PROPOSED AMENDMENTS TO THE EUROPEAN COMMISSION'S PROPOSED GENERAL DATA PROTECTION REGULATION

December, 2012

I. Recital 34

Article number	Commission proposed text	Proposed text	Justification
Recital 34	(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context **to the extent that it is proven that significant pressure was exercised on the employee so that he had no choice but to provide his consent**. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	*In particular for data processing companies that employ a vast amount of employees throughout the EU, and therefore find themselves subject to significant administrative obligations, it is important to be more precise as to when exactly an employee's consent will not provide a valid legal ground for the processing of personal data in the employment context. If such criteria are not strictly defined, it could open the floodgates for unwarranted claims against such companies. Furthermore, employee consent may help ensure legal certainty in cases where it is not absolutely clear if processing of employee data based on the general legal terms is admissible, or in cases the employee would receive an advantage.*

II. Article 17: Right to be forgotten and to erasure

Article number	Commission proposed text	Proposed text	Justification
17(1)(a)	(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed **and, where the data controller or processor has not foreseen a regular deletion of data which is considered reasonable for the applicable sector and/or in compliance with the relevant data retention rules.**	*It is important to ensure that compliance with Article 17 would not require disproportionate effort. For example, in the payments industry, annual transactions processed by (i.e. credit / debit card processors) are counted in billions and selecting individual data could cause huge effort or can even be technically impossible e.g. when the identification of the data subject is not possible for the payment processor (i.e. when only card numbers, but no cardholder names are processed), or when data is stored in not only one system or if there exist back-up copies etc.. Indeed, with regards to financial data, it is often not feasible to conduct selective deletion upon request and instead more practical to ensure total destruction of data after a certain period of time has lapsed.* *Therefore, we would prefer a more general obligation to delete data instead of a right of each data subject to request his/her data to be deleted.*
17(1)(d)	(d) the processing of the data does not comply with this Regulation for other reasons.	(d) the processing of the data does not comply with this Regulation for ~~other reasons~~ **reasons that constitute a material breach of it.**	*For the reasons mentioned above, it is imperative to ensure that the conditions as to when a data subject shall have the right to erasure are clearly defined so as not to impose disproportionate, or in some cases even impossible, duties on the data processor or controller. The condition of material breach provides a reasonable qualification that would cover all relevant cases while providing more clarity and legal certainty than "other reasons".*
17(2)	(2) Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.	(2) Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps **within its control,** including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.	*In the payment processing industry for example, some payment processors have merchant details and the credit/debit card numbers of cardholders but do not have names, addresses or any contact details of the cardholders so are unable to identify an individual's information for deletion.*

17(3)	(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;	(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; **or for compliance with preservation periods prescribed by statutes or contracts, provided a legitimate aim is pursued and the essence of the right to the protection of personal data is respected.**	*Retention periods are not only provided for in Union or Member state laws but sometimes as well. in statutes or contracts. For example, a controller may have to comply with specific organizations' rules (e.g. German Banking Industry's) providing for specific storage periods and may thus have to ensure that not only the controller itself but also the sub-contractor it uses comply with these requirements.*
17(4)	(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;	(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained **or there is a legitimate interest to maintain them** for purposes of proof;	*In order to avoid an understanding that it requires an objective need, e.g. a lawsuit, to maintain data for purposes of proof, we recommend a legitimate interest to be sufficient.*
17(6)	Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.	Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing, **provided the controller has the data necessary to inform the data subject without unreasonable effort**.	*Credit / debit card processors often are not able to inform cardholders as they only process card numbers, but no names and addresses and further contact details. In addition, to inform data subjects would mean that up to millions of cardholders would have to be informed.*

III. Article 18: Right to data portability

Article number	Commission proposed text	Proposed text	Justification
18(2)	(2) Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.	(2) Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn **except in instances where data security could be compromised or such transmission would cause unreasonable effort for the controller without providing evident benefits for the data subject.**	*Although the "data portability" right may have been targeted at select Internet services, broadly subjecting all data to portability requirements could create unintended consequences that may harm consumers.* *For example, requiring data portability for consumer credit information could expose consumers to a higher risk of fraud and identity theft especially where data is transmitted to an unsecure third party. Equally or even more so, merchant and cardholder data controlled and processed by banks and payment systems that is stored on various systems and data carriers would be exposed to the above mentioned risks.* *Furthermore, the right to data portability could cause unreasonable effort for the controller. Credit/debit card processors often have data of several hundred thousands of (small) merchants and/or cardholders the portability of which implies little, if any, value to the data subjects involved (i.e. records of past transactions for which statements were regularly sent to the data subject).* *Therefore, we believe that the proposed carve out is necessary in order to protect the security of data subjects.*

