ENPA and EMMA Position paper on

PROPOSAL FOR A DATA PROTECTION REGULATION, 25 JANUARY 2012 (COM(2012) 11)

Introduction

The Commission proposal for a draft Data Protection Regulation of 25 January 2012 impacts various activities of newspaper and magazine publishers' businesses. As well as affecting editorial press freedom, it also impacts press distribution for both the consumer and the business to business press and therefore the economic sustainability of magazines and newspapers across Europe. Furthermore, given the broad scope for delegated acts by the Commission proposal, the framework for data protection in the future remains to a large extent uncertain and unpredictable for European companies.

Given the fundamental importance of the press for any democracy, it is essential that the long term prosperity of a pluralistic, diverse and independent media is safeguarded. It is therefore important that an adequate balance is found between the legitimate interest of individuals with regard to the processing of their personal data and the free movement of such data. It is essential that the revision of the current data protection framework does not lead to an increase in the already substantial regulatory and administrative requirements, which cannot be fulfilled, in particular by European small and medium sizes companies.

ENPA, the European Newspaper Publishers' Association, and EMMA, the European Magazine Media Association would like to highlight the following points in particular in this paper:

KEY CONCERNS FOR MAGAZINE AND NEWSPAPER PUBLISHERS

1. A robust, directly applicable exemption for processing of personal data for journalistic purposes is crucial to preserve editorial press freedom and safeguard a free and independent, quality press (for further details see point 21, below).

2. The possibility for the press to continue to be able to reach out to potential new as well as current subscribers via direct marketing is essential to safeguard press distribution for the consumer as well as the business to business press, in order to preserve readership, future press subscriptions and media pluralism (for further details see points 4, 5, 6, 7, 9, 11, 12, 15, 17 below).

3. The future of the digital press must not be jeopardized: publishers today are innovating and investing in business models to take full advantage of the opportunities provided by new technology to serve their readers on all platforms. The sustainability of newspaper and magazine content on all platforms depends on advertising and digital subscriptions, as well as e-commerce. It is therefore essential that the Regulation does not restrict these possibilities and make it difficult for publishers to be able to interact easily with their readers, and adapt to their needs (for further details see points 1-12, 14, 15 and 17 below).

Concerns of magazine and newspaper publishers in more detail (in chronological order by Article)

1. Definition of personal data (Articles 4(1) and 4(2) and Recital 24)

According to the definitions in these provisions, all data, which can be related directly or indirectly to any particular person, can be considered as personal data. This broad definition covers a wide scope of applications as it simply refers to the general possibility of being able to identify a natural person. This problem is underlined in Recital 24 which points out that identification numbers, location data, online identifiers and other specific factors as such "need not necessarily be considered as personal data in all circumstances", while not completely excluding this possibility.

This wide scope and the associated requirements for the processing of practically all data, leads to an unmanageable burden for companies, which does not seem to be justifiable, even from a consumer protection standpoint.

Furthermore the wide definition of personal data does not take into account the possibility to use pseudonyms of the user data. This is foreseen, for example, in the German Federal Data Protection Act in order to exclude the identification of the data subject or to make it significantly more difficult. This possibility to use pseudonyms for user profiles, in combination with the right to object of the person concerned, should also remain possible.

In order not to extend the scope disproportionately, it is the knowledge or the knowledge capabilities of the data controller that must be the basis for determining whether a person is identifiable. It should also be made clear that the possibility to identify a person indirectly is not sufficient. Article 4 (2) should therefore be amended, so an actual identification is required and not just the abstract possibility of identification.

To increase legal certainty, it would be also appropriate to include within the list of various definitions set out under Article 4 "special categories of personal data". This definition – in line with Article 9 on processing of "special categories of personal data" - should cover information which shows the racial or ethnic origin, political beliefs, religion or belief or membership of a trade union as well as genetic data, data concerning health or sex life and data relating to criminal convictions or related security measures. this group of sensitive data should also be taken into account when determining other obligations of the data controller (see proposed amendment to Article 31).

