BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 16:00
To: Verweij, Ellen
Subject: FW: Meeting with Tele2 28 of Februari
Attachments: GSMA Europe_ETNO_GDPRAmendments_Applicable law_clean_05Dec2012.doc; GSMA Europe_ETNO_GDPRAmendments_Gen Obligations and Documentation_clean_05Dec2012.doc; GSMA Europe_ETNO GDPR Amendments_Transfers_clean_05Dec2012.doc; Amendments to GDPR_Consent_ETNO GSMAE_final_5Dec2012.docx; GSMA Europe_ETNO_GDPR Amendments_Sanctions_30Nov2012.doc

From: [redacted] [mailto[redacted]]
Sent: vrijdag 1 maart 2013 15:25
To: Kaai, Geran
Cc: [redacted]
Subject: Meeting with Tele2 28 of Februari

Dear Geran

I would like to thank you on behalf of Tele2 for taking the time to meet us yesterday, and for a very fruitful and engaging discussion on the upcoming Regulation concerning data protection.
Please find attached a few amendment proposals from GSMA/ETNO concerning the Regulation.

We hope that this may be useful for you in your upcoming work.

We look forward to staying in touch regarding this important matter.

Have a great ski vacation and weekend.

Kind regards

[redacted]

[redacted]
[redacted] Regulatory Affairs
Tele2 AB (publ)
Mobile: [redacted]
Direct: [redacted]
Fax: [redacted]

unauthorized interception or other interference without the knowledge of sender or recipient. Tele2 only send and receive e-mails on the basis that Tele2 is not responsible for any such computer viruses, corruption or other interference or any consequences thereof.

GSMA Europe/ ETNO

Proposals for Amendments to the General Data Protection Regulation[1] regards the subject of Applicable Law

05 December 2012

Art. 3 (Territorial scope)

Proposal for a regulation	*Amendment*
1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.	1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:	2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) the offering of goods or services to such data subjects in the Union; or	(a) the offering of goods or services to such data subjects in the Union, ***whether the goods or services are free or paid for***; or
(b) the monitoring of their behaviour.	(b) the monitoring of their behaviour**;** or
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.
	4. This regulation applies to the processing of personal data by a controller not established in the Union but who makes use of equipment and/or software, automated or otherwise, situated on the territory of the said Member State, unless such processing is undertaken only for purposes of transit through the territory of the Union.

Justification

The proposed amendment aims at reintroducing the directive 95/46/EC, Article 4.1.c) criteria of the territorial scope which provided National Data Protection Authorities with a mechanism to enforce EU data protection rules, and which is still required today.

We have also proposed amendments to avoid uncertainty over what 'offering'

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

means. Explicit criteria should be added to the Article pursuant to the ECJ decisions[2] in Pammer and Hotel Alpenhof, cases C-585/08 and C-144/09, and the Article 29 Working Party Opinion on the Reform Proposals[3].

To avoid uncertainty in interpretation and application, the Article must apply to data that are 'collected' and not just 'monitored'.

Art. 51.2 Competence

Proposal for a regulation	*Amendment*
1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.	1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.
2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.	2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.
3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	***3. The competent supervisory authorities may vary according to different lines of business, within a group of undertakings.***
	4. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity

Justification

The context of specific processing activities should be a key factor in determining the lead Data Protection Authority. For example, the main establishment of a company may be Berlin, but the data subjects may reside in the UK, or Ireland, and the processing of their personal data may take place in those member states by group companies incorporated in those states. Where a non-compliance arises, the lead authority should be from one of the member states of the group company processing personal data and not Berlin (data subjects may lack language skills etc to assist their engagement with a German regulator whom they may know little about). *(See also recital 98 and Article 4.13)*

---

[2] Judgment of the Court (Grand Chamber), In Joined Cases C585/08 and C144/09 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008CJ0585:EN:HTML & http://conflictoflaws.net/2010/ecj-on-pammer-and-hotel-alpenhof/

[3] Article 29 Working Party Opinion 8/2010 on Applicable law http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

The proposed extension allows for the inclusion of a group of undertakings with multiple line of business that are managed in different geographical locations. A group of undertakings should have the possibility to define a "main establishment" by line of business.

