telenor

Justisdepartementet
Lovavdelingen
Postboks 8005 Dep

0030 OSLO

Vår dato
14.06.2012

Deres dato
19.04.2012

Referanse
PVS-2012-007

Referanse
201201634 ES
LLE/AHI/mk

Vår saksbehandler:
Personvernombud for Telenor i Norge,
Anders Holt, 47901919

HØRINGSSVAR EU-KOMMISJONENS FORSLAG TIL NYE PERSONVERNREGLER

Telenor viser til Justisdepartementets brev datert 19. april 2012 med invitasjon til høring angående EU-Kommisjonens forslag til nye personvernregler.

Telenor vedlegger ETNO sitt høringssvar om samme sak. Telenor er medlem av ETNO, og Telenors syn samsvarer i det store med ETNO sitt.

Med vennlig hilsen
For Telenor i Norge

Anders Holt

Anders Holt
Personvernombud / LPO

Telenor Norge AS
Hovedkontor

Kontoradresse:
Snarøyveien 30
1331 Fornebu

Postadresse:
1331 Fornebu

Telefon:
67890000
Fax:
67894964

Bankkonto:
7058 06 93936

Hovedkontor:
Snarøyveien 30
1331 Fornebu
Organisasjonsnummer:
NO 982 463 718 MVA

ETNO and GSMA Europe
Joint Statement on the draft General Data Protection Regulation proposal (GDPR)

Brussels, December, 2011

1. Executive Summary

ETNO and GSMA welcome the fact that the current draft proposal for a Regulation addresses many key concerns of our members. We would like to highlight the following issues, which we believe have been addressed in a positive manner within the draft text:

- The choice of the legal instrument being a Regulation represents an important step forward in achieving higher levels of harmonisation within Europe.

- The issue of a consistent user experience is also addressed by extending the scope of the Regulation to all activities directed at data subjects residing in Europe.

- Safe international data transfer is facilitated by the codification and simplification of Binding Corporate Rules (BCRs). Further simplification is, however, necessary.

- The concepts of 'main establishment', the one stop-shop system for data controllers and the concept of applying BCRs to a data transfer within a group of undertakings have the potential to significantly reduce administrative red tape for industry. However, further clarification is necessary.

- The extension of data breach notification obligations to all sectors and administrations would address the concerns of European consumers.

- The support for self-regulatory initiatives and the development of certification and privacy seals is a positive step.

At the same time, some concerns remain:

- The proposed rules on consent are not adapted to the online environment. Privacy is a contextual concern that requires flexible application mechanisms in order to suit consumer expectations.

Legal text proposals: ***new text*** / ~~*deleted text*~~

- The introduction of administrative sanctions of up to 5% of a company's worldwide annual turnover could represent a penalty disproportionate to the gravity of the impact of the infringement.

- The recourse to 'delegated acts' is excessive and should be limited.

- The simple extension of the obligation of the controller to the processor would undermine the development of cloud services in Europe.

- Overlaps with the e-Privacy Directive should be reconciled in order to achieve technology and sectoral neutrality as those issues are covered by both legal instruments.

2. Harmonisation and enforcement

Legal instrument

- ETNO and GSMA welcome the fact that the legal instrument chosen is a **Regulation**. A Regulation will help to achieve full harmonisation, which will foster increased consumer confidence and trust, and which will facilitate the free movement of data in order to strengthen economic growth.

Cooperation of authorities

- We welcome the clear **objective of co-operation** as set out by the Commission in regards to ensuring that national Data Protection Authorities of the Members States (NDPA) apply the Regulation in a consistent manner. We furthermore support the principle of **one leading authority** which is naturally complemented by **mutual recognition** of an enforceable measure taken by a NDPA of one Member State in all Member States (Article 45(2)).

- We consider that the defined **co-operation schemes** mentioned under Chapter VII will be crucial in ensuring a harmonised application of the Regulation. We believe the Commission will need to monitor closely that the co-operation is executed sufficiently in order to avoid divergent interpretations of the provisions of the Regulation. For example, we believe that Article 53 should be extended to include co-operation action as stated in Article 55(4). Furthermore, it is important that mutual assistance and joint operations are carried out in a transparent and timely manner.

