European-American Business Council

EABC EU Data Protection Regulation
Analysis & Prescriptions for Reform
22 June 2012

ARTICLE 4(2): DEFINITION OF PERSONAL DATA

Impact & Problems

The definition of "personal data" in Article 4 is extremely broad and resulting differences in interpretations of "personal data" will lead to greater legal uncertainty.

EABC Proposed Solutions

In Article 4(2) amend to "'personal data' means any information that can identify a data subject", and confirm in this binding Article that anonymised data is not considered personal data, as stated in Recital 23.

ARTICLE 4(13) & RECITAL 27: MAIN ESTABLISHMENT

Impact & Problems

The process for determining "main establishment" is unclear. Recital 27 states both "effective and real exercise of management" and "central administration" may serve as the basis for a decision; however, these two functions could very well be located under different jurisdictions.

EABC Proposed Solutions

Create a transparent and predictable process for determining "main establishment," taking into account input from data controllers while safeguarding against possibilities for forum shopping. This process should explicitly eliminate the possibility of requiring multiple establishments in the EU for any one enterprise.

ARTICLE 5: DATA MINIMIZATION

Impact & Problems

Organizations require some flexibility in determining what personal data may be needed for a particular purpose and that determination will vary from organization to organization and industry to industry. Requiring the "minimum necessary" personal data be collected in relation to the purposes for which they are processed could be interpreted to exclude important, if not critical, data. For example, credit reporting agencies could be required to restrict the amount of data available to a lender when making judgements on a loan. This could reduce consumer access to affordable credit.

EABC Proposed Solutions

In Article 5(c) replace ". . . limited to the minimum necessary . . ." either with "not excessive" or "proportionate".

In Article 5(d) add ", where necessary," after "kept up to date".

ARTICLE 7 & RECITAL 34: CONSENT

Impact & Problems

Organizations need to be able to rely on consent confirmations made by other organizations ("piggy back" on consent). Downstream organizations may have no direct opportunity to obtain consent from the data subject and therefore have to rely on a confirmation by the original organization which cannot necessarily provide evidence of each and every consent to the downstream organization.

Because credit reporting is not only based upon consent, but also on a legitimate interest of the entity engaged in transaction, the consent requirements under Article 7 could significantly hamper consumer authentication tools used for the prevention of fraud, identity theft and money laundering.

EABC Proposed Solutions

Restrict the requirement for the controller to bear the burden of proof of consent to the original controller to whom consent was given.

ARTICLE 7 & RECITAL 34: LEGAL BASIS OF CONSENT IN THE EMPLOYMENT CONTEXT

Impact & Problems

The relationship between employer and employee should not be generally regarded as a situation of "significant imbalance" in an absolute manner as consent may provide more transparency to the employee/data subject as well as legal certainty in some cases.

EABC Proposed Solutions

Limit the exclusion of consent for employees to cases where it is apparent that a relationship of significant imbalance exists, was abused and no opt-out was provided to the employee without jeopardizing the employment relationship.

ARTICLE 12, 14-16: ACCESS AND RECTIFICATION

Impact & Problems

Allowing consumers to have unfettered access to their personal data at no cost, coupled with the ability to edit their data, does not recognize that there are costs to providing these

services, especially where a "deletion" service is not feasible. Data protection does not necessitate unfettered access to one's personal data, which, by its nature, can lead to greater security challenges and vulnerabilities.

EABC Proposed Solutions

Recognize that there is a need to charge a reasonable fee for services relating to the access and correction of data. Require sufficient proof of identity from the consumer to protect against unauthorized access of their data.

Recognize that not all data records can be efficiently accessed and updated, as the current text of the draft Regulation may require. For example, the cost of accessing and updating data on back-up tapes and disaster recovery systems can be significant.

ARTICLE 17: RIGHT TO BE FORGOTTEN

Scope

Impact & Problems

Controllers' responsibilities to erase public data cannot reasonably extend beyond their control.

EABC Proposed Solutions

In Article 17(2) add "within its control." after "Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps".

