MEMO

PrivaSense
Privacy and Trust in the Digital Society

Systematic mistakes in the proposal for a General Data Protection Regulation

[redacted]

February 5, 2013

Introduction

The General Data Protection Regulation, as proposed by the Commission on January 25, 2012 (COM 2012, 11) contains a number of mistakes, which contradict the system of Regulation itself. If not corrected, such mistakes will eventually lead to implementation difficulties for controllers and processors or to unintended consequences for data subjects. This memo outlines such mistakes and provides advice as how they should be corrected.

Art. 3 – Establishment of the controller or processor

The Regulation repeats same mistake as Directive 95/46/EC, which leads to unintended and unwanted consequences as to the application of the Regulation. Just like the Directive, the Regulation frequently uses the term 'establishment of the controller/processor'. However, the term 'establishment', especially in art. 3, suggests that the Regulation only applies to organizations (companies, governmental bodies, associations, etc). However, as the household exemption of art. 2(2)(d) already suggests, the Regulation also applies to *individuals*. People are not 'established in the Union', but have their *'habitual residence'*. Art. 3 fails to mention this.

Suggestion: Replace "controller/processor" by an establishment of a "public body or enterprise or any other body, as well as any natural person residing in the Union acting as controller or processor".

Article 17(1)(c): Erasure after objection

This article allows the data subject to have the data erased if an objection to the processing of personal data pursuant to article 19 has been upheld.

This article misinterprets the scope of the definition of processing. Even if corrected, the article is superfluous.

'Processing' is defined as "*any* operation or set of operations" (see art. 4(3)). This means that a data subject may not only object to the entire processing operation, but also to a particular type of processing. Art. 19(1) allows a data subject to object to a particular disclosure to a

PrivaSense BV
Harrie Janssenstraat 22
5063 CG Oisterwijk, NL
www.privasense.eu

third party or a particular type of secondary use (e.g., opt-out from marketing, see art. 19(2)). The right of erasure does not make sense after the a successful objection to such disclosure or use, as in most cases there will still be a legitimate interest to continue the processing of the personal data, more in particular for the purposes for which the data were collected.

Article 17(1)(c) would only make sense if the objection is aimed at the collection or retention of personal data, as it would be aimed at the purposes for which the data are collected. In such case, the objection would block/take away the grounds for data processing as stated in art. 6(1). This means that even if the term 'processing' in art. 17(1)(c) would be interpreted as 'collection' or 'retention', it would be superfluous in light of art. 17(1)(a).

Suggestion: Delete art. 17(1)(c), as it is superfluous.

Article 17(4)(b) – Retention of data for purposes of proof

This article allows the controller not to erase the data if the data need to be maintained for purposes of proof. However, the retention of data for purposes of proof is already covered by art. 17(1)(a), as 'proof' is a 'purpose for which the data are otherwise processed'. The restriction of the processing as envisaged by art. 17(4) is already covered by art. 5 and 6(1). Therefore, art. 17(4)(b) is superfluous.

Suggestion: Delete art. 17(4)(b).
(Note: all parts of art. 17(4) are problematic, as art. 17(4)(a) confuses the right of correction with the obligation to erase the data. If at all, this article should be part of art. 16; art. 17(4)(c) is a case without an obvious use case scenario; and art. 17(4)(d) should be deleted in view of the fact that art. 18(2) is wrong, see below).

Article 18(2) – Data Portability

This article contradicts the definition of 'controller' (art. 4(5)).
A 'right' of the data subject implies an 'obligation' of the controller. In the case of art. 18(2), this controller is not the controller *from* which the data are ported (as this is covered by art. 18(1)), but the controller *to* which the data are ported. In other words, art. 18(2) *implies an obligation to collect* the data on the side of the controller to which the data are ported. This contradicts the principle, as laid down in the definition of controller in art. 4(5), that it is the *controller* who decides which data are collected and for what purpose, not the data subject.