European Data Protection Board

- We support the establishment of the **European Data Protection Board** (EDPB). We believe that the Regulation should include clear rules on transparency and the process by which the EDPB seeks input from a broad group of stakeholders to ensure the practical and harmonised application of the decisions. Due to time constraints, open consultation may not always be possible, however, at a minimum, when the EDPB is reviewing the practical application of the guidelines (Article 65(1.c), input from stakeholders should be sought. We suggest to include the following new provision:

  Article 65(1)(h) new: ***where appropriate, and in particular when reviewing the practical application of the guidelines, the European Data Protection Board shall consult broadly and share information and documentation in an open and transparent manner.***

- We furthermore believe that Article 66(1) should build on **transparency** and we suggest the following wording:

  [...]inform the Commission ***and the public, in a timely manner and on a regular basis*** *,about the outcome of its activities[...]*

- Article 65(1) includes the wording 'Advisory Body'. In order to avoid confusion we recommend use of the word 'Board' when referring to the EDPB.

Lead national data protection authority

- To ensure the highest level of harmonisation and a consistent application of the Regulation, there is a need for clear rules to define which NDPA is to be considered the **leading authority** for processing activities for a data controller and data processor. That said, the choice to go with full harmonisation via a Regulation does alleviate the concerns with regards to forum shopping. To further facilitate harmonisation the current definition of 'main establishment' stated in Article 3(13) should be defined in a more precise manner. We propose a definition which is in line with Article 49 of the Treaty and with current case law of the European court of Justice:

  Article 3(13): *'main establishment' means the location within the Union where the controller~~'s~~ or the processor~~'s~~* ***actually carries out its central decision making in relation to any economic activity, irrespective of where the processing of personal data takes place. If the controller does not carry out any central decision making within the Union, the main establishment shall be decided by the habitual residence of the majority of European data subjects whose personal data are being processed by the controller*** ~~*central administration in the Union is located and, in case of the controller, where the purposes, conditions and means of the processing of personal data are determined*~~*;*

- We wish to ensure consistency in the application of Article 75(2) of the Regulation by including a reference to 'main establishment' of the controller or processor.

- We propose that the Regulation clarifies the rule of **Applicable Law** when there is a judicial remedy recourse against a controller or processor. Regardless of the legal framework being a Regulation, differences will be seen, such as rules for the right for compensation, penalty and liability. We propose that the applicable law is based on the law of the country considered to be the main establishment of the controller and processor. This will provide for a consistent application since Article 50 of the Regulation outlines that the NDPA in the Member State of the main establishment will be carrying out the supervision of the processing activities.

Sanctions

- Concerning administrative **sanctions**, we are surprised at the high level of the fines, ranging up to 5% of the infringing enterprise's annual global turnover. Article 79(5) states that the administrative fine should be proportionate and that the amount should be based on the

gravity and duration. The wording of Article 79 correlates with the wording of Article 23(4) Regulation 1/2003[1].

- We consider there to be a need for sanctions to be applied in a similar manner across the Union, however we are worried that the Commission is missing essential differences between infringement of data protection and competition law when copying the provisions for imposing fines. For example *intentionally* under competition law means an intention to *restrict* competition, not an intention to infringe the rules.[2] The sanctions and the structure of competition law are meant to prevent actors from distorting competition which would have negative economic effects on *a specific market*. For data protection, the intentionally (and negligent) infringement of, for example Article 79.2.(a-c)3.(a-c), would not necessarily mean that the data controller does not obey the data protection rules on a general basis but would rather mean that the controller in one instance has not complied with the provision, i.e. not leading to a far-reaching negative effect on privacy protection. We propose that administrative sanctions are put at a level which can be seen as proportionate to the *gravity of the impact* of the infringement.