2. Explicit consent (Article 4(8))

The full consequences of the data subject's consent having to be "explicit" in future remain unclear, but this inevitably poses the risk of further restrictions online and offline:

a) **It remains unclear if implied consent is still possible** (e.g. by inserting a business card into an appropriate box.). In this regard the specific characteristics of the selected communication channel have to be taken into account. Offers such as mobile applications and websites are typically used differently than, for example, postcards and forms. The possibility to grant consent therefore has to be adapted to the respective medium, if necessary in the form of an implied consent. The call for explicit consent is therefore problematic not only for traditional means of communication, but also precludes future technical innovations.

b) **Relationship with E-Privacy Directive**. The requirement for explicit consent also raises the question of whether this has any impact on the ability to express the required consent in certain circumstances through browser settings in the context of the E-Privacy Directive (Recital 66 of Directive 136/2009).

c) **No consent where there is significant imbalance (Article 7(4))**. It is also unclear when there is a "significant imbalance" between the position of the data subject and the controller, in which case under Article 7(4), consent would not provide a legal basis for data processing. In this respect, Recital 34 just states that this is especially the case where the data subject is in a situation of dependence from the controller. This explanation cannot, however, sufficiently explain all possible applications.

d) **Competitive advantage for global business models based on log-in systems**. The requirement of explicit consent generally favours large international companies such as free e-mail providers or social networks, which base their business models on log-in systems. For those companies it is relatively simple to obtain the required consent of their customers, due to the direct contact inherent in the system with their customers.

   The requirement that consent must be explicit poses also the serious risk that consumers will be more likely to give their consent to large global companies, which they are already familiar with and may have already created a comprehensive profile, than to unknown, smaller companies operating at a national level and which are less in the public view.

   Many companies, including many publishers, allow free access to their content without any such restraints. Any direct contact with the customer to obtain consent (such as respective pop-up windows on websites) will therefore carry the **risk of being perceived by the user as a disturbance** and therefore as a negative aspect of the offering. This approach risks resulting in a **huge competitive disadvantage for publishers.**

   At the same time, it is questionable how far the provision of explicit consent contributes to the protection of privacy, insofar as consumers often quickly click 'YES' in order to reach the particular webpage they are looking for, without paying full attention to what they are agreeing to. This puts into question the real value of providing explicit consent.

3. Definition of "child" (Article 4 (18)) and related obligations

The draft Regulation refers to children in several provisions (and therefore to the age limit of 18 years as defined in Article 4(18)), e.g. in the provisions about the right to be forgotten (Article 17, Recital 53), information requirements (Article 11, Recital 46) or profiling (Recital 58).

The general **classification of anyone under 18 years as a child appears inappropriate** given the different stages of development and experience of children, teens and young adults. Also the reference by the Commission to the United Nations Convention on the rights of the child cannot justify this. The Convention contains essential standards for the protection of children, but is not however intended to establish a universal definition of "children". The limit of 18 years chosen is especially questionable given the fact that consent of the parents or guardians in accordance with Article 8(1) is required for the processing of personal data of a child below the age of 13, which is directly offered as a service of the information society.

Recital 38 states that there needs to be "careful assessment" of whether the right to process data, which is lawful if it is in the "legitimate interests" of the data controller data processing, is overridden "where the data subject is a child" (as required under Article 6(1)(f)). In reality, it is questionable as to whether there would actually be the possibility to do so.

If an age verification was required for every contact this would be pose **significant burden for enterprises and numerous business models**. This approach raises the question of how companies can determine in a legally appropriate way, whether the respective services are viewed or requested by a child, especially as regards their digital business models. As it would be very difficult to know for sure if the data subject was in fact a child, companies might feel obliged to not go ahead and process data, which would not be proportionate given the various data processing operations which might be applicable under this article.

4. Principles relating to personal data processing (Article 5).

It is difficult to understand the need for having a list of "principles" in addition to the regulatory requirements in Article 6. These principles, if retained, would constitute an unreasonable burden for businesses taking into account the associated costs and additional efforts they would result in. It is particularly important that the requirements contained in Article 5 (b) should be deleted in this regard.