Applicability

Impact & Problems

The principle of "right to be forgotten" must be careful to exclude accurate, but perhaps negative, personal data. For example, allowing consumers to delete information from their credit file would increase the cost of credit or reduce the availability of credit, since lenders could not reliably assess credit risk.

In some cases erasing data may not be technically feasible. In the payments industry, annual transactions processed by credit card processors are counted in billions. Data is massive and stored in various systems, backup copies are created etc. selecting and deleting is technically impossible. Additionally, those processors have merchant details and the credit card numbers (which is personal data) but do not have names, addresses or any contact details of the data subjects so they would be unable to inform them. Finally, assuming a cardholder could somehow request deletion of the data, the processor would breach contractual obligations.

EABC Proposed Solutions

Further consideration of the implications Article 17 may have on individual industries and data types should be given (e.g. credit reporting agencies). Where needed, alternative industry specific solutions should be provided (e.g. total destruction rather than selective erasure upon request of a data subject after a certain period of time has lapsed).

ARTICLE 18: DATA PORTABILITY

Impact & Problems

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 would harm consumers and negatively impact innovation. Attempts by the European Commission to develop and specify "technical standards, modalities and procedures" in this complex and changing environment could undermine current industry driven initiatives and create a net loss for both privacy protection and innovation.

For example, requiring data portability for consumer credit information would expose consumers to a higher risk of fraud and identity theft and if the data was transmitted to an unsecure third party. The same is also true for merchant and cardholder data controlled and processed by banks and payment systems that are stored on various systems and data carriers.

EABC Proposed Solutions

Encourage industry-driven, market-based initiatives for developing open and global data portability standards as opposed to mandated specifications from the European Commission that might cause greater harm for consumers, as the prior examples from the credit reporting and financial and payments sectors demonstrate.

ARTICLE 20: RESTRICTIONS ON AUTOMATED PROCESSING

Impact & Problems

The restriction on profiling and automated processing in the draft Regulation is a drastic change from the current policy that allows for the processing of personal data for legitimate interests without requiring consent.

EABC Proposed Solutions

The consent requirement in the draft Regulation could place restrictions on important consumer authentication tools used to detect fraud and money laundering. Further, it could also lead to an increase in indebtedness by removing important tools that a lender uses to gauge a consumer's ability to pay their loan.

ARTICLE 23: DATA PROTECTION BY DESIGN AND DEFAULT

Impact & Problems

The meaning of "default" is unclear and could be interpreted to require the most restrictive privacy settings. Such an interpretation discounts users' expectations and would reduce the adoption and use of innovative products and services. For example, the application of "privacy by default" would likely have prevented the use of anonymous Wi-Fi access point data to assist in the growing market of location-based services.

More fundamentally, privacy by design and by default are means to greater privacy protection, not privacy protecting measures by themselves. By their nature these concepts are better suited for guidelines than legislation.

EABC Proposed Solutions

Allow privacy by default principles to be developed by users and providers in the form of guidelines and best practices.

ARTICLES 26-29: PROCESSING

Impact & Problems

Subcontracting only with the controller's permission can be highly problematic for large data processors with many affiliates especially as, so far, they cannot benefit from the BCRs. Such companies have shared services functions, restructure frequently and have a huge pool of clients to seek permission from. Submitting them to constant data controller authorisation would make their business impossible.

Such large processors also have the need for multiple providers and suppliers. Seeking approval among many controllers-clients would be impossible given the administrative effort involved and the fact that a single customer could block whole projects even if they were absolutely reasonable and there was no specific risk for the personal data (i.e. because all necessary controls would be in place). On the contrary, controllers-customers, in our experience, occasionally object due to other reasons (i.e. in order to negotiate better prices) but invoking privacy concerns. Their right to object to subcontracting is now less important as in the new regime the processor is also responsible for privacy breaches.

EABC Proposed Solutions

This problem could be partially solved by extending the BCRs regime to Data Processors, that is, regarding subcontracting to affiliates within the same group. However, it would not resolve this problem for external providers.

Another solution would be to foresee differentiations (i.e. between subcontracting within the EU/EEA or between various categories of personal data).