- It is worth emphasising that in some cases (Art. 42(2))) companies are put in a very difficult position where a **third country judgment for disclosure** has been conducted and the NDPA does not allow the company to obey the judgment. The situation may have far-reaching economical implications and result in uncertainty for a company in the third country. The disclosure of data in a situation where there is no judgment of a court or tribunal may be dealt with differently, however when there is a judgment based on national law in a third country it cannot be considered necessary or proportionate to introduce sanctions on controllers or processors for obeying court orders. We therefore propose a modification of art.79 (4) (j) to take into account these exceptions.

2. The role of self-regulation in relation to delegated powers to the Commission

Self-regulation

- A legal framework for data protection needs to be established for different specific circumstances, products and services as they arise. This is particularly the case when a Regulation is the legal instrument of choice. Today and in the future, Data Protection Authorities (DPA) both at EU level and in the Member States fulfil this requirement by adopting implementing acts, opinions and regulations for specific services and industry sectors – mostly ex-post after data protection issues have been identified.

- However, industry players are best placed to understand the privacy implications of their new services and should therefore take a more central role than DPAs in setting up sector-wide, consistent and binding codes of conduct (CoC). CoC do not replace legal requirements or fundamental rights but rather they help address specific situations, as DPAs do today. Minimum standards for CoC and their development have been provided in Art. 35 GDPR (draft proposal) and should be further strengthened.

---

[1] The Council Regulation on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty

[2] Cases T-305-7, 313-16, 418, 328-29 and 335/94 Re. The PVC Cartell II Limburgse Vinyl Mij NV and others v. Commission 1999, 5 CMLR.

- Art. 27 of the existing Data Protection Directive has failed to deliver self-regulation to date. In order to encourage industry players to draw up CoC, clear incentives need to be evident in the new legal framework. It is important to provide incentives for signatories over non-signatories by allowing them to enforce the CoC in their own manner and to exempt individual companies from DPA supervision, enforcement and fines as long as the respective DPA recognizes the CoC as being functionally operational.

- ETNO and GSMA therefore welcome Art. 35(4) of the Regulation which allows the Commission to enforce sector codes of conduct vis-à-vis all sector undertakings. Self-regulation can be further strengthened by giving industry the right of an opinion on the lawfulness of codes of conduct:

> Article 35(2): *Associations and other bodies representing categories of controllers or processors which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in a Member State. The supervisory authority* ***shall*** ~~***may***~~ *give an opinion* ***as to*** *whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects on these drafts.*
>
> Article 35(3): *Associations and other bodies representing categories of controllers may submit draft Union codes of conduct and amendments or extensions to existing Union codes of conduct to the Commission.* ***The Commission shall give an opinion as to whether the draft code of conduct or the amendment is in compliance with this Regulation. The Commission shall seek the views of data subjects on these drafts.***

Delegated acts

- ETNO and GSMA do however not agree with the excessive recourse to the Commission's delegated acts which should be limited in the draft proposal. Looking at Article 86 alone, one can understand the omnipresence of this type of secondary legislation, especially if compared with the current Directive 95/46/EC where recourse to the Commission's implementing measures appears in just one case (to determine a third country's adequate level of protection). Such measures should only be used when the processing of personal data due to technological and social trends renders clauses of the Regulation out of date. In any case, self-regulation can be a more flexible tool to address these technological and social changes.

- We thus suggest deleting at least all references to delegated acts where the Commission is empowered to define bureaucratic processes, as for example in Articles 10(5), 12(7) and 13(3). Furthermore, regarding the remaining provisions in the Regulation where the Commission may be empowered to adopt more detailed provisions, pursuant to Art. 86, the method of self-regulation might be preferable over delegated acts by the Commission. In order to provide legal certainty, Art. 86 should read as follows:

> Article 86(2): *The delegation of power referred to in Articles [...] shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.* ***Before exercising these powers the Commission shall take due account of existing codes of conducts within the meaning of Article 35. In the absence of these, the Commission should encourage data controllers and processors to develop their own respective codes of conduct.***

Article 86(4): *As soon as it adopts a delegated act, and* ***following due consultation with data controllers, processors and subjects,*** *the Commission shall notify it simultaneously to the European Parliament and to the Council.*

3. Equivalent services, same rules

- ETNO and GSMA very much welcome the change of scope of the draft Regulation which now acknowledges the importance of an equivalent treatment for equivalent services. The proposal to apply the Regulation to every activity directed at data subjects residing within the Union Article2 (2) is a sound way to achieve such equivalent treatment. Moreover, we support the aim of the Union to develop effective international cooperation mechanisms in order to enforce data protection legislation as suggested in Article 43.