GSMA Europe/ ETNO

Proposals for Amendments to the General Data Protection Regulation[1] regards the subject of General Obligations and Documentation

05 December 2012

Insert new Recital (61a)

Commission proposal	Proposed amendment
	(61)(a) This Regulation encourages enterprises to develop internal programmes that will identify the processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, and to put in place appropriate privacy safeguards and develop innovative privacy-by-design solutions and privacy enhancing techniques. Enterprises that can publicly demonstrate that they have embedded privacy accountability do not also require the application of the additional oversight mechanisms of prior consultation and prior authorisation.

Justification

This and our other suggested amendments below (Articles 22 *et al.*) set the scene for a risk based approach based on accountability and that incentivises good organisational practices and shifts the burden of the costs of compliance and assurance to the marketplace rather than the public funded enforcement and monitoring.

Art. 22 Responsibility of the controller

Proposal for a regulation	Amendment
1. The controller shall adopt ***policies and implement*** appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	1. The controller shall adopt appropriate measures to ensure and be able to demonstrate that the processing of personal data ***under its responsibility*** is performed in compliance with this Regulation.
2. The measures provided for in	2. The measures provided for in

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

paragraph 1 shall ***in particular*** include:

(a) keeping the documentation pursuant to Article 28;

(b) implementing the data security requirements laid down in Article 30;

(c) performing ***a*** data protection impact assessment pursuant to Article 33;

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(e) designating a data protection officer pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

paragraph 1 shall include:

a) data governance policies that are proportionate to the amount and type of personal data processed by the controller and to the risk of harm to the data protection and privacy of data subjects as identified via impact assessments;

(b) evidence of top-level management commitment to implementing the data governance policies throughout the enterprise so as to ensure compliance with this Regulation;

(c) keeping the documentation pursuant to Article 28;

(d) implementing controls for ensuring compliance with data governance policies and this regulation

(e) implementing the data security requirements laid down in Article 30;

(f) performing data protection impact assessment***s*** pursuant to Article 33;

(g) designating a person to be responsible for ensuring data protection and privacy compliance pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors. ***The presence of such mechanisms shall be considered a mitigating factor in any sanction process related to that controller and specific non-compliance.***

4. Controllers who can demonstrate that internal mechanisms have been implemented and independently verified by a certified assessor shall be entitled to a waiver from the

	supervisory authority for the requirements of Article 22(3), Article 33(2), and Article 34 (1-2).
	5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

Justification

A key objective of reform of the EU data protection legal framework is make data controllers accountable for their processing of personal data, while removing unwarranted and excessive administrative burdens from data controllers *and* supervisory authorities. As proposed Article 22 does not appear to have achieved these laudable objectives and is excessive.

The proposed amendments to Article 22 are intended to demonstrate the importance of accountability and that accountable organizations should be treated differently to those with a willful disregard for the regulations or found purposely neglectful of their obligations.

"Under its responsibility" is added for consistency with other requirements in this draft.

The proposed amendments will permit organisations to adopt information management methodologies most appropriate to the organization and associated risks arising from the processing of personal data.

Art. 28 (Documentation)

Proposal for a regulation	*Amendment*
Documentation	**Documentation**
1. Each controller ***and processor*** and, if any, the controller's representative, shall maintain documentation ***of all*** processing ***operations*** under ***its*** responsibility**.**	1. Each controller and, if any, the controller's representative, shall maintain documentation of ***the policies and measures taken to ensure that the processing of personal data under its responsibility is performed in compliance with this Regulation as laid out in Article 22.***
2. The documentation shall ***contain at least the following information:***	2. The documentation shall **ensure all**
(a) the name and contact details of the controller, or any joint controller	

or processor, and of the representative, if any;

(b) the name and contact details of the data protection officer, if any;

(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

(d) a description of categories of data subjects and of the categories of personal data relating to them;

(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

(f) where applicable, transfers of data to a third country or an international organization, including the identification of that third country or international organization and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

(g) a general indication of the time limits for erasure of the different categories of data;

(h) the description of the mechanisms referred to in Article 22(3).

parties adopt a coherent and systematic framework that meets the requirements of this regulation:

