BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 16:01
To: Verweij, Ellen
Subject: FW: Request for a meeting on 13, 14 or 17 December 2012
Attachments: [redacted]no photo.doc; Comments on Data Protection Regulation 2-7-1.doc

---

From: BRE-JUS
Sent: maandag 3 december 2012 01:09
To: Grave, Martijn-de; Ruiter, Mieneke-de; Dam, Caroline-ten; Alink, Marnix; Dopheide, Tessa; Kaai, Geran; Timmermans, Marieke; Sorel, Alexander
Subject: FW: Request for a meeting on 13, 14 or 17 December 2012

Van: [redacted]
Verzonden: maandag 3 december 2012 1:08:23 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Aan: BRE-JUS
CC: [redacted]
Onderwerp: Request for a meeting on 13, 14 or 17 December 2012

Dear Mr. Spaan,

I am writing to you on behalf of [redacted] Oracle who will be in Brussels on 13, 14 and 17 December. [redacted] would very much like to meet with you to discuss the draft privacy Regulation and the issues we see with text from the European Commission.

[redacted]is, among others, chairing a number of international privacy fora in the OECD, APAC and the US, and he is working with the US Government on their privacy, cloud and Internet of Things issues. He is also a well-known public speaker on privacy issues here in Europe and he has been the key expert driving the privacy issues in European Commissioner Kroes' Select Cloud Computing Industry Group. I have attached his bio for your information.

[redacted]has developed a list of detailed comments to a number of the Articles in the Draft Regulation which I have attached for your information. In the left column you will find the Articles as listed in the draft Regulation. The middle column lists Oracle's comments and you find the proposed resolution in the right column.

We understand and agree with the need to revise Directive 95/46 to make it more applicable to today's business and technological environment, more effective in the protection of privacy and less administratively burdensome. That being said, we believe that the draft Regulation needs to be reviewed to assure 4 major concepts have been properly taken on board:

1. The draft Regulation is narrowly tailored to achieve compelling public policy goals - this avoids unintended consequences and undue burdens.

2. The provisions of the draft Regulation are part of a risk-based analysis that provides for flexibility to recognize both nuances of circumstance and context to determine what are reasonable applications and implementation of the terms of the Regulation.
3. That while business models need to be compliant with the law, the law should not unnecessarily constrain the flows and uses of data which underpin business models and thus needs to be drafted in a way which provides the needed certainty related to what needs to be implemented with the needed flexibility; and
4. Getting the level of detail in drafting and requirements is thus critical. Accountability and other concepts should be drafted to assure that companies are capable of demonstrating systems of governance and privacy compliance programs. This prevents documentation and filing requirements from becoming needless burdensome and overly proscriptive while assure that company programs have been developed in a thoughtful, complete and effective manner.

[redacted] would be happy to go over the above comments with you and provide additional clarification as needed.

We look forward to hearing back from you and do hope, that despite the short notice, it will be possible to find some time in your undoubtedly very busy agenda to meet.

Best regards,

[redacted]

--

ORACLE

[redacted]

Phone: +32[redacted] | |
www.oracle.com
Oracle
ORACLE Belgium BVBA | Belgium | Medilaan 50 | 1800 Vilvoorde
Ondernemingsnummer BTW BE 0440.966.354 RPR Brussel

--

Oracle Detailed Comments on Data Protection Regulation:

Provision	Issue	Solution
Article 4(5) data controller - alone or jointly with others determined the purposes, conditions and means of processing of personal data	Could be some confusion that determining "means of processing" creates a controller – often part of the role of the processor is help optimize the processing based on the instructions of the controller.	Could add "directly or through services of third party processors" or could add to processor definition that may determine means and conditions on behalf of processor. Alternatively could strike means and conditions
Article 4(8) Consent – freely given specific, informed and explicit by statement or clear affirmative action	Questions arise with employees as to whether consent is "freely" given if there might be negative consequences to withholding consent. Broadening of "explicit" consent requirement.	Solutions should be introduced not in definition but in applicable sections on employee consent and data subject consent. Perhaps introducing a balancing test to see if consent is freely given?
Article4(9) Personal data breach included accidental or unlawful destruction, loss, alteration, unuathroized disclosure of or access to personal data	Broadens concept of what breach may apply to. Definition of breach has no required potential for harm or adverse effect. Also mere inadvertent access, for example: an employee misspells the name of the customer file he is searching and accesses the wrong file should not be considered a breach. Also, hard to see how an accidental loss of information should be a breach...	Would delete "loss or destruction" those should be part of the integrity of information requirements under security obligation. At a minimum, accidental should not cover loss or destruction. Finally, definition of breach should exclude inadvertent access within organization.
Article 4(13) Main Establishment – where main decisions as to purposes conditions and means of processing are determined, or if that not in EU, where main processing	May be multiple places that fit those descriptions for a multinational headquartered outside of EU. Most multinationals are data controllers in more	Provide a role for the company to suggest where main establishment is based on reasonable justification with provisions against potential for forum shopping

activities in context of activities of establishment of controller take place	than one member state.	
Article 4(18) Child is defined as below 18	This is greater than the generally accepted age of 13	Replace 18 with 13 or even better refer to external document that is more suited to where a child's age should be defined.
Article 7(2) if consent is in a written declaration also concerning other matters the requirement to give consent must be distinguishable in appearance from the other matter	There needs to be a balance between clarity and usability. One cannot have endless consents for topics of similar import.	Clarify the nature of the granularity of consent to avoid needless separation of related consents.
Article 7(4) Consent is not a legal basis for processing where there is significant imbalance between data subject and controller	This may create needless issue with employees and small customers. Consent should not be impossible in all cases of size disparity.	Better drafting would be that imbalance of position may deserve closer review, but should not be eliminated as a legal basis
Article 8(1) processing of information of child below age of 13 requires consent of parent	Confusing in light of definition of child being 18	Redact definition to be 13
Article 14(1) requirements of data collector to "provide" information to data subject	What does provide mean?	Perhaps make available is better phrasing? This should be able to be accomplished through website
Article 14(1)(c) Controller shall disclose the period for which personal data will be stored	This may be problematic as it may be interpreted to require disclosure related to each data element collected	Better drafting: disclose information on how long types of data are retained.
Article(14)(1)(g) where controller transfers information to third country or international organization must disclose the level of protection of that third country or organization by reference to adequacy decision	It is not always possible to specify or know in advance which countries may require access either to provide customer service or as transfers are made related to cloud services (back up etc).	Better phrasing – controllers should disclose whether they may transfer information to third countries. The disclosure should provide notice of types of information which may be disclosed, for which general purposes and to what countries.
Article 14(2) provide information on whether collection of information is voluntary or mandatory and consequences	This seems to be an overly detailed requirement – for example and address for delivery is obviously required. Unclear the	We should perhaps limit this to say that Notice should be provided where consequences for not providing

of not providing information	level of detail such notice would require – every data element collected?	information are unclear, negative and material.
Article 14(3) where information not collected from data subject provide data subject with source of information	As written this would require every processor to contact every data subject	Better phrasing – if a company uses information about a data subject for their own business purposes then they should make information required under the Regulation as well as the source of the information available to the data subject
Article 15(1)(d) – right of access	Same issues as 14(1)(c)	
Article 15(1)(g)/15/2 "communication" of personal data undergoing processing and available information on source	Communication seems like a positive obligation to transmitting information in a specific manner	Strike the word communication – may replace with "make information available"- this also allows for accessing information via a self-service web application
Article 15(4) Implementing Acts	The level of detail in the implementing acts are too granular without clear demonstration of need to specify such detail and are covered by the general delegated acts provision. This comment is applicable across all delegated acts.	Strike clause.
Article 16 Right to Rectification	This right must be limited to the information collected by or originating with the controller. May also apply to records in their control, but those records if updated periodically from third sources will have the problem again. The controller should have no obligation to rectify information originating from third sources.	Limit the obligation to data directly under the control of the controller.
Article 17 (2) Right to be forgotten	This paragraph creates significant and impracticable burdens of erasure on information no longer within the control of the controller. Does this apply to the	Strike this paragraph or redact it to clarify and limit the nature of the obligation to transfers of information that were in the sole discretion and benefit of the