It is also not appropriate to impose on the controller a general responsibility for compliance with the Regulation.

5. Conditions for lawful processing of data (Article 6)

A **press subscription is a product that must be explained**, but which has no dedicated retail outlet which would allow a publishers' representative, for example, to explain it to a potential customer. In order to safeguard press distribution, direct marketing is therefore crucial.

Article 6 sets out which conditions must be met for the lawful processing of personal data. One of the six alternatives contained in Article 6 has to be met. Consent is one alternative, but not the only one. This is also appropriate because it reflects the fact that there are many different situations where data must be processed.

a) Article 6 (1)(f)

Under Article 6(1)(f), the Regulation continues to allow businesses such as publishers to communicate with potential customers where there is a "legitimate interest" of the data controller, on the condition that strict information requirements are met (Article 14) and consumers have control with the right to object to receiving any further communications (Article 19).

However, the wording does not guarantee that publishers can continue to address potential new readers via direct marketing without prior consent as the possibility to process personal data also for **legitimate interest of third parties** is not included in the text anymore. This is, however, in many cases the necessary condition to conduct direct marketing. Only this possibility ensures that necessary legitimate data processing procedures like the transfer of address lists, the purchase or renting of addresses or the conduct of certain marketing measures by specialized service providers of services can continue to be employed. **This alternative must therefore be reintroduced**. **This is especially important for the thousands of SMEs, which can neither afford big media advertising nor masses of unaddressed direct mail.**

If the **possibility to process personal data for legitimate interest of third parties is not reintroduced as is the case in the current Directive, this poses the serious risk of a dramatic loss of new subscribers and decrease in circulation of many titles across the EU dependent on subscriptions sales and press distribution**. This is even more significant when considering the direct applicability of the Regulation. In many Member States a large percentage of the subscription circulation of certain newspapers and magazines depends on direct marketing by letters sent to third-party addresses without prior consent, which is permitted by national laws based on Article 7 (f) and Article 14 Directive 95/46/EC under the condition of information to the addressee and his right to object.

- As regards the **consumer press**, figures we have received from national publishers' associations, as well as individual publishers, in the following Member States show that such marketing letters to third party addressees without consent account for the following percentage of subscribers for various publications: in Germany (up to 20%, as regards regional and local newspapers: a recent inquiry revealed that 20 % of new subscriptions and up to 50 % of new temporary subscriptions

depend on direct marketing via addressed letters without prior consent; France (up to 42%); Sweden (up to 46%); Portugal (up to 95%); UK (up to 45%).

- As regards the **business press**, B2B magazines are often sent to their readers (e.g., doctors, computer and financial specialists etc.) based on special address lists of the respective target group for free and without prior consent. This so-called '**controlled circulation'** (which accounts for up to 90% of the readership of some business titles in some Member States) is necessary to advertise for a subscription of the magazine but also to secure the required reach in order to attract advertisers and therefore to finance the magazine. This would simply not be possible anymore if this form of marketing was not allowed. The benefits to both customers and publishers from this approach can be contrasted with the marginal objection rates to receiving direct marketing by mail without prior consent (e.g., less than 10 objections out of 100,000 letters).

The Regulation's proposed wording also raises the question of whether external service centres (e.g., subscription fulfillment houses) to which publishers provide personal data to distribute their magazines, would be in breach of the Regulation.

Information and control guarantee the right of self-determination of the consumer. This is guaranteed in the proposal for a regulation. It is stipulated that an individual must be informed about the processing (Article 14) and may object to it (Article 19 (1)). Specifically for direct marketing, a provision was introduced according to which the person concerned has not only the right to object to the processing of their personal data for direct marketing purposes, but must also explicitly be informed about this right (Article 19 (2)).

It must also be ensured that no requirements are introduced, that can only be relatively easily fulfilled by large, globally active companies but not by the majority of small and medium-sized enterprises in Europe (see point 2(d) above for further details). In addition, there is the practical concern that the broad definition of personal data would lead to an inflation of consent requests to the user and to a huge volume of data in the databases of the companies.

