Protection Regulation

- **Inconsistencies between the GDPR and the e-Privacy Directive**
  Inconsistencies between the 2002 Directive and the proposed Regulation are likely to lead to inconsistent consumer privacy experiences and rights for equivalent services and data. We discuss possible ways to avoid this.
  Articles concerned 2, 3, 4, 31, 89 - Link

- **Applicable law**
  We welcome the proposals in this field, but suggest some key improvements to ensure legal certainty for business and consumers and to ensure European consumers are protected irrespective of from where a service or product is being provided.
  Articles concerned 3, 4, 51 - Link

- **Consent in the online environment**
  We highlight key issues of over-relying on consent and suggest a context-based approach, while highlighting the link with transparency requirements and compatibility issues with the ePrivacy Directive. We propose measures to create consistent and effective privacy experiences for consumers.
  Articles concerned 4, 6, 7, 9, 14, 79 - Link

- **International data transfers**
  We welcome measures to simplify transfers and the codification of Binding Corporate Rules (BCRs). However, we are concerned that related procedural requirements are too strict and call for a review of these.
  Articles concerned 4, 6, 42, 43 - Link

- **Sanctions**
  We highlight the importance that sanctions are not only proportionate but fair, necessary and assist in ensuring effective protection for privacy.
  Articles concerned 15, 28, 32, 79 - Link

- **Documentation obligations**
  We point to the risk that new documentation obligations will lead to costly, time-consuming burdens without improving the protection of personal data.
  Articles concerned 22, 28 - Link

- **Futureproofing the GDPR**
  We express our views on how consistency mechanisms, delegated powers, comitology and self-regulation can play a key role to ensure the future-proofness of this regulation.
  Articles concerned 38, 57, 60, 62, 86, 87 - Link

- **Data Protection Impacts Assessments**
  While supporting PIAs, we suggest improving the text in order to avoid unreasonable burdens to businesses and innovation.
  Articles concerned 33, 34 - Link

- **Data breach**
  We welcome harmonization in this field and point to a few improvements aimed at ensuring that the principle is applied in a fair and proportionate way.
  Articles concerned 31, 32 - Link

Europe

GSMA Europe and ETNO
Briefing paper on the proposed General Data Protection Regulation (GDPR)

Consent in the Online Environment

September 2012

Summary

ETNO and GSMA welcome measures to provide individuals with greater transparency, choice and control over their personal data. However, we believe the new requirements and emphasis on explicit "consent" in the General Data Protection Regulation (GDPR) present significant issues and challenges for both individuals and companies.

- The GDPR expands the current definition of consent to mean a freely given, specific, informed and *explicit* indication of an individual's agreement to one or more notified uses of their personal data. We recommend that the GDPR should limit any requirement for explicit consent to contexts and categories of data that present real privacy risks for consumers;
- An explicit consent model is not suited to the reality of the online world where the collection and sharing of an individual's data takes place in real-time, simultaneously between multiple parties. We believe the Commission's objectives can be better achieved in the GDPR by strengthening privacy by design, self-regulation and accountability;
- The GDPR also requires that consent be indicated by a statement or clear affirmative action. We believe that in many cases, this will frustrate and burden consumers, lead to privacy fatigue, create a tick-box consent culture and undermine the take-up of products and services;
- Companies are required to retain evidence of obtaining consent. This will add costs and other burdens to business and consumers without enhancing privacy;
- The GDPR overlooks the fact that individuals' privacy interests[1] are shaped by dynamic social and economic contexts that increasingly take place in a complex globally connected online ecosystem. We believe this should be addressed and the GDPR should recognize and support contextual and consumer-friendly privacy experiences;
- The GDPR proposes that companies that fail to provide sufficient information and notice under the consent regime will be subject to significant fines. We believe this will prompt companies to provide an excessive number of consent notices to individuals, which will burden and overwhelm them with choices at times not appropriate or consistent with their privacy interests;
- The GDPR proposes that consent will not be valid where there is a significant imbalance of power between an individual and a company. The ambiguity of what constitutes a significant imbalance will result in challenges for companies, contract law and individuals;
- The over-reliance on consent does not reflect other provisions in the GDPR that require greater transparency and that give individuals strengthened rights of access and control over their data. We support these measures together with more contextual ways to help individuals make decisions about their online privacy;

[1] In the context of this paper, privacy 'interests' are expectations, needs, wants and concerns.

- The GDPR fails to create consistent consent rules or consistent privacy experiences regarding the processing of location and traffic data currently regulated by the E-Privacy Directive (2009/136EC). Conflicting provisions in the e-Privacy Directive should be repealed from the e-Privacy Directive by means of the GDPR;
- The GDPR should more strongly support the legitimate interests of data controllers that do not present privacy harms. It should support the use of data in ways that help meet public policy objectives and the creation of broader social and economic opportunities.