3. The documentation shall contain **all information necessary for a supervisory authority or an internal or external auditor to ascertain that the controller has complied with this Regulation, including a description of any of the applicable internal measures and mechanisms intended to comply with Article 22.**

4. The controller and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority ***or to an independent internal or external auditor pursuant to Article 22(3)***

5. The obligations referred to in paragraphs 1, ***2, 3 and 4*** shall not apply to the following controllers :

(a) a natural person processing personal data without a commercial interest; or

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

Justification

The Regulation is in danger of creating great confusion over the role of data processors and imposing unnecessary and ineffective administrative burdens for business. The current prescriptive documentation requirements for each data processing activity is unachievable for a major multinational enterprise – or even for smaller enterprises – and would not lead to greater privacy protection for individuals. The GDPR should support the role of privacy by design and privacy enhancing technologies, and accountability mechanisms to help create innovative and effective privacy programmes.

For the sake of clarity and consistent user privacy experiences, the regulation should also clarify the role of Data Controllers in setting the internal rules for the processing of personal data for which it is responsible. The Regulation should also free data controllers to choose from a range of methodologies by which they can implement and demonstrate their compliance.

We believe Article 28 conflicts with the principles of accountability and efficiency that are set out in Article 22 of the GDPR, therefore it should be simplified in order

to become effective and proportionate.

GSMA Europe/ ETNO

Proposals for Amendments to the General Data Protection Regulation[1] regards the subject of International Transfers of personal data

05 December 2012

Recital 79 -

Commission proposal	**Proposed amendment**
(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.	(79) This Regulation is without prejudice to international agreements ***and adequacy decisions*** concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects, ***but shall be reviewed within an appropriate time frame to adjust them to the standards, requirements and rules of this Regulation and to ensure a consistent level of data protection.***

Justification

A general statement that the GDPR is without prejudice to international agreements would undermine the aim of the regulation to achieve a harmonised and consistent level of data protection. The same holds true for adequacy decisions. Hence, International agreements and adequacy decisions should remain in force after the adoption of the regulation, but need to be reviewed within an appropriate time frame after the adoption of the regulation, to ensure adoption of relevant rules.

Article 34: Prior authorisation and prior consultation

Commission proposal	**Proposed amendment**
1. The controller **or *the processor as the case may be*** shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation. 2. The controller **or processor acting on the controller's behalf** shall consult the supervisory authority prior to the processing of personal data in order to	1. The controller shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation. 2. The controller shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:
(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks**; or**
(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.
3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.
4. ***The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.***
5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.
6. The controller ***or processor*** shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.
7. Member States shall consult the

particular to mitigate the risks involved for the data subjects where:
(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks.

3. A controller who has complied with the requirements of Article 22, including Section 4, shall receive an exemption from the requirement for prior authorization or prior consultation.

4. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

5. The controller shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.
6. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.

8. The Commission may set out standard forms and procedures for prior authorizations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for

supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects. 8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2. 9. The Commission may set out standard forms and procedures for prior authorizations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

The EU data protection reform seeks to reduce and remove administrative burdens on data controllers while strengthening the role of accountability. However, Article 34 seeks to impose unwarranted burdens regards the need for prior authorisation or consultation with supervisory authorities. This is likely to place a significant burden on already over stretched supervisory authorities, create significant, inevitable delays in the rollout of new products and services, and generally disincentivise the creation of effective corporate privacy programmes. The GDPR should help create effective programmes by which Data Controllers may attest to their compliance and in which, supervisory authorities may have confidence – this will help reduce the administrative burdens on SRAs and data controllers.

The GDPR should also seek to ensure legal certainty for data subjects, data controllers and data processors, by clarifying the relationship and responsibilities between a data controller and data processor.

Article 41 Transfers with an adequacy decision

Proposal for a regulation	*Amendment*
8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.	8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission. ***They shall be reviewed within an appropriate time frame to adjust them to the requirements of the regulation.***

Justification

Existing adequacy decisions should remain in force after the adoption of the regulation, but should be reviewed within an appropriate time frame after the adoption of the regulation in order to ensure a consistent level of data protection.