Furthermore, when discussing direct marketing it must not be forgotten that the aim is to create a legal framework for the processing of personal data. The problem of annoying advertising or unsolicited messages is already sufficiently regulated in the Unfair Commercial Practices Directive 2005/29/EC (in particular Articles 6, 7, 8 and 9) and the E-Privacy Directive 2002/58/EC (see in particular Article 13).

b) <u>Article 6 (4)</u>

The current wording also does not guarantee that publishers can continue to address existing customers. The conditions for a legitimate change of purpose for further processing must take account of all possible forms of data processing. Data processing for purposes other than to those for which the data were originally collected can be necessary and in the interest of the customer for various reasons. It must, for example, remain possible for press publishers to send addressed direct marketing letters to their own readers or former readers, to inform them about a new subscription offer for a new or even the same publication, even if those readers have not originally given their prior consent to the use of their address also for this specific purpose. Another example is informing a relevant target group about the launch of a new B2B magazine after the success of a certain topic at a trade fair.

Such a change of purpose must be permitted if the conditions for data processing without prior consent within the meaning of Article 6 (1) are fulfilled. The proposal foresees this in Article 6 (4) only for the alternatives of Article 6 (1) (a) to (e) but not for Article 6 (1) (f). There is however no reason for such a limitation. On the contrary, this would lead to the anomaly that for personal data, which has been previously collected or used, including with consent for the original use, stricter rules would be applied than for such data that has never been used (i. e. Article 6 (1) f) would not apply). This limitation should therefore be removed and Article 6 (4) should generally refer to Article 6 (1).

6. Conditions for consent (Article 7)

a) The establishment of additional requirements for consent must not result in excessive demands that cannot properly be implemented in practice. In particular, the requirement in Article 7 (1), that consent has to be granted for specified purposes, should be deleted. This deletion will avoid long and complex texts having to be used for declarations of consent which are not read by users but regarded as a nuisance.

b) In Article 7 (3), it should be clarified that the original recipient of the consent provided is the sole addressee of the withdrawal of consent. This clarification is essential for cases where the data related to the consent provided are passed on to third parties or published. Furthermore, where there are contractual or statutory "special agreements" in place, these rules apply and have priority over Article 7 (3).

c) In Article 7 (4), it should also be clarified that any assessment of a “significant imbalance” between a data subject and controller must always to relate to individual cases and to the specific consent provided.

7. Information to the data subject (Article 14)

The extension of already considerable information requirements that the data controller is obliged to provide the data subject under Article 14 is apparently aimed at data processing in an online environment. It would be unacceptable however if, as a consequence, traditional and proven marketing channels could no longer be used, because the tremendous amount of required information can simply not be adequately provided. The draft Regulation does not take into account the following:

a) In order to be able to continue to provide appropriate press distribution, it has to be possible to provide information in a general way. The requirement that information has to include the contract terms and general conditions (Article 14(1)(b)), where the processing is necessary for the performance of a contract or to conduct pre-contractual measures, is in particular not practical for direct marketing activities that take place by mail or by phone, as opposed to online. While we have doubts that the information required would in fact bring any added value for data protection. In many cases, the **provision of this information e.g. on an order card, as regularly used for subscriptions, will simply be impossible**.

b) In many cases it **will not be possible to pre-determine the period of data storage (Article 14(1)(c)) in advance**. At the time of conclusion of a subscription for an unlimited period it is impossible to know the length of the subscription period, and thus for how long the personal data has to be stored. Even after the termination of the contractual relationship there might be a legitimate interest to continue using the respective data.

c) The obligation to **indicate the contact details of the supervisory authority (Article 14(1)(e) combined with the liability for any incorrect information** will be a further burden for businesses.

d) It is unnecessary for the data subject to be informed about the recipients or categories of recipients **(Article 14 (1)(f))** of the data in circumstances under which he would already expect that data to be forwarded without receiving such information (for example to a subcontractor).