IV. Article 23: Data protection by design and by default

Article number	Commission proposed text	Proposed text	Justification
23(5)	N/A	(5) **Data controllers shall have three years following the application of the Regulation as set out in paragraph 91(2), to comply with the requirements referred to in paragraphs 1 and 2 of the present Article, and in any case no less than two years from the adoption of delegated acts or technical standards as set out in paragraphs 3 and 4 of this Article.**	*It is imperative that a suitable transition period is established for compliance with Article 23 since the scale of change necessary for some organizations with large and/or older systems to comply with the requirements of the Regulation will require significant time to implement. Indeed, compliance with the relevant data protection by design provisions requires integration well in advance of any project and therefore needs more time.*

V. Article 26: Processor

Article number	Commission proposed text	Proposed text	Justification
26(d)	(d) enlist another processor only with the prior permission of the controller;	(d) enlist another processor only with ~~the prior permission of the controller~~ **prior notification to the data controller. The controller should also be able to audit the process and request termination where it has been established that a specific subcontractor has not processed the data in a lawful and/or secure way.** **Processors with approved BCRs can freely transmit data among their group companies [and/or to third parties].**	*Subcontracting only with the controller's permission can be highly problematic for large data processors with many affiliates that often have shared services functions, restructure frequently and have a huge pool of clients to seek permission from. Such large data processors also have the need for multiple providers and suppliers. Seeking approval among a huge number of data controllers/ clients would be effectively impossible given the administrative effort involved and the fact that a single customer could block whole projects even if they were completely reasonable and there was no specific risk for the personal data (i.e. because all necessary controls would be in place and for reasons that may not be related to data privacy concerns (e.g. in order to negotiate better prices).* *It is more practical to award the data controller audit control rights so that in the case where a data controller were to assume -based on objective reasons- that a subcontractor of the data processor was not handling personal data lawfully or securely, the data controller could request termination.* *We further suggest that some substance is given to the BCRs for processors. Given the high standards to be adhered to and the BCRs' explicit upfront review and approval by the DPAs, group companies of processors with BCRs should be a safe place for the handling of data. Imposing further consent and notification obligations to processors with approved BCRs for their internal data transfers weakens the value of the BCRs mechanism and makes little sense.* *Though less obvious, even the choice of external providers*

			should be more prudent by processors with approved BCRs.
26(g)	(g) hand over all results to the controller after the end of the processing and not process their personal data otherwise;	(g) **to the extent technologically feasible and reasonable**, hand over **or delete** all results to the controller after the end of the processing and not process the personal data otherwise;	*In some instances, it can be extremely challenging to hand over the results to the data controller after the end of processing as this process involves complex de-migration projects and is even not feasible in some cases, e.g. in the credit/debit card payment industry where a huge number of payment transactions may be concerned. Therefore, it is more practical to provide for infeasibility as well as the possibility for the deletion of data as an alternative in appropriate cases.*

VI. Article 31: Notification of a personal data breach to the supervisory authority

Article number	Commission proposed text	Proposed text	Justification
31(1)	(1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.	(1) In the case of a **material** personal data breach, the controller shall without undue delay ~~and, where feasible, not later than 24 hours~~ after having become aware of it, notify the **material** personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within ~~24~~ **72** hours.	*Mandatory 24-hour breach notification to the supervisory authority would dramatically increase the number of cursory breach notifications without allowing time for sufficient assessment and understanding of the nature of the breach, its affect and the most appropriate solution. It is also an unrealistic timeframe for companies significant in size and geographical presence.* *Moreover, without a minimum breach threshold or specified types of personal data that would trigger a notification, data controllers will report every breach (even when immaterial in nature) and will lead to "notification fatigue" for DPAs and data subjects. It is thus important to establish a reasonable risk threshold, such as a material breach, for data breach notification to which the envisaged requirements will apply.*