Art. 42 Transfers by way of appropriate safeguards

Proposal for a regulation	*Amendment*
4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34***(1)*** from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.	4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(***2***) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

Justification

To amend an *incorrect* reference in the proposed text.

Art. 43.1 and 43.2 Transfers by way of Binding Corporate Rules

Proposal for a regulation	*Amendment*
1. A supervisory authority shall ***in accordance with the consistency mechanism set out in Article 58*** approve binding corporate rules, ***provided that*** they:	1. A supervisory authority shall approve binding corporate rules. ***In extraordinary circumstances the authority may make use of the consistency mechanism set out in Article 58. The binding corporate rules shall not be approved unless*** they:
(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;	(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;
(b) expressly confer enforceable rights on data subjects;	(b) expressly confer enforceable rights on data subjects;
(c) fulfil the requirements laid down in paragraph 2.	(c) fulfil the requirements laid down in paragraph 2.
2. The binding corporate rules shall at least specify:	2. The binding corporate rules shall at least specify:
(a) the structure and contact details of the group of undertakings and its members;	(a) the structure and contact details of the group of undertakings and its members;
(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected ***and the identification of the third or countries in question***;	(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected;
(c) their legally binding nature, both internally and externally;	(c) their legally binding nature, both internally and externally;
(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;	(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;
(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;	(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;	(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;
(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;	(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;
(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;	(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;
(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;	(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;	(j) the mechanisms for reporting and recording ***significant*** changes to the policies and reporting these changes to the supervisory authority;
(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.	(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

Justification

Art. 43.1: The main rule should be a simple "one stop shop" procedure, i.e. the relevant national authority should make its own independent decision without involving other external bodies.

Art. 43.2 (b): The BCR are supposed to be applied to all undertakings in the group, no matter in which countries they are localised. Therefore it seems unnecessary and inappropriate to identify the countries in question.

Art. 43.2 (j): Unclear what the term "policies" refers to. Is it e.g. meant to cover the specified "contact details" in 2 (a)? If so, an obligation to go through a burdensome

procedure to report such minor changes should be avoided.

GSMA Europe/ ETNO

Proposals for Amendments to the General Data Protection Regulation[1] regards the subject of 'consent'

5 December 2012

Recital 25

Proposal for a regulation	*Amendment*
Consent should be given ***explicitly*** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in ***this*** context the data subject's ***acceptance of the proposed processing of their personal data***. *Silence or inactivity should ~~therefore~~ not constitute consent.* ***If the data subject's consent is to be given following an electronic request, the*** request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided***.***	Consent should be given by any appropriate method enabling a freely given**,** specific and informed indication of the data subject's wishes***. Consent can be given*** either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct ***such as selecting default settings***, which clearly indicates in ***the specific*** context the data subject's ***agreement***. *Silence or inactivity should not constitute consent.* ***Any request to give consent electronically*** must be clear, concise and not unnecessarily disruptive ***or burdensome to the data subject and*** to the use of the service for which it is provided**,** ***and should facilitate clear choice***.

Justification

Consent should not be the primary means of ensuring the 'lawfulness' of processing. Requirements for consent and limitations on the processing of personal data should be proportionate to the sensitivity of data and any assessed risks to the data protection and privacy of individuals arising from the use of personal data.

An excessive, prominent notice and 'opt-in' regime will overwhelm users with 'being informed' and 'giving consent' and will numb them to the purpose of notice and choice, and will lead to their disengagement from the consent process and ultimately to the potential for greater privacy harms. We believe the Commission's objectives can be better achieved in the GDPR by strengthening the role of privacy by design, self-regulation and accountability. The approach should enable organisations to proactively design for the expression of consent via appropriate mechanisms - including the technical mediation of consent via default settings - according to the context of the service, the sensitivity of the personal data and to the potential privacy harm arising from its use. This should encompass the design and implementation of key components of consent, such as clear and transparent disclosure, comprehension, voluntariness, competence, agreement and minimal distraction.

---

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Recital (31)

Proposal for a regulation	*Amendment*
In order for processing to be lawful, personal data ***should*** be processed on ***the basis of the consent of the person concerned or some other*** legitimate ***basis, laid down by law***, either in this Regulation or in other Union or Member State law as referred to in this Regulation.	In order for processing to be lawful, personal data ***must*** be processed on ***one*** of the ***legitimate*** bases ***laid down by law***, either in this Regulation or in other Union or Member State law as referred to in this Regulation.