e) Information about the intention of the data controller “to transfer the data to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission” (Article 14(1)(g)), **can often not be realised in a practical manner**. It must be considered that this requirement would already apply if only parts of the data processing, e.g., the invoice processing or material management, take place in a third country. In particular, it is difficult to see how information requirements on the respective level of data protection in a third country could easily be met via certain traditional marketing channels (e.g. a postcard, letter).

f) The already extensive information requirements are even more amplified by a blanket clause obliging the data controller to provide any other information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected (Article 14(1)(h)). This **provision will not provide legal certainty for individual companies** as regards which information must be made available in each individual case.

g) The information provided to the data subject as to whether the provision of personal data is mandatory or voluntary and the possible consequences of failure to provide such data (Article 14(2)) does not only extend the amount of information to be provided, but would in many cases be **unnecessary since it would already arise from the context** (e.g., the indication of a delivery address for the delivery of a subscription is necessary in order to receive the respective newspaper or magazine). However, it must be at least possible to provide this information using representations appropriate to the circumstances (e. g. asterixes to indicate the mandatory information).

h) Where the personal data is not collected from the data subject, the data subject has to be informed according to Article 14(3), as regards the source from which the personal data originated. This general obligation is too extensive and not necessary, particularly in light of the fact that the respective data could also come from public sources or may have been published by the data subject in question.

i) The requirements regarding when information has to be provided (Article 14(4)) do not take into account the fact that data are usually obtained in traditional press distribution on completion of the order form, etc. The obligation to provide this amount of information would mean that **this sort of distribution would simply be no longer feasible**.

j) For the many publishers that still depend on traditional practices for gathering and processing personal data (e.g., with regard to subscription marketing that is highly dependent on traditional tools, such as postcards or return coupons) it would in many cases be **impossible to fulfill the new information requirements** suggested under Article 14. Furthermore, the threat of huge fines of up to 1% of the worldwide annual turnover of the company which does not provide information or provides information in an incomplete or insufficiently transparent manner (under Article 79(5)(a)) leads to a **significant risk that businesses will want to avoid.** It therefore **needs to strike a better balance between transparency and practicability**.

k) The **exemption to the information requirements** under Article 14 (1)–(3) set out in Article 14 (5) (a) – i.e., where the data subject already has the information referred to in those paragraphs - **needs to be extended** to those cases where the data subject has to expect a respective data processing procedure based on their experience of common practices. This scenario should be treated in the same way as those cases where the person already has the information.

l) In addition, the **information requirements should not apply where communication of the respective information is impossible**, regardless of whether the data have been collected from the person concerned or not. The Commission proposal is disproportionate on this point by limiting this exception to only cases where data are not collected from the data subject. This limitation should therefore be deleted from Article 14 (5)(b).

8. Right of access (Article 15)

Under the suggested new rules on the right of access, which go further than the current rules, many of the requirements for controllers are excessive and would pose the risk of being an unmanageable burden on many publishing houses:

a) The data subject now has the right to "obtain from the data controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed". This creates an **unreasonable burden**.

   Our comments on the need for information obligations to be significantly reduced in the context of Article 14 are also valid here. In many cases, the obligation to inform the data subject will not be practicable. Many publishers for example do not use "plain data" for the representation of certain internal transactions, but certain variables instead (e.g., specific figures which correspond to specific products or processes). Apart from the fact that the information about the relevant data could possibly affect trade secrets of the company (e.g., relating to internal processes), the advantage gained by consumers in these cases would, we believe, most likely be accordingly low.