In our view, giving the controller information and audit control rights would be sufficient. In case a controller were to assume based on objective reasons that a subcontractor of the

processor does not handle personal data lawfully, the controller may have the right to object to the use of the specific subcontractor.

ARTICLE 31-32: BREACH NOTIFICATION

Impact & Problems

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. The timeframe is especially unrealistic for companies of a significant size and geographical presence.

Without a minimum breach threshold or specified types of personal data that would trigger a notification, controllers will report every breach, even when immaterial in nature – and will lead to "notification fatigue" for DPAs and data subjects.

There must be a difference between the obligation and threshold to report to DPAs on the one hand and notification to affected individuals on the other.

EABC Proposed Solutions

In Article 31(1): remove ". . . and, where feasible, not later than 24 hours after having become aware of it," to better align the draft Regulation text with the breach notification requirements in Article 4(c) of the e-Privacy Directive.

Establish a risk threshold for data breach notification, below which the draft Regulation breach notification requirements do not apply, i.e. limit reporting to DPAs to "material" breaches and notification to individuals of breaches where there is a real risk of significant harm. Or, specify types of personal data that would trigger a notification as, for example, is the approach in German law.

ARTICLE 33: DATA PROTECTION IMPACT ASSESSMENTS

Impact & Problems

The draft regulation's language on when a PIA is required is both vague and broad, e.g. ". . . are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes." As a result, the administrative burden on controllers and processors could be greater than that of Directive 95/46.

Consultation of data subjects could delay the provision of new products to the market without necessarily guaranteeing greater privacy protection. In other cases, consultation may be unrealistic (e.g. by card processors, for the reasons listed in Article 17 above). Organizations are best placed to make such assessments as they know best their own business and operations and can follow industry practices as appropriate.

By means of an example, in the payments industry, a bank and its processors agree that the overall compliance responsible (AML, privacy, KYC) is the bank that has the contractual relationship with the credit card holders. The processor does not even know who the data subjects are but processes personal data as they have the credit card numbers. The processor does not necessarily have a global overview of the complete processing of personal data and in particular, if the controller uses multiple processors for parts of the processing. This makes it impossible for the processor to assess the risks correctly.

EABC Proposed Solutions

Allow Privacy Impact Assessments to be developed by users and companies in the form of best practices and guidelines. However, should PIA specifications remain in the draft regulation, we recommend the following edits:

- Clarify the conditions under which PIAs are required.
- Delete the obligation to consult data subjects or their representatives by removing Article 33(4).
- Strengthen the role of the Data Protection Officer as an independent control instance that assesses the data protection impacts without any consultation requirements.
- Include an exemption for key-coded data from PIAs, as such data does not present specific risks.
- Exclude data processors (or at least certain categories of data processors) from the PIAs.

ARTICLE 34: PRIOR AUTHORIZATION AND CONSULTATION

Impact & Problems

The requirement for prior approval could be very broadly applied and the costs of consultations, documentation, and prior approval could be overly burdensome. Furthermore, certain DPAs react in a less timely manner to authorization requests, creating a need for a maximum allowable timeframe for approval decisions.

EABC Proposed Solutions

Develop clearer and more narrowly defined requirements for prior authorization.

Include a maximum allowable time for approval decisions before permission is automatically granted.

Delete prior authorization and consultation requirements as long as a Data Protection Officer is in place.

ARTICLE 41: DETERMINATION OF ADEQUACY DECISIONS

Impact & Problems

The process and timeline by which adequacy decisions are determined are opaque and undefined.

EABC Proposed Solutions

Increase transparency for both existing and future adequacy determinations.

ARTICLE 43: SCOPE OF BINDING CORPORATE RULES (BCRs)

Impact & Problems

In view of the increased responsibility of data processors in the draft regulation, processors should be included in the scope of BCRs and allowed to participate in a significant tool already available to controllers.

While the notion of group of undertakings has been adopted by the draft Regulation and the international transfer of data within a group of undertakings is covered by BCRs, the simplification of the transfer of data within a group of undertakings within Europe has not been covered by the proposal.

EABC Proposed Solutions

Expand the scope of BCRs beyond one group of undertakings to include processors and organizations that are involved in shared information value chains.