Proposed rules in the GDPR

The GDPR expands the existing definition of consent[2]. Under Article 4(8) "'the data subject's consent' means any **freely-given, specific**, **informed** and **explicit indication** of his or her wishes by which the data subject, either by a statement or by a **clear affirmative action**, **signifies** agreement to personal data relating to them being processed." Recital 25 further exemplifies that 'affirmative action' would be "ticking a box when visiting an Internet website".

Article 7(1) requires companies to retain proof that an individual has given consent for one or more 'specified purposes'.

Article 7(4) states that consent "shall not provide a legal basis for the processing [of personal data] where there is a significant imbalance between the position of the data subject and the controller."

Article 4(1, 2) extends the definition of 'personal data' to include an identification number, location data or online identifier from which an individual could reasonably be identified.

Article 79 gives regulators the power to impose fines of up to 1 or 2 per cent of a company's worldwide turnover for not complying with the information and consent requirements.[3]

Issues and impact

The requirement for explicit consent in the GDPR overlooks the increasingly contextual nature of privacy. The importance of context when considering privacy and consent is well established and was first recognised in 1987 by Spiros Simitis[4], one of the first European data protection regulators. What is required in the GDPR is a balanced approach that helps consumers participate in the management of their privacy, in the context in which they are using or accessing services.

The GDPR consent proposals will not necessarily enhance privacy; they certainly will:

- Add costs to (re)design systems and processes to provide consumers additional mechanisms for giving consent and to capture evidence of their consent;
- Burden consumers with excessive information and decision-making requirements;
- Have a negative impact on innovation in technology and data use that presents significant social, economic and public benefits[5].

Impact on consumers

As the proposed regulation is currently written, companies risk large fines for failure to provide sufficient information in transparent ways or for failure to meet the consent conditions. We believe this will lead companies to provide excessive notices, information and choice mechanisms.

---

[2] Under Article *2(h) of the current Data Protection Directive 95/46EC,* 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. Article 7(h) qualifies 2(h) (a) by requiring that "*the data subject has unambiguously given his consent*"

[3] See ETNO GSMA Europe briefing paper on sanctions in the GDPR proposal.

[4] *"… the value of a regulatory doctrine such as 'informed consent' depends entirely on the social and economic context of the individual activity"* Spiros Simits: *Essay: Reviewing Privacy in an Information Society* in the University of Pennsylvania Law Review, 1987. Simitis was Data Protection Commissioner of the State of Hesse (1975-1991)

[5] See European Commissioner Neelie Kroes' support for innovation in healthcare that involves the IoT, mobile etc http://blogs.ec.europa.eu/neelie-kroes/innovating-healthcare/

This could burden and overwhelm consumers with the need to make decisions and choices at times not appropriate or consistent with their privacy interests. The result could be a tick-box consent culture that neither reflects consumers' real privacy interests nor helps them make decisions when it matters in specific social and economic contexts.

An individual may not understand the privacy implications or consequences of the service/product they are using when they first access it and are prompted to give consent via a lengthy notice. What is required is a 'just-in-time' notice and choice approach, rather than rigid formulaic consent mechanisms.

Lengthy legal notices do not help individuals understand what is being asked of them and could result in them paying less attention to notices and consent prompts.

The importance of context and issues of rigid consent mechanisms within the GDPR are even more critical to resolve when considering services enabled by the Internet of Things (IoT). The GDPR proposals are impractical in the context of the IoT, which relies on machine-to-machine communication of data in real time.

For example, an explicit consent regime may require that consumers formally approve the use of their data, by providing their signature, or by ticking a consent box for every modification or every upgrade of an IoT service or application. These will not only burden consumers but may prevent the upgrade of services that are in the individual's interest (for example in health services). It would also add significant and unnecessary cost to business.

Impact on business

Where consent is required under the GDPR, it must be explicit and separate (i.e., it cannot be bundled with other consents). This will add unnecessary costs and administrative burdens to business, as the requirement to collect and maintain evidence of separate and explicit consent will require companies to redesign systems and processes that are built on compliance with existing Member State laws.

It is uncertain whether individuals' existing consent (i.e., consent that has already been secured under current data protection laws) will remain valid if it was captured in ways that do not meet the GDPR's higher standard. Any requirement for companies to resecure consent from individuals will undermine existing business practices and add the cost of communicating with customers or users.