   Furthermore, it is unclear what is meant by the requirement in Article 15 (1) (h) to provide information about "the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20". We believe that this extension of the information requirements is unnecessary.

b) The obligation in Article 15(2) to provide the information in electronic form when the data subject has made the request in electronic form **poses unmanageable risks to businesses**. It is generally not possible for a company to verify if the person about which information has been requested is the same person requesting the information, where the request has been made in an electronic format. Therefore such a requirement poses a significant risk of obliging businesses to disclose data to unauthorized people. It should therefore only be incorporated as an alternative, but not as a duty.

c) Exclusion of right of access. The right of access shall give the data subject the possibility to understand who has stored which personal data about him. This right is therefore taking account of the fact, that the data subjects often do not have their own access to their personal data. In certain cases however this interest of the data subject does not prevail any longer, if for example the data subject already has the information (Article 14 (5) a). The same must apply when the data subject has access to the stored personal data at any time (e.g. via a customer profile on the Internet). An interest in information that might justify a right of access does also not exist, if the processed personal data are publicly accessible.

9. Right to be forgotten and to erasure (Article 17)

The right to be forgotten and to erasure in Article 17 could be extremely problematic for readers' contributions (e.g. comments, contributions to opinion forums, product reviews, etc.) in the context of professional journalistic offerings. Furthermore, these requirements might also be a significant burden to other forms of data processing, for example regarding the processing of an objection in the sense of Article 19.

a) First of all, Article 17 itself is worded so broadly that it allows for not only deletion of people's own posts, but also the deletion of posts by others referring to another person, by giving the right to request deletion of content *relating to* the person concerned.

b) It is **questionable whether the exemption in Article 17(3)(a) for exercising the right of freedom of expression in accordance with Article 80 is sufficient for publishing houses**. While this exception would indeed have a wider scope with a broad definition of journalistic activity (in Recital 121), it is not clear whether this broad definition will remain.

c) **Requiring publishers to delete commentaries** of readers, not only under instructions from the person posting the comment, but also from someone that this person was commenting on (e.g., a powerful person that does not particularly like what has been written) with the threat of a fine of 500,000 euros or up to 1% of worldwide turnover for an enterprise (Article 79), is **disproportionate** and would interfere with the (often pseudonymous) dialogue which is only understandable if the entire context is published.

d) Furthermore, such an obligation leads to a **considerable burden for web site operators, but also for companies that process the corresponding data by traditional means**. This applies equally to the obligation contained in Article 17 (2), to inform third parties about the desired deletion. This obligation should therefore be deleted.

e) As regards **direct marketing**, the problem might arise that a person asks for the deletion of data about him/herself because he objects to the processing of his data for future direct marketing. However to comply with the proposed rules, his address must be blocked, and not deleted, to avoid his address being used for future promotional activities. Article 17 (4) refers to cases where instead of a deletion of data, the data processing might be restricted. It is nevertheless questionable whether this provision indeed covers all relevant cases. The Commission points out in the explanatory memorandum to its proposal for a regulation under section 3.4.3.3 that it wants to avoid the ambiguous expression "blocking". However, it has to be ensured that at least cases and particular situations like the one described above are also regarded as an exception.

   This could be clarified, for example, by deleting the possibility for the data subject to object to the processing of personal data pursuant to Article 19 (under Article 17 (1) (c)) and specifying that instead of erasure, a limitation of the data processing is also possible if the data processing officer must retain the data. There should also be the possibility to waive erasure if the deletion is associated with a disproportionate effort; affects the legitimate interests of the data subject; precludes the predominant legitimate interests of the data controller or a third party; the attribution of the data stored to the data subject based on the information provided would necessitate disproportionate effort; or the data subject has not been identified itself with sufficient certainty.

10. Right to data portability (Article 18)

The right to data portability, and in particular the obligation to grant to the data subject the opportunity to transmit their personal data and any other information provided by the data subject in an electronic format which is commonly used into another automated processing system, will in many cases be **difficult to realise**.

Many publishing houses do not save the data in a standard electronic format which is commonly used, but use specific formats, tailored to their specific needs. A relevant transmission would be in many cases not only be technically difficult, but in addition would not necessarily reveal any relevant information concerning the data subject, since the corresponding data are often not presented as plain data, but it is rather variables that are used.

If this right is maintained, however, it has be ensured at the very least that the data controller is not disproportionately burdened. In particular it must be possible to charge the person concerned for the costs associated with this purpose.