Clearly define the benefits of BCRs.

Simplify transfer of data within a group of undertakings within Europe by allowing BCRs as a legal basis for such a transfer.

ARTICLE 47(5): UNFUNDED MANDATES FOR DPAs

Impact & Problems

The absence of predictable funding for member state DPAs could result in irregular implementations, slow administrative processes that lead to delays in determinations, and an institutional predilection towards fines.

EABC Proposed Solutions

Specify the meaning of "adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers" and include clear requirements for member states to provide this.

ARTICLE 73: RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY

Impact & Problems

Article 73(¶2-3) may have the consequence that Works Councils gain the right to lodge complaints on behalf of data subjects. Works Councils are very challenging to deal with in countries like Germany and Austria, and may event abuse this right, e.g. in job reductions.

EABC Proposed Solutions

Explicitly exclude Works Councils from the scope of Article 73.

ARTICLE 79: ADMINISTRATIVE SANCTIONS

Impact & Problems

Negligence caused by unclear and ambiguous guidance is punishable to the same degree as intentional violations.

A fine of up to 2% of global turnover is significantly disproportionate to damages caused by non-compliance with data protection regulations.

There are serious questions as to the appropriateness and enforceability of targeting revenues beyond the EU.

Consideration should be given to the addition of factors to consider in determining the level of a fine, e.g. existence of procedures, nature and scope of non-compliance, history, etc.

EABC Proposed Solutions

Expand the scope of Article 79(3) (warning for first and non-intentional violation) to controllers.

Remove "negligence" from Article 79(4)-(6) and create a separate subsection for negligent failure to comply.

Replace "shall impose a fine" with "may impose a fine" in Article 79(4)-(6).

Implement fines based on a percentage of turnover with a fixed maximum, e.g. ". . . up to 2% of EU turnover, but not to exceed €_____."

PROCESSOR AND CONTROLLER RESPONSIBILITIES

Impact & Problems

The current Directive 95/46/EC has established clear and adequate roles for data processors and controllers, and thereby provides data subjects with legal certainty about who is responsible for their data. The draft Regulation, inversely, alters responsibilities of processors and controllers and thereby negatively affects legal and commercial certainty. The responsibility of the processor is to process data in accordance with instructions from the controller, as defined by prior contractual obligations between the processors and

controllers. The draft Regulation would require impractical obligations on processors and impede upon, or potentially violate, member states' "freedom of contract" laws.

EABC Proposed Solutions

Preserve from Directive 95/46/EC the clear distinction between processors and controllers.

DELEGATED & IMPLEMENTING ACTS

Impact & Problems

26 of the Articles in the draft Regulation contain the use of delegated and implementing acts. Delegated and implementing acts create uncertainties for processors and controllers and could hinder job creation and economic growth.

EABC Proposed Solutions

Remove delegated and implementing acts that go beyond the criteria agreed upon in the Common Understanding adopted at COREPER I.

Allow for industry involvement and consultation in the development of delegated and implementing acts.

Create a fixed period for delegated acts of no longer than 6 months, to improve legal certainty for enterprises.

PRESERVE THE US SAFE HARBOUR AGREEMENT

Impact & Problems

There is concern that the adoption of the current Regulation could result in the EU finding the Safe Harbour Agreement inadequate and, in doing so, jeopardize a significant section of the global digital economy.

EABC Proposed Solutions

Clarify the continued applicability and utility of the Safe Harbour Agreement, and establish a reasonable timeframe for a review of existing international agreements after the adoption of the regulation, in order to adapt them to the new laws.

RELATIONSHIP WITH THE E-PRIVACY DIRECTIVE

Impact & Problems

The relationship between the draft Regulation and the e-Privacy Directive needs to be clarified.

EABC Proposed Solutions

Articles within the e-Privacy Directive covering the same issues as addressed within the draft Regulation should be revoked.

For more information please contact:
Alex Propes, Policy Manager, Washington: 202-828-9107 or alex.propes@eabc.org
Justine Korwek, Brussels Director, Brussels: +32 2 791 7516 or justine@eabc.org