	transfers of information necessary to accomplish the transaction? If the concept of data retention exists and is enforced then this clause is creates undue burdens and duplication.	controller, not those needed to accomplish the transaction or in furtherance of legitimate purpose to serve the customer where reliance may be had on existing principles.
Article 17(3)(d) exceptions to erasure requirements	Limitation of exception for compliance with law to Member State law is unduly constraining and does not reflect the global nature of processing or the fact that EU controllers and processors may have non-EU citizen information in the EU.	Strike limitation to Member State law and replace with duly authorized legal requirements.
Article 17(9) delegated acts in right to be forgotten	Scope of delegated acts undermines any certainty in this section and makes it impossible for companies to cost effectively develop and implement systems that may be subject to change without clear demonstration of need and limitation of scope.	Strike section or limit section to where significant issue has been demonstrated and subject proposed solution to stakeholder consultation to avoid undue burdens and unintended consequences.
Article 18 (1) Right to data portability – copy of data ... in an electronic and structured format commonly used and allows for further use by the data subject -	Agree with attempts to prevent lock-in and the need to provide data in standard format, but must assure that these standards are objective, broadly in use and may be reasonably chosen by the provider of the service. Also assurance that request does not extend to non-structured data.	Clarify the provider's ability to choose the format of structured data as long as it is structured and commonly used. This should actually be an extension of the access requirement, not a data portability requirement.
Article 18(2) "have the right to transmit"	This goes beyond making the data available to the data subject but rather requires the creation of a specific export function. Even data in commonly used and structured formats is not usable across all systems so export function may not work. Further this creates a technical mandate that could impose significant and needless overhead.	Limit obligation to make data available to data subject in commonly used structured form.

Article 18(3) delegated acts	Again potentially overbroad in scope and Commission should not limit choices of providers on commonly used standards.	Import limitations of 18(1) and (2) above into delegated acts.
Article 19(2) objection to direct marketing	Where ad based services are provided; direct marketing is the basis of the provision of the service and cannot be provided without such marketing.	Clarify that not using the service after clear disclosure of marketing based service is a legitimate way to allow the user to object to the processing of the information.
Article 20 profiling	This is a general concern of application. Certain workplace health and safety information or internet based security controls may use automated processing of data and may have impact on the person related to their ability to work or use a service.	Create a public policy exception to assure that safety and security procedures are not unduly impacted by this clause.
Article 21 restrictions	In many cases businesses are required to undertake acts in support of compelling public policy objectives including public health, economic stability, fraud prevention, security and others. The role of business in furthering these compelling public policy objectives is not properly recognized in this section.	Clearly indicate that these actions may, at times, be undertaken by business in furtherance of these specified interests.
Article 23 (1)(2) Privacy by design	Paragraph 1 describes measure and procedures where Paragraph 2 addresses mechanisms. There may be confusion that paragraph two may only be technical where that is not the case – technology can support compliance but does not provide a defacto limitation to only compliance.	Clarification that privacy-by-design is an ecosystem concept.
Article 23(2) privacy by default – not be made accessible to an indefinite number of people	While this may contemplate public settings in social networks, a variety of systems have an indefinite number of people that may need to access data. This a poor drafting	Redraft to reflect that data access should reflect the reasonable needs of the service and not be overbroad or indiscriminate

	substitute for trying to limit overbroad access.	
Article 26 (2)(C) processor responsibility of security	Security requirements may change depending on the nature of the data, the processor can only take security requirements based on what they have been told by the controller concerning the data and will also follow the directions of the controller related to security. Processors obligations need to be derivative from Controller obligations and under specification by controller. Independent obligations on processor will create legal uncertainty.	Processors should have appropriate security practices to accomplish the instructions of the controller in a secure manner.
Article 26(2)(f) assist controller	This is an open-ended requirement of assistance that need to be predicated on the role of the processor and to the extent practicable.	Assist the controller as relevant to role as processor as practicable under the circumstances.
Article 26(2)(h) provide information	This is a very open-ended requirement; needs to be limited by reasonableness and should build in protections for proprietary information.	Information reasonably required to control compliance while preserving confidential and proprietary information
Article 26(3) Documenting instructions	As with all documentation requirements in the Draft regulation scope and detail is the issue.	A limiting reference of "reasonable" or "proportionate".
Article 27 – authority of the controller	Processor should have the ability to issue instructions to sub-processors that are needed to carry out controller instructions. The power is thus derivative from the controller, even though it is still processor to processor.	"except to accomplish the instructions of the controller provided directly or, where sub and co processors are involved, provided by the processor who engaged the sub- or co-processor
Article 28(1) Documentation	The level and detail of the documentation – "of every processing operation" is ill-	Rather – relevant and appropriate documentation should be maintained by