11. Right to object (Article 19)

The new formulation of the right to object in Article 19 creates legal uncertainty for businesses and unnecessarily makes them vulnerable to huge fines:

a) The proposal foresees a general right to object in Article 19 (1) and thereby changes the current effective and proven provision on objection set out in Article 14 (a) of Directive 95/46/EC where the data subject has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him. There are no known practical problems in this area which would justify or necessitate such a legislative

change. This is particularly significant as the Regulation will now apply directly and thus without the flexibility of the Directive.

b) It is not taken into account that it may be necessary to retain certain data even after objection. In this respect it is preferable that the wording used in Article 14 (a) of the current Directive- is also used in the new Regulation.

c) Furthermore, it would be clearer if the legal consequences for an objection being upheld were set out on a case-specific basis in paragraphs 1 and 2, rather than being regulated under Article 19(3). Paragraph 1 should therefore specify that in cases of justified objection the processing by the controller may no longer refer to this data. In paragraph 2, it should be clarified that in the case of a justified objection the processing by the controller may no longer refer to this data for direct marketing.

d) Another problem is that it is not clear when the information about the right to object can be regarded as **"intelligible"** as defined in Article 19 (2). In addition, it is not taken into account that a clear, explicit and understandable notice is also possible, where - such as on a post card - due to limited space a spatial separation from other information is not possible. This leads to considerable legal uncertainty, which can have significant consequences for companies because under Article 79 (6) (c) a violation of this obligation is threatened with a fine of up to 2% of the global annual turnover of the company.

e) The question also arises as to whether it is not already a **prohibited use or processing according to Article 19(3), if the data processing company records the objection of the data subject** to its personal data, which is probably regularly required in order to comply with the respective obligation.

12. Profiling (Article 20)

The future of newspaper and magazine publishers depend on their ability to respond to users' demands for innovative digital offers on various platforms (online, tablets, mobile, smart phones, etc). These challenges not only concern how editorial content can be received under various forms, but also how advertising can be displayed in the digital environment. Article 20 relating to profiling, which goes beyond the current EU rules on automated individual decisions (Article 15 of Directive 95/46/EC), **threatens to prevent the development of digital publishing** and the competitiveness of the European press in the digital environment by the burdens it creates.

Due to the general formulation of Article 20 there is the risk that this provision might also **significantly burden traditional and proven business models or even make them impossible**:

a) It is not defined, in particular, when and which consequences of a measure **"significantly affect"** a person. Therefore it cannot be excluded that certain forms of direct marketing activities or certain forms of controlled circulation of journals could be affected by this provision. In addition, this provision could have an impact on online advertising methods such as e.g., so-called online behavioural advertising.

b) Furthermore, it is not clear which conditions a measure must fulfill to be based solely on automated processing of data. This is especially true for cases where the corresponding data processing is automated but based on previously determined criteria. The scope of the provision has been extended in comparison to the current Directive (Article 15) to those measures intended to analyse or predict certain personal aspects related to the data subject.

   It cannot therefore be excluded that numerous data processing processes that are important for publishers, such as **measures within the framework of customer relationship management,** or certain forms of interest-based advertising that might be relevant as an important form of advertising in the online publishing sector, also fall under this provision, and **may be negatively impacted**.

c) Due to its large scope, this provision **could even apply to certain forms of data processing, which do not identify a particular person**, such as the creation of pseudonymous or even anonymous user profiles for the purpose of excluding the identification of the data subject or to make it significantly more difficult. As pointed out in Recital 24 identification numbers, location data, online identifiers and other specific factors as such, do not necessarily need to be considered as personal data in all circumstances, but it is also not completely excluded from the scope of the provision. Therefore, there is still the possibility that this could include certain forms of data processing which are relevant for publishers, such as certain ways of contacting their own customers, certain forms of direct marketing or new forms of online advertising, etc.