- ETNO and GSMA welcome the intention and efforts of the Commission to also achieve technology neutrality, and to adopt a general data breach notification very similar to the system applicable to information society services via the e-Privacy Directive. However, in other areas, such as the use of location data and traffic data (Art. 6 and 9 e-Privacy Directive), differences between the e-Privacy Directive and the proposed Regulation remain. For the sake of a consistent user experience, we call for these issues to be aligned either by reconciling the Regulation with existing legislation or by adding a section in the Regulation which deletes those parts of the e-Privacy Directive that would be covered by both instruments. The changes should be outlined in Article 89 of the Regulation in relation to Articles 2(b), 2(c), 2(f), 4, 6 and 9 of the e-Privacy Directive.

4. International data transfers

- The draft proposal includes several significant improvements compared to the current situation regarding international data transfers. Notably, ETNO and GSMA welcome the codification of the possibility to utilise Binding Corporate Rules for data transfers and the simplification of the approval process for Binding Corporate Rules by only one supervisory authority.

- Furthermore, the recognition of the 'group of undertakings' and the new possibility to use Binding Corporate Rules in order to transfer data within a group of undertakings will allow for a significant reduction in administrative red tape.

- It should be explicitly clarified in Articles 2(17) and 40 of the Regulation that Binding Corporate Rules can also be agreed between controllers and processors that are not part of the same group of undertakings.

5. Key definition and concepts

Data controller and processor

- We propose that the roles of controller/ processor are simplified and that the obligations of the two are differentiated. Concerning the definition of controller - Article 3(5) - we are concerned with the reference to national law as the definition stated in the Regulation should

be determined solely by Union law. The role and purpose of a controller is different from that of a processer, as defined under Article 3 (5-6). Therefore, it is not sufficient to simply extend the obligations of a controller to the processor. If the regulator believes that there is a need to introduce further obligations on processors, there must be special provisions outlining in detail when the processor would have an obligation rather than the controller. There is a need to ensure a clear division of obligations between controllers and processors for achieving innovation and business growth especially in the area of Cloud Computing.

Consent

- Strict rules on consent also need to be practical and adapted to the online service environment. Privacy is a contextual concern that requires flexible application mechanisms. Individuals need to make informed and simple contextual decisions instead of being obliged to answer to mechanisms which systematically require consent. A strict application of the explicit consent rule would massively hinder the development of commercial consumer propositions.

- When it comes to the **online environment,** the concept of consent is a key example of the problematic application of the current Directive and we believe it to be disproportionate for consent to be the primary justification for processing personal information. We are concerned that requiring explicit and affirmative consent (as mentioned in Article 3(8) and in Recital 24 of the Regulation) for all processing activity will ultimately undermine privacy. Individuals will become accustomed to always agreeing to a stated purpose without necessarily understanding what is being asked of them. In addition, it will undermine the user-friendliness of products and services and will therefore slow down the innovative power of online services in particular.

- The Regulation needs to recognize that **consent is dynamic, contextual and operates at multiple levels**. Individuals have privacy interests, concerns, needs and expectations that occur at different points in a relationship with the entities providing services to them and in relation to specific categories and uses of their personal information. ETNO and GSMA support a focus on transparency and ensuring mechanisms by which individuals can meaningfully express their choice and preferences as regards the use of their personal information rather than having an overly restrictive focus on 'affirmative' consent.

- A key objective for data controllers should be to develop easy-to-use mechanisms by which users can make informed choices depending on the context of specific uses of data and the value exchange understood by the individual. For example, a person requesting a location based information service to locate the nearest automatic teller machine, is actively asking to be located, and should not be required to negotiate cumbersome, lengthy, legalistic privacy notices by which they may further indicate their consent. Such impositions would intrude into the user experience and do little, if anything, to enhance the user privacy experience.