Companies may also face significant challenges under Article 7(4), which states that consent is not valid where there is a "significant imbalance between the position" of the individual and a company. The article is ambiguous and requires further clarification on what might be considered an imbalance in the position between the consumer and providers of services. This is particularly important for services delivered across multiple companies and players in a value chain (e.g. apps, app developers, app stores).

A further issue arises from the relationship between the GDPR and the e-Privacy Directive. The GDPR extends the definition of personal data to include location data and traffic data. These are already subject to the e-Privacy Directive when processed by a telecommunications network provider. The e-Privacy Directive requires the prior consent of individuals before their location or traffic data can be processed to provide value-added services or for marketing. This raises the question as to which takes precedent — the GDPR or the e-Privacy Directive, and which consent standard applies.

Policy considerations

- In today's complex online environments, personal information is volunteered, acquired, derived and inferred from the activities of consumers. Businesses continue to invest in these processes and use data to generate opportunities and benefits to a broad range of actors. The GDPR should place less emphasis on consent and rely more on transparency and business accountability in order to support the personal data economy[6], while respecting and protecting an individual's privacy.
- A focus on accountability — supported by privacy impact assessments (PIAs), privacy by design, codes of conduct and assurance schemes as proposed under Articles 23, 38 and 39 of the GDPR — could help drive an approach to privacy that is more oriented towards consumer privacy interests. This approach is consistent with requests from many policymakers that business avoid lengthy privacy statements and terms and conditions that do little to enhance privacy.
- A requirement for 'explicit' consent for non-sensitive categories of data, and an over-reliance on consent in general, will lead to less privacy for individuals, not more. It will also frustrate and undermine the online user experience, which is crucial to driving growth. The GDPR strengthens the rights of individuals to manage their personal data after it has been collected. These include the right of access, rectification and erasure. Together with obligations on transparency of processing, these rights create significant opportunities for individuals to manage their data in accordance with their privacy interests and ongoing online relationships.
- A better approach would be to contextualise the way consent is expressed by individuals according to the kind of service they are using, the sensitivity of the data and to the potential harm arising from its use. If, in the context of the current proposal, this scalability is not possible, practical alternatives should be sought. These alternatives may include specific instances where explicit consent may not be an appropriate mechanism for protecting privacy, for example where data have been appropriately anonymised, aggregated or pseudonymised[7]. This could encourage the development of business models with enhanced data protection. It could also, as discussed below, support the use of derived data for delivering real social and economic good to societies, communities and individuals.
- The GDPR must recognise and support broader societal and economic objectives. There is the danger of a loss of utility from data derived from mobile and fixed online use. This will significantly impact on the ability to derive social and economic good from such data. Mobile-derived data may help governments meet important public policy objectives such as those related to traffic management. Many governments are seeking to improve traffic congestion in order to reduce noise and air pollution and fuel consumption — this directly benefits societies, communities and individuals. The GDPR should protect the ability to derive social and economic good from Big Data use and more clearly define and protect the legitimate interests of business and broader societal benefits accruing from data. This will require examining concepts of personal data and consent.

[6] The World Economic Forum has explored the personal data economy extensively and recently published a report with further detail, *Rethinking Personal Data – Strengthening Trust*.

[7] See, for example, the UK Information Commissioner's draft code of practice on anonymisation.

About GSMA

The GSMA represents the interests of mobile operators worldwide. Spanning 219 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organisations. The GSMA also produces industry-leading events such as the Mobile World Congress and Mobile Asia Congress.
For more information, please visit Mobile World Live, the online portal for the mobile communications industry, at www.mobileworldlive.com or the GSMA corporate website at www.gsmworld.com.

In the European Union the GSMA represents over 100 operators providing more than 600 million subscriber connections across the region. www.gsmworld.com/gsma_europe

About ETNO

ETNO, the European Telecommunications Network Operators' Association, is the voice of Europe's leading providers of e-communications services and investors in tomorrow's services and infrastructure.

ETNO's 38 member companies and 11 observers from Europe and beyond represent a significant part of total ICT activity in Europe. They account for an aggregate annual turnover of more than €600 billion and employ over 1.6 million people. ETNO companies are the main drivers of broadband and are committed to its continual growth in Europe.

ETNO contributes to shaping an investment-friendly regulatory and commercial environment for its members, allowing them to roll out innovative, high-quality services and platforms for the benefit of European consumers and businesses.

More information: www.etno.eu

GSMA Europe
Martin Whitehead
Director GSMA Europe
Park View, 4th floor
Chaussée d'Etterbeek 180
1040 Brussels
T: +32 2 792 05 56
E: mwhitehead@gsm.org

ETNO
Daniel Pataki
Director ETNO
Avenue Louise, 54
1050 Brussels
T: +32 2 219 32 42
E: pataki@etno.be