Justification

Emphasise that consent should not be considered the general rule regards the processing of personal data but reserved for those contexts where consent is appropriate and in circumstances in which it truly can be given freely

Insert new Recital (33a)

Proposal for a regulation	*Amendment*
	Consent should be relied on as the legitimate basis for processing only when data subjects can meaningfully provide and revoke their consent. In other cases, data controllers should ensure the fair and lawful processing of personal data on other legitimate grounds. Obtaining explicit informed consent can carry high costs for individuals. This regulation also recognises that consent may not be the most desirable means of legitimising the processing of personal data. The use of consent should be reserved for contexts that pose a risk of harm to individuals and/or situations where the processing of personal data would infringe an individual's rights to data protection and privacy. When used in inappropriate contexts, consent loses its value and places an unnecessary burden on the data subject. For example, consent is not an appropriate justification when the processing is necessary for a service the user has requested or when subjects cannot refuse consent without impacting the underlying service requested.

Justification

Reinforces the point that an excessive prominent notice and consent regime may undermine privacy when overused or used out of context, particularly in online services. There is a danger that an over reliance on consent will burden users with inappropriate choice and lead to notice and choice 'fatigue' where individuals 'agree' to a purpose simply to remove a frustration and burden in the user experience. Where consent is necessary it should be specific, informed and *meaningful*, and when used outside that context it loses its value and role in all contexts regards ensuring meaningful transparency, choice and control for data subjects. Our recommendation here is aligned closely with the Article 29 Working Party in its Opinion 15/2011 on the definition of consent (at p. 10).

Field

Art. 4.8 Definitions - Consent

Proposal for a regulation	*Amendment*
'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;	'the data subject's consent' means any freely given specific and informed indication of his or her wishes by which the data subject signifies agreement to personal data relating to them being processed;

Justification

The GDPR should recognise different forms of consent, and that any requirement for explicit consent should be reserved for those categories of data and contexts that pose significant risk to the data protection and privacy of individuals. The GDPR should not seek to prescribe the form of consent, as this will quickly be undermined by changes in technology, services, and consumer attitudes, and may not create effective user privacy experiences. The need for, and the form of consent, should be determined by appropriate impact assessments that consider any specific privacy risks arising from the processing, that takes into account the user context and that create effective user experiences that enhance user comprehension and decision making. For example, the UK implementation of the 'cookie' requirements of the e-Privacy Directive 2002/58EC, has generally resulted in negative user experiences without creating meaningful comprehension and choice on the part of users. It is undermining privacy and is a clear example where imposed 'consent' is numbing people to the importance of making meaningful decisions – users simply agree to cookie consent notices because they are too numerous and burdensome on the user experience and context of engagement. Users 'consent' simply to get rid of an annoying notice, rather than comprehending what is being asked, and understanding the importance of decision-making.

We ask that the definition be less prescriptive. The form of consent should be guided by an impact assessment that determines the precise needs in a particular user experience context and crafts a privacy-protective interface proportionate to the results of the assessment. This approach would have avoided, for example, the results we have seen from the ePrivacy directive's prescriptive consent requirements for cookies, which negatively impact the user experience while providing no large improvements in privacy protections. We have included the impact assessment requirement in the Article 7 recommendation below. Requirements for specific, informed and explicit consent have been retained, but apply only where an impact assessment has not been conducted.

Designing for consent in context and to ensure effective privacy experiences is in line with the objectives of Recital 25.

Art 6 Lawfulness of Processing

Proposal for a Regulation	*Amendment*
(4) Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis in one of the grounds referred to ***in points (a) to (e) of*** paragraph 1. This shall in particular apply to any change of terms and general conditions of contract.	Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis in one of the grounds referred to in paragraph 1. This shall in particular apply to any change of terms and general conditions of contract.