- The proposed Articles 5(1)(b) and 12(1)(b) of the Regulation should therefore make it clear that they also cover cases where e.g. a customer requires information based on his/her geo-location and is thus providing his/her authorization for personal location data to be processed. The level of consent required should relate directly to the context, sensitivity and risk of this scenario.

Definition personal data and data subjects

- In regards to the definition of personal data and data subjects, the definitions now build on each other. We believe this creates a level of uncertainty which is unnecessary and we do not understand the need for this structure. We therefore propose the following wording:

> Article 3(1): ***Personal data means data which can identify, directly or indirectly, a data subject, by means reasonably likely to be used by the controller or by any other natural or legal person who may receive the data from the controller, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical physiological, genetic, mental ,economic, cultural or social identity of the data subject*** ~~*'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;;*~~
>
> Article 3(2): *A* ***data subject means a natural person*** ~~*'personal data' means any information relating to a data subject;*~~

Definition of child

- The definition of 'child' should not include teenagers. The rights of teenagers to fully benefit from a responsible online experience and to privacy should be considered. The provision in the Regulation also provides for high legal uncertainty regarding the undertakings obligation to collect and verify the age of its users.

- Most Member States' jurisdictions recognize the right of minors to make informed decisions independent from the will of their parents, among others on purchases, their membership of religious organisations, their civil status and on privacy. Depriving minors of all ages from their right to make decisions on their privacy, even though they can be generally deemed sufficiently mature at the age of 13 and above, raises concerns regarding the respect of fundamental rights. This is especially valid when parents decide to e. g. publicly provide their 17 or 18 years old children's personal data. We thus believe that setting an age of 18 is especially problematic and may interfere with the rights to privacy of young people. Rather than focus on an age, the focus should be on the competencies and abilities of young people. In the online world young people are becoming increasingly aware of the privacy implications and consequences of engagement, and are actively managing their privacy.

- We recommend placing emphasis on awareness and education efforts and self-regulatory approaches to specific services or contexts that may impact on the privacy of young people. Therefore we propose to delete point 18 of Article 3 and change Recital 27 as follows:

> Recital (27): *Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data.* ~~*To determine when an individual is a child, the Regulation should take over the definition made by the UN Convention on the Rights of the Child.*~~

Administrative burdens

- We support the Commission's objective of cutting administrative red tape and minimising burden. However, we are worried that the introduction of new procedures for controllers may

lead to new, costly and time consuming burdens for controllers without leading to a better protection of personal data. For example, in Article 19(3) we consider firstly that such a policy adoption cannot be seen as necessary or proportionate. Secondly, it is in controller's interest to follow the obligations stated in the Regulation, for example Article 27 regarding the security of processing personal data. Therefore, the focus should rather be on ensuring that the measures are being carried out rather than on burdensome administrative procedures.

- We believe that instead of requiring controllers and processors to carry out descriptive impact assessments of the risk of processing certain types of personal data, the Regulation should rather focus on describing what Article 30 is intended to achieve, i.e. the objective of the provision. We note that the way of ensuring the highest level of data protection is to focus on the outcome rather than how this shall be achieved. An administrative task as described in article 30 is not likely to assist in the protection of data subjects.

- Due to the fact that it is often very time consuming to provide data subjects with information of data being processed, we consider that there should be a limitation in the frequency of such access. We propose that Article 13 has the following wording:

> Article 13(1): ***The data subject shall have the right to obtain from the controller once per year without cost, information in accordance with this paragraph.*** *The data subject may at any time obtain confirmation as to whether or not data relating to the data subject are being processed. [...]*

<u>Right to be forgotten</u>

- Regarding the right to be forgotten, Recital 47 and Article 15(2) go as far as demanding the erasure of any publicly available copies even in the online sphere. This is not achievable in a practical sense for data controllers and processors. ETNO and GSMA therefore suggest deletion of the legal text in Article 15(2) and Recital 47.