VII. Article 33: Data protection impact assessment

Article number	Commission proposed text	Proposed text	Justification
33(1)	(1) Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	(1) Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller ~~or the processor acting on the controller's behalf~~ shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	*In the payment processing industry, the processor does not always have a global overview of the complete processing of personal data and, in particular, if the data controller uses multiple processors for parts of the processing. This makes it impossible for the processor to assess the risks involved correctly.*
33(4)	(4) The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	~~The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.~~	*In addition to the potential delay that this Article would cause to the provision of new products to the market, in the payment processing industry in any case, it is often unfeasible to consult with data subjects since payment processors often only have merchant details and the credit card numbers of cardholders but do not have names, addresses or any contact details of the data subjects/cardholders and so are unable to identify individual data subjects.*

VIII. Article 43: Transfers by the way of binding corporate rules

Article number	Commission proposed text	Proposed text	Justification
43(1)	(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 in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules **adopted by a controller or processor**, provided that they:	*It is important to clarify the application of BCRs to data processors, especially since such an extension under the Regulation is the intention of the Commission (see notably Article 43(1)(a) 43(2)(f) as well as 43(3)) although it is not explicitly covered in all cases.*
43(3)	(3) 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 binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.	(3) 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 binding corporate rules **adopted by a controller or processor** within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned	*It is important to clarify the application of BCRs to data processors, especially since such an extension under the Regulation is the intention of the Commission (see notably Article 43(1)(a) 43(2)(f) as well as 43(3)) although it is not explicitly covered in all cases.*

IX. Article 77: Right to compensation and liability

Article number	Commission proposed text	Proposed text	Justification
77(1)	(1) Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.	(1) Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor, **as appropriate in relation to each one's liability,** for the damage suffered.	*It is important to ensure that in practice both the data processor and data controller are not held liable for the same offence. It may not even be in the interests of the data subject to believe, as suggested by the initial proposal that they can pursue without distinction or any basis as to the real liability of each one.*
77(2)	(2) Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.	~~(2) Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.~~	*It is important that data processors are not held liable in circumstances where they were simply acting on the instructions of the data controller. Indeed, joint and several liability is wholly disproportionate and in fact weakens collective liability. There is also the question as to whether this provision violates any of the individual Member State's civil liability regimes which cannot be harmonized by an internal market measure.*

77(3)	(3) The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.	(3) The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage**, notably in cases of fault of the data subject or *force majeure*.**	*We believe that the text in Article 55 of Directive 95/46/EC is more precise and suitable in this context.*

X. Article 79: Administrative sanctions

Article number	Commission proposed text	Proposed text	Justification
79(2)	(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 organisational 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 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 organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach. In addition, data controllers or processors who have established a BCR regime shall have this attribute taken into account as a mitigating factor in the calculation of any fine imposed.	*Firms having implemented an effective compliance program such as a BCR regime should have this attribute taken into account as a mitigating factor in the calculation of any fine imposed.* *This will also provide incentives for firms to implement BCRs throughout their business thereby further promoting a high level of data protection at EU level.*

79(4)	(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:	(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 **in the relevant geographic area to which the infringement directly or indirectly relates** to anyone who, intentionally ~~or negligently~~:	*Given that the Commission has decided to draw its inspiration from the current EU cartel regime it should, at the very least, exercise consistency in the application of the various elements found under that regime. Indeed, the Commission cannot simply "cherry pick" the provisions it desires and apply them to a very specific sector such as data protection without also providing for the appropriate checks and balances set out in EU cartel legislation.* *Indeed, under current EU cartel law, the application of worldwide turnover is balanced by the leniency program. Thus, with no leniency regime currently envisaged under this draft Regulation, the application of worldwide turnover would result in a completely disproportionate penalty* *A more appropriate method for calculating the relevant fines is to be found in the Commission's* **Guidelines on the method of setting fines** *imposed pursuant to Article 23(2)(a) of Regulation No 1/2003. Here, the Commission generally starts its calculation by taking the value of the concerned undertaking's "sales of goods or services to which the infringement directly or indirectly relates in the relevant geographic area". This ensures that the final penalty imposed is proportionate and appropriate for the violation. In this way, a 'blanket' penalty, lacking in any sort of gradation, is avoided.* *Moreover, the very sweeping criteria of worldwide turnover that the Commission has chosen to use to calculate the fine amount could result in unintentionally onerous consequences for businesses with global operations and may very well discourage new players to enter the EU market.*

79(5)	(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:	(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 **in the relevant geographic area to which the infringement directly or indirectly relates** to anyone who, intentionally ~~or negligently~~:	***See above justification to Article 79(4)***
79(6)	(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:	(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 **in the relevant geographic area to which the infringement directly or indirectly relates** to anyone who, intentionally ~~or negligently~~:	***See above justification to Article 79(4)***