Art 7. Conditions for consent

Proposal for a regulation	*Amendment*
1. ***The Controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.***	***1. Where consent is required, the form of consent captured for the processing of a data subject's personal data shall be proportionate to the type of data processed, the purpose for the processing and any identified risks, as determined through a data protection impact assessment.***
2. ***If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter***	2. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	***3. For the processing of special categories of personal data described in Article 9, consent shall be captured by a freely given, informed and explicit statement or other clear and affirmative action, by which the data subject signifies their agreement.***
	4. Consents captured before the coming into effect of this Regulation shall remain valid after such coming into effect.

Justification

This amendment ties the identification of proportionate consent to impact assessments, privacy by design and accountability in order to ensure effective privacy experiences for data subjects, and in order ensure a balance between individual rights and the legitimate interests of business. Adopting this approach will encourage the use of impact assessments in ensuring good information governance, and promoting the adoption of privacy by design and accountable business practices. It also stresses the contextual nature of consent and that it should be reserved for those categories of data and contexts that pose a real risk

of privacy harm or that may otherwise infringe on the right to privacy and data protection of individuals.

If over used, the value of consent will be eroded. For example, requiring consent for the processing of personal data necessary to provide a service requested by the data subject, serves no purpose for the individual or business. Processing in this context is in the legitimate interests of the data controller and the interests of the data subject. To require consent in these circumstances would frustrate the customer experience, burden the individual with unnecessary decision-making, and erode the purpose and value of consent in the eyes of the individual. It would also add unnecessary costs and burdens to business – resources that could be used to support privacy management.

The amendment refocuses efforts on proportionality and the role of impact assessments,

GSMA Europe/ ETNO

Proposals for Amendments to the General Data Protection Regulation

Sanctions

30 November 2012

Article 79 – paragraph 2

Proposal for a regulation	*Amendment*
2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. ***The amount of the*** administrative fine shall be fixed with due regard to the nature***,*** gravity ***and duration*** of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.	2. The administrative sanction shall be in each individual case effective, proportionate***, justified*** and dissuasive ***as regards future non-compliance. The supervisory authority shall determine the most appropriate sanction in line with the severity of the infringement, including behavioural remedies, and in the case of more serious breaches, the imposition of administrative fines. The supervisory authority will monitor the effective implementation of behavioural remedies. In cases of more serious infringements, where an*** administrative fine ***is justified and proportionate it*** shall be fixed with due regard to the nature ***and*** gravity of the breach, the intentional or negligent character of the infringement, ***the particular categories of personal data and adverse impact on the data subject,*** the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.

Justification

Sanctions must proportionate, fair and applied according to objective criteria and the harm caused by non-compliances to the data protection and privacy of individuals. As proposed by, the GDPR provides for disproportionate, unwarranted and excessive sanctions to be enforced for minor infringements that will not result in harm.

Sanctions should not solely be based on financial fines. Supervisory Authorities should rather aim at behavioural remedies in order to prevent continued non-compliances. For example, a prohibition on processing (as permitted under some Member States' laws today) may be a more effective sanction than a fine.

Article 79 – paragraph 3

Text proposed by the Commission	*Amendment*
3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:	3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:
(a) a natural person is processing personal data without a commercial interest; ***or***	(a) a natural person is processing personal data without a commercial interest; or
(b) an enterprise or an organization employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.	(b) an enterprise or an organization employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities, ***and the non-compliance does not have an adverse affect on data subjects; or***
	(c) an enterprise or organization employing more than 250 people and the processing of personal data does not have an adverse affect on data subjects.

Justification

It is imperative that the regulatory sanctions must concern how a data breach adversely affects data subjects, not the protection of the personal data itself. The individual should be the protected interest, not the data.

Article 79 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:	
(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);	
(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).	

Justification

The non-compliances in this paragraph do not justify the proposed fines.

Article 79 – paragraph 5 (whole paragraph)

Text proposed by the Commission	*Amendment*
5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (...)	***deleted entirely***

...

Voting recommendation

GSMA Europe/ ETNO support the approach taken in the draft report by ITRE Committee.

Article 79 – paragraph 6 – (whole paragraph)

Text proposed by the Commission	*Amendment*
6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (...)	***deleted***

Voting recommendation

GSMA Europe/ ETNO support the approach taken in the draft report by ITRE Committee.