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

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

Breach notification

September 2012

Summary

ETNO and GSMA welcome the objectives of the data breach notification obligations in the General Data Protection Regulation: to encourage data controllers to manage personal data securely and foster confidence in third-party data processing. Security has always been of upmost importance for telecom operators, not only to protect our networks but to build trust and confidence among our users.

We welcome the extension of the data breach notification obligation within the proposed General Data Protection Regulation (GDPR) to all data controllers; this will ensure the same rules apply across different service providers and a **consistent protection framework** for European data subjects. However, we believe there are a number of additional issues within the GDPR that need addressing.

- The requirements imposed by the GDPR and the e-Privacy Directive should be aligned by incorporating the rules from the e-Privacy Directive into the GDPR. This helps to **avoid a dual notification obligation** for e-communications providers and a different level of protection for data subjects;
- The **24-hour requirement** for notification of personal data breaches is both impractical and counterproductive;
- Based on experience from the e-Privacy Directive, the GDPR must ensure a **harmonised implementation**, including processes (e.g., a designated competent authority) and formats (e.g., standardised notification forms and single points of contact). Given the limited time frame for notifications and the potential associated sanctions, this process should be as simple and efficient as possible;
- **Not all breaches threaten user privacy.** For the European Union's regime to be workable, the notification must focus on personal data breaches that are likely to have serious and negative consequences for individuals, rather than on all breaches. Controllers should be required to notify supervisory authorities and data subjects only when a breach is likely to lead to significant risk of substantial harm to the data subject and the data subject can be identified, and if no technical measures have been applied to render the data unintelligible.

Proposed rules in the GDPR

Articles 31 and 32 of the GDPR introduce new rules for the notification of a personal data breach to the competent authority and, when the breach is likely to "affect adversely the protection of the personal data or privacy of the data subject," to the data subject.

The notification to the competent authority should be done "without undue delay and, where feasible, **not later than 24 hours** after having become aware of it." The regulation also sets out a minimum level of information to be included in the notification.

Notification to the data subject shall be carried out "without undue delay" and describe the nature of the breach and at least information and recommendations provided for under Article 31 (3) (b, c).

Issues and impact

Alignment with the e-Privacy Directive (2002/58/EC)[1]

Further clarification on the relationship between the draft regulation and the e-Privacy Directive is needed to avoid a dual notification obligation for e-communications providers. We believe requirements need to be aligned by incorporating the data breach rules from the e-Privacy Directive into the GDPR so that the same rules apply for providers granting data subjects the same rights. In consequence data breach rules need to be repealed from the e-Privacy Directive by the GDPR.

Practicality of the 24-hour notification requirement

The 24-hour requirement for notification of personal data breaches is impractical and may even be counter-productive (e.g., due to lack of accuracy): What is essential is the definition of when a company has become aware of a breach. Indeed, the data controller will usually require more time to determine all the circumstances of a breach and its impact on individuals. Internal investigative processes are complex and involve many departments. Moreover, once a data breach has been discovered, the priority for an organisation is to investigate it, limit and contain any loss or damage, and understand how and why it happened so that procedures can be implemented to avoid recurrence. Depending on the nature and scope of a personal data breach, the controller then needs time to understand who is affected and determine the actual harm or risk to individuals.
In the case of a breach in multiple Member States, it is impractical to issue a notification 24 hours after having become aware of it. Reporting a personal data breach before the essential facts are known would not only be premature but could jeopardise an investigation if the breach involves criminal activity or unduly distresses (or causes undue distress to) data subjects, for instance when they do not face tangible harm or cannot take action to protect themselves until more information is known.

Ensuring harmonised implementation

Learning from the e-Privacy Directive's data breach notification requirements, it is crucial to ensure harmonised implementation of the regulation across Member States. This should extend to details such as ensuring notification forms are standard across Member States, and a single point of contact (e.g., a supervisory authority) is designated for major EU-wide incidents to handle notifications on behalf of counterparts in other Member States. This process should be as simple and efficient as possible, given the

[1] As amended by 2009/136/EC

desire to ensure notifications are made without undue delay. Harmonisation should cover both the obligation included in the GDPR and in the e-Privacy Directive.

Practicality of notifying all breaches to supervisory authorities
The GDPR requires that supervisory authorities be notified of *all* breaches regardless of size or severity. This could include the loss of names and addresses used for a mailing list but which data are available in the public domain and whose loss, therefore, will not cause harm. It could also include stolen or lost laptops, tablets and USB sticks, even when these devices have been encrypted. The result is that the authority would be inundated with reports where a breach does not result in harm to individuals. This will undermine the ability of authorities to handle personal data breaches properly. Although Recital 67 recognises this risk, it is clearly not reflected in the relevant articles.

Consumer notification and end-user relationships
The breach notification provisions should also consider that not all providers have a direct relationship with (or can even identify) the end user. We therefore welcome the distinction between the controller and processor. Indeed, processors are typically at least one step removed from individuals using the service and therefore should only notify the controller. Unless it is possible to identify an individual, notification to downstream service providers appears to be the only clear means for upstream business providers to comply with the intentions of the provision. Only the provider with the retail relationship (i.e., the controller) should notify the end user of any personal data breach.

Exemptions
The draft regulation provides for notification exemptions, such as "if the controller demonstrates (…) that he has implemented appropriate technical measures (…) rendering the data unintelligible." While we welcome this recognition, it is unclear why these exemptions do not also apply to the supervisory authority notification process.

Impact on consumers and business
In terms of consumers, breach notification should not cause unnecessary anxiety or overburden the data subject. This could lead to a loss of trust and confidence in the information society or have the opposite effect where, due to the sheer volume of communications to the data subject, reports are simply ignored. For businesses, certain personal data breaches can be complex and business-sensitive. The priority should be to identify and solve the problem first. To be effective, this depends on accurate and complete information that may take some time to gather.

Policy considerations

- The primary focus of the GDPR with regard to breach notification should be to put in place effective and practical processes. A 24-hour requirement for notification of personal data breaches is impractical and counterproductive;
- Incorporate data breach rules in the e-Privacy Directive into the GDPR and repeal them from the first by the latter;
- Controllers should not be required to notify all breaches to supervisory authorities (e.g., stolen or lost laptops, tablets and USB sticks, even when these devices have been encrypted), regardless of size or

severity. This level of notification risks inundating supervisory authorities and undermining their effectiveness in handling important personal data breaches properly. This needs to be further addressed in the draft regulation;

- In essence, given the limited timeframe for notifications and the potential associated sanctions, this process should be as simple and efficient as possible;
- The Commission should also consider recent guidance issued by the European Network Information Security Agency on the 'technical implementation of the Article 4 of the e-Privacy Directive[2]. These recommendations came about as result of the Commission establishing an Expert Group composed of representatives of the EU institutions, the Article 29 Working Party, national DPAs and industry.

[2] http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/dbn

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