The right to data portability as an obligation to collect, as mentioned in art. 18(2), only makes sense in a small number of cases where it is logical that the data subject has a say in

PrivaSense BV
Harrie Janssenstraat 22
5063 CG Oisterwijk, NL
www.privasense.eu

which data are collected by the controller, such as in case of 'user-generated content' (e.g., social networks) and medical data in case of a change of doctors. But in the vast majority of cases, such as in case of employee data or customer data, the controller would have no use for the data which were originally collected by another controller, so the right of data portability, as laid down in art. 18(2), should not exist in such cases. If the purpose of such controller would coincide with that of the original controller, such data could simply be collected from the data subject, which means that there is no need for such right.

Suggestion: Delete art. 18(2) or restrict its scope to user-generated content and medical data.

Article 19(1) – Right to objection
This article has several mistakes.

First of all, it has been drafted in such a way ("shall have ...., unless") that technically the right to objection can only be exercised if the controller does not demonstrate compelling interests. This would make the exercise of the right to objection dependent of the interests of the controller, which is a mistake. A data subject should always have the right to object to the processing, but the controller may deny the request if his interests override the interests of the data subject.

Secondly, the use of the word 'compelling' is wrong. Art. 19(1) is a logical complement of art. 6(1)(d), (e) and (f) and has a particular function in data protection. Art. 6(1) requires the controller to balance his own interests (or, in case of a disclosure, those of a third party) against the *assumed* interests of the data subjects. Most cases, the interests of the data subjects are *collectively* taken into account, as it is impossible for the controller to take into account the specific interests of each data subject concerned at the time of the balancing of the interests. Art. 19(1) gives the data subject the right to request an *individualized* balancing of interests ("their particular situation"). In such case, the data subject will provide the controller with information relating to his particular interests, which the controller did not have/know at the time the collective interests of the data subjects were taken into account pursuant to art. 6(1).

However, the objection by the data subject should not lead to a change in the position of the data controller (as suggested by the use of the term 'compelling' in art. 19). The interests of the controller, which he takes into account under art. 6(1) and art. 19(1), should be exactly the same in both cases. And in both cases, the controller's interests have to override the data subject's interests in order for the controller to deny the objection. There is therefore

no need to require 'compelling' interests on the side of the controller in art. 19(1), as this would mutatis mutandis mean that also the interests under art. 6(1) should also be compelling (quod non).

Suggestion: Redraft art. 19(1) and delete 'compelling'.

Article 30(1) and 30(2) – Security and processor

The obligation of the processor to implement technical and organizational security measures contradicts art. 26(2)(c), which requires the controller to stipulate the security measures in the processor contract. In view of art. 26(2)(c), art. 30(1) and 30(2) are superfluous with regard to the processor's obligations.

Moreover, if art. 30(1) and 30(2) would apply independently to processors, in practice 2, possibly conflicting, security policies would apply to the processing (one of the controller and one of the processor), none of which – from the perspective of the Regulation – would be dominant over the other, as both the controller and the processor can be fined for not taking the appropriate security measures pursuant to art. 79. Therefore, from an accountability point of view, the security policy of the controller should supersede the security policy of the processor.

If at all, the processor should only be required to implement security measures if the controller does not comply with art. 26(1).

Suggestion: Delete 'processor' from art. 30(1) and 30(2) or amend art. 30(1) and 30(2) to the situation where the controller has failed to close a processor contract pursuant to art. 26(1).

Art. 31 – Breach notification to supervisory authorities.

This article fails to mention *which* supervisory authority should be notified. This is especially important in case of the use of cross-border processing systems, in case the data subjects of multiple Member States are affected and in case the controller is located in another Member State than where the breach has occurred (e.g., where the breach occurs with a processor in another Member State).

Suggestion: Include a designation of the supervisory authority which should be notified to avoid that multiple supervisory authorities must be notified, preferably the supervisory authority of the Member State where the controller is established.

PrivaSense BV
Harrie Janssenstraat 22
5063 CG Oisterwijk, NL
www.privasense.eu