	defined, poorly scoped and may create needless administrative costs and burdens	the controller regarding its systems, processes and controls. Controllers should assure that processors and other parties acting under their authority maintain appropriate documentation to assure the controller that their instructions related to the processing of personal information are being carried out in a secure and compliant manner.
Article 28 (2) elements of documentation	Potential burdens specific to (c),(e),(f) and (g) – again based on documentation per processing operations as to types of processing operations and types of data.	Use of broader categories and where possible systems level requirements are more reasonable.
Article 30(2) Security/risk	Following an evaluation of risk – again the issue is one of scope. All parties engage in risk analysis but based on systems and types of data. As drafted it may imply that this is done with each new processing contract or operation.	Remove "following" replace with– shall appropriately evaluate risks, take...
Article 30(3)(4) Delegated Acts/State of the Art	The ability of the Commission in delegated acts to determine the state of the art. The state of the art is fluid and changes fast in technology. Once written it becomes obsolete. In Para 4 specifying requirements, depending on the level of the drafting may constrain innovation and needless increase cost of tailoring of solutions to sectors, infrastructure and specific context if drafted too narrowly.	That the commission may wish to provide "guidance" related to new technologies may well be appropriate, but not "define" the state of the art or "specify requirements". Furthermore the level of drafting must retain a flexibility of implementation and not attempt to micromanage security.
Article 31(1) Security Breach	24 hour notification remains the baseline expectation, though now with a possibility to explain why it took longer. This is neither practicable nor realistic. One may become	Track the language of the –e privacy directive on delay and adverse impacts add a good faith exception for inadvertent access to information by employee/agent

	aware of a penetration of system. After that an organization has processes t establish the implication of that penetration and whether personal information may have been compromised. In complex systems that takes more than 24 hours. Furthermore since the definition of breach is overbroad the potential number of reports of trivial breaches with little potential of harm/adverse impact could overwhelm DPAs and make them lose focus on the very serious cases they should be pursuing.	of controller with no further use or distribution of information (may best be to fix that in the definition and not define it to be a breach in the first place).
Article 32(2) Communication of data breach	In requiring that notifications be made, especially by publication, care should be taken that notifications do not also provide what may be a mere hardware thief with data on the value of the information on the device.	Provide guidance on what details to avoid in a notification.
Article 32(3) Technical Protection/breach	While technical protection may be an exception to notification, should it be an exception to breach? If properly encrypted is it PII at all? If there is no PII can you have a breach? Also COE has also used a concept of unintelligible to other persons based on reasonable effort/likelihood of compromise.	Create a safe harbor: Information, appropriately secured by technical protection measures that reasonably make any PII contained unintelligible to others should not be subject to reporting or notification.
Article 33(1) DPIA	Separate DPIA obligation on the processor is not appropriate and should, where appropriate, be a derivative obligation required by the controller. The processor does not have an independent knowledge of the data being processed and must rely	Eliminate direct obligation on processor, in favor of derivative obligation from controller to be appropriately required in contract or other due diligence.

	on controller assertions related to what is needed to secure or otherwise appropriately process the data. This may be accomplished by certification schemes of overall processes and systems that are not a typical DPIA. Furthermore only relevant obligations may be evaluated. Where processor has no customer contact, notice, consent and a host of other privacy requirements are not applicable.	
Article 33(2) Specific Risk	Definition of specific risk is overbroad, especially (a) and (b) and is too open-ended (e). Some of the information in (a) and (b) may only be aggregate or non-identified to form population baselines etc. While that information is not identified, it may play a role on impacting the individual if that person's information is somehow impacted by its relation to the baseline. It might be more useful to highlight the risks which the drafters wish to address and require DPIAs where those risks pose a credible threat of occurrence. This is trying to define scenarios, rather than applying g risk. Also as to (e) the potential scope creep and uncertainty created by such an open provision needs to be bounded, perhaps though the consistency mechanism.	Further limit the definition of specific risks to the risk trying to be addressed and not just types of information it might apply to. Better assure that impacts are limited to identified information to avoid needless burdens on aggregated-identified information. Limit nature of additional risk that can be defined by supervisory authority and require consistency across authorities in such additions.
Article 33(4)Data Subject Consultation	Seeking the views of data subjects on intended processing is not a concept that would be of general application and as described is likely to have little useful impact as it will be based on theoretical	It is better to assure that users of any service have the ability to provide feedback and lodge complaints and that those are appropriately reviewed and taken into account in the lifecycle of the service.

	collection rather than actual circumstances.	
Article 33(6)Risk Criteria	This current list of criteria with potential further specification by DPAs is already considered overbroad and potentially open-ended. The unfettered delegate acts provision further diminishes certainty and practicability/	Remove or significantly limit the delegated act and require a consultation and economic impact analysis to further additions to the text.
Article 33(7)Standards/Audit	The Commission is not well placed to develop standards of audit or review. Furthermore such new specification would be duplicative and needlessly burdensome and costly.	We would first propose that absent an investigation, these standards should be based on normal audit protocols used by the company or practices common in the industry. Where such standards are necessary, they should be chosen from existing standards or practice and review already in use related to the sector or technical/audit community.
Article 34 (1)Prior Consultation	The concept of prior consultation/authorization creates a needless burden and inherent delay in the deployment of new business services. It is also unclear when a new consultation or authorization will be required for the expansion of change to the service. Experience on these issues related t fairly simple registration statements created multi-year backups within resource constrained authorities. Such administrative functions draw needed resources from true investigation and compliance activities	The two limitations in the paragraph are not clear and may be read very broadly. Why should this review take place where a recognized model contract is being used? A contract may need to be filed with an Authority that may be able to review it in due course, but the use of a model contract should provide a presumption of compliance subject to confirmation after the fact. Reference to appropriate safeguards is equally unclear as the application of the concept is not well specified. Concepts of when and how adequate safeguards should be applied are too unclear.
Article 34(2)Processor Obligations	Paragraph 2 seems to enable direct consultation between the Processor and the	The obligations on the processor should only be derivate through the controller's

	Authority. While it can be envisioned that the controller can direct such consultation, there should be no such direct obligation on the processor as it merely serves to undermine the controller processor relationship, in which the process relies on directions from the controller as opposed to independent knowledge of the information to make processing decisions.	obligation.
Article 34(4) Prior Consultation Designation	The Supervisory authority is entitled to make lists of processing operations that are subject to prior consultation. This will again diminish certainty and creates the potential risk of considering processing operations without context leading to identification of potential harms in theory that may have almost no possibility of occurring in practice.	Substantial constraint should be required in such specification and Supervisory Authorities should be required to engage in consultation with industry on these proposed operations to assure that undue burdens and unintended consequences are identified and minimized. All such requirements should also be subject to harmonization through the consistency mechanism. Compliance will be complicated if there are multiple requirements across Member States and which are applied differently depending on the nature of the commerce.
Article 34(6) Additional Information/Delay	The PIA is required to be provided as a matter o course and supplemented with additional information as needed. There may well be more information that is required which will only serve to further delay the review process.	The Supervisory Authority should articulate its concern with the type of processing proposed and request information relevant to allaying that concern which might include elements of the PIA or other materials.
Article 34(7)Domestic Regulation	We question the need for domestic regulation to enforce a requirement provided for in an EU Regulation?	Delete
Article 35(10)Method of Contact	Individual right to contact data protection	Better to suggest that there be effective

	officer may be overwhelming in large consumer facing companies.	ways to contract the office of the data protection officer and assure that there is appropriate senior review of such communications and their outcomes.
Article 37(1)(c) Privacy by Design/Default	The responsibility to monitor implementation of privacy by design/default, security and other issues represent shared responsibilities among various development, security and privacy groups.	Better to suggest that DPO work with other appropriate groups and staff in the organization to monitor... This avoids the impression of complete as opposed to shared ownership.
Article 37 (1)(f)DPIA Oversight	To monitor the performance of DPIAs by the controller or processor may be misread to require a DPO of a controller to directly monitor the DPIA of the processor.	Better to remove controller processor in the subsections under the chapeau text and refer to the DPO of the company/organization.
Article 38 (1) Codes of conduct	Codes of conduct are suggested for functions from a-h, yet the practices they cover may well vary by sector and it would be hard to see how compliance with a cone on collection creates a meaningful statement of compliance.	Codes are most useful to address many of these factors within a sector or type of practice, financial, health care etc. What the Commission could provide in these areas is practice guidance and exemplars of ways to comply, but codes should be sectoral and multi-function.
Article 38(4)Code Interoperability	Codes are envisioned within the EU, but they are also international vehicles of compliance and like BCRs possible bridging mechanisms for cross-border transfers.	Concepts of interoperability of codes across jurisdictions as well as cross recognition of codes should be introduced.
Article 39(1)Certification	Certification mechanisms may play an important role, but in terms of technology and processing services can only attest to the tools and potential functionality as well as actual security deployed. Beyond that data protection is the confluence of policies, practices and people supported by technologies which is less suited to an	Certification where appropriate may be used to attest to the security level of the product or service as well as the features and policies/practices that may contribute to complying with regulatory requirements of data protection within the remit and context of the products operation or service provided.

	outcome certification or a quantification of the "amount" of data protection provided by the technology which varies by implementation and coordination with policies, practices and procedures...	
Article 39(2)(3) Multiple Certification Schemes	For certification to play a practicable and sufficiently tailored role in cloud or any other complex implementation t is unlikely that any one certification scheme or set of criteria will provided the needed breadth of coverage or be appropriate across implementation context. As various certifications already exist and new private sector based certifications are being developed, the Commission should not preclude the developing solution or otherwise force detailed criteria or requirements on the marketplace.	The Commission should provide high level guidance on factors which could benefit from certification as well as information on certification that may be available. The Commission should also consider providing more specific guidance on which certification might apply to SMEs as some certification programs may be beyond the technical or financial capacity of SMEs.
Article 41 Equivalence vs. Effective Privacy	There is an established history of practice related to Adequacy pursuant to Directive 95/46. That being said, the Draft Regulation provides an opportunity to further clarity that adequacy is not the same as equivalence, but rather a finding that effective protections exist in the destination jurisdiction which are commensurate with the elements of data protection in the EU. The more granular as opposed to principle-based nature of the Regulation may make adequacy findings unworkable if the concepts of equivalence are applied at too fine a level of detail.	The language should be revised to have a greater focus on finding effective privacy protection in the transfer destination that is commensurate with the main elements and principles of EU data protection regulation as opposed to a term-by-term analysis.
Article 42(3)(5) Clarification of Appropriate	Further information would be useful to	

Safeguards	better understand the extent of applicability of "appropriate" safeguards, especially where no binding instrument is involved. Furthermore, if enhanced use of appropriate safeguards occurs, further attention will need to be paid to requirements of prior notification and approval related to these transfers which could create undue delay and burden to business that rely on transfers of information.	
Article 43 (1)(a) Apply BCRs between Organizations	The current rules only apply to BCRs within a corporate group, but do not extend across groups. Thus a multinational may transfer data across its subsidiaries pursuant to a BCR, but this does extend to transfers between two nonrelated companies that have both had BCRs approved (like transfers between countries that have been found adequate). In today's era o global flows of data and cloud computing these cross company flows are essential.	Expand the current rules to include flows of data between organizations that have approved BCRS.
Article 44(h) Clarification of Legitimate Interest	There is great interest in both the potential and limitation of transfers pursuant to legitimate interest. In some cases processing is centralized for reasons of cost, scale, facilities or expertise. The extent to which legitimate interest may apply is far from clear. Similarly what do the limitation of frequent or massive mean? In a large company a centralization of processing certain HR benefits for instance could involve large data sets that are frequently	Legitimate interest may add needed flexibility to the application of the regulation, and may be very beneficial, but requires clarification.

	updated – does that preclude applying the legitimate interest derogation.	
Article 58(3) Access to Consistency Mechanism	Pursuant to the guidance related to the consistency mechanism, requests for review of consistency may only be made by a supervisory authority or the EDPD. While it is understandable that those entities should be able to request a review, there should be some mechanism for companies or individuals who believe that they are not being fairly or consistently treated to also request some review.	We recognize a concern that resources for these reviews are not abundant, but there should be some process beyond that initiated just by the specified authorities for aggrieved parties to request a consistency review.
Article 62 Implementing Acts	At various points we have commented on the overuse and over-breadth of implementing acts. We appreciate the desire of the drafters to create a living document, but we equally see a need for finality and legal certainty.	Limit both the number and scope of implementing acts. Where implementing acts are deemed necessary they should be limited to needed adjustments in the subject matter of the regulation and not be directed to how a company implements the regulation in its own system. Finally, implementing acts should be subjected to a process of consultation to assure that they neither introduce needless burdens nor result in unintended consequences.
Article 79(2) –(6) Over-breadth of Sanctions/Penalties	The premise of administrative sanction being "proportionate" is completely undercut by the required nature of sanctions (shall not may in paragraphs 4-6) and by removal of potential for a warning letter to organizations with more than 250 employees. The scope and nature of the fines was "meant to get the attention of the CEO". The attention was first drawn to corporate	Fines should not be mandatory and the full range of less draconian sanctions should be available regardless of the size of the enterprise. It's the context of the transgression not the size of the firm that should be determinative of the sanction and some judgment needs to be left to DPAs in applying the rules. The consistency mechanism exists to assure that outliers of soft enforcement don't

	teams looking for new investments and sites for expansion. The charts they create are very broad and do not go into the detail of extraterritorial jurisdictional impact. Thus in a comparative analysis, the new EU sanction scheme that is a global outlier in terms of high end fine will be seen as a factor making the EU less desirable for investment or location of facilities. Is this the right time to make the EU less competitive in attracting investment, jobs, or new facilities? Furthermore the nature of the fine and negligent/intentional nature of the action are not appropriate to the fining structure. The categories make no sense. "does not provide transparent information" is important, but in many ways is an issue of judgment and perception – yet that is in the category of fines up to 1% of world-wide turnover. Processes data without legal basis – again sometimes an issue of interpretation can be susceptible to a fine of up to 2% of world-wide turnover. Finally these are for negligent and intentional violations. In the first years of the implementation of the regulation it will be very hard to distinguish a good faith effort at compliance from negligence in compliance as all parties will be trying to understand what the regulation requires.	exist. There is no question that the fine structure under the Directive did not provide deterrent effect. Reconsider fines with ranges of penalty not tied to global turnover but rather fixed numbers that are more in keeping with the nature of the harm and transgression. The categorization of transgression and fine needs to be reconsidered so that there is some causal relationship between the potential fines and the potential transgressions. The more substantial fines should only apply to intentional misconduct. Where good faith efforts to comply fall short they should be subject to minimum fines or warning letters where continued failure can result in more substantial penalty.
Article 81 Health Data	While the current provisions create some exception for the processing of health data, we believe that improvements in	The Regulation should encourage continued work to responsibly use information for the benefit of patients in

	technology and analytics will be able to generate substantial and beneficial outcomes both for treating patients in hospital and providing lower cost, preventative, in home health care. In order to accomplish these compelling public policy objectives, more data may well need to be made available for use in both research and treatment.	research, treatment and preventative care both in hospital and at home. Processes short of delegated acts should be in place to allow supervisory authorities to review and accept "use cases" for information with established practices and controls that may be used where obtaining individual consent is impracticable.
Article 83 Research	This exemption has been established over time but may need broader application today. Cities are using applications where they are using location data from cell phones to manage traffic, add bike lanes and assure pedestrian flows among other logistic improvements in our new "smart cities".	The concept of these less traditional forms of research and uses of information for the public good should be included in the scope of this paragraph.