   In this case, the strict requirements of Article 20(2) would then also be applicable for those measures, and the processing would be subject to the general requirement of consent of the data subject, if the profiling is not carried out during the course of entering into or fulfilling the contract or authorized by an EU or Member State law. Furthermore, it is not taken into account that certain national rules already provide for a variety of data processing procedures more detailed rules. The German Telemedia Act (Telemediengesetz), for example, ensures the necessary consumer protection by introducing a prohibition of merging pseudonymous user profiles with the owner of the profile combined with a penalty and the right to object for the individual. It also remains unclear how anonymous profiling would affect the interests of the person which is unknown to the data processing entity.

d) Although certain forms of data processing continue to be regulated under the provisions of the E-Privacy Directive (such as e.g. the setting and reading of cookies), other forms could end up being covered by the Data Protection Regulation. Those could be considered as profiling measures in terms of the Regulation and the more stringent requirements of the Regulation would therefore apply to them.

13. Responsibility of the controller (Article 22)

The obligations of the controller laid down in the draft Regulation would in many cases constitute a significant burden for companies. Due to the general concerns relating to the obligations laid down in Article 34 concerning prior authorisation of data processing, the reference to this provision in the obligations in Article 22 (2) (d) should be deleted.

To clarify that the review of the effectiveness of the procedures established by the controller can continue to be carried out, for example, by the internal auditor or the company's data protection officer, the ambiguous definition that the control must be carried out by independent internal or external auditors should be deleted.

In addition, it cannot be excluded that the processor also employs staff not involved in the data processing. There is no reason to demand the fulfillment of strict confidentiality obligations for these employees. Article 26 (2) (b)) should therefore be changed so that this requirement must only be satisfied as regards those staff which are entrusted with the processing.

It is also not obvious why under Article 26 (2) (h) there is a general obligation for the processor to provide information. It should be considered sufficient when the information is made available upon request.

14. Data protection by design and by default (Article 23)

The requirements for the implementation of data protection by design and by default require assessment by the companies concerned, having regard to the state of the art and the cost of implementation, which **especially for small and medium-sized companies will not be easy to realise**.

The application of this provision would in many cases impose a subjective view on users as regards what data protection settings should look like. This raises the question as to how consistent such a requirement is with the overall concept of a responsible consumer, who is usually regarded as being able to make an informed decision.

Furthermore, there is also the risk that such a general determination leaves no room for privacy settings that are more adapted to the individual needs and which can be stricter, less extensive or simply differentiated. For example, modern browser settings already provide users with the choice, as to whether they want to accept cookies in general, for the current browser session only, or on a case by case basis.

15. Processor (Article 26)

The possibility to undertake data processing by outsourcing it to data processors is essential for many businesses and business processes. Therefore, it must be ensured that the review of the regulatory framework does not make these proven and important forms of outsourcing of certain tasks practically impossible. Against this background it should be considered sufficient in Article 26 (1) that the selected processor provides reasonable assurance for compliance with the respective obligations under the Regulation. The term currently used - "guarantee" - could easily be misunderstood.

16. Co-operation with the supervisory authority (Article 29 and Article 53)

It has to be ensured that the review of the regulatory framework does not lead to a mixing of responsibilities. It has to be ensured that the data controller does not become the deputy of the supervisory authority. However, there is this very risk in view of the formulation of Article 29 (1), which might be interpreted as broad obligations of the controller. It should rather be stressed in this provision, that the authority should advise and support the controller, the processors and any representative of the controller with regard to their typical needs. In addition, it should be made clear that the obligations of the controller, the processor and any representative of the controller vis-à-vis the supervisory authority alone is to provide it with the information necessary for the performance of its investigative powers under Article 53. The duties and powers of the supervisory authority are exhaustively regulated in Article 52 and 53 respectively of the draft, so further specifications contained in Article 29 (2) should consequently also be deleted.

17. Bureaucratic burden on businesses must be reduced

One of the aims of the Regulation is to reduce bureaucratic burdens for companies. This will only be achieved if, in return, there are no new burdensome requirements introduced, such as extensive information (e.g. Articles 14, 15), documentation (Article 28), notification (Art. 31, 32) and consultation requirements (Articles 33, 34).

18. Certification (Article 39)

The requirement in Article 39 for the Commission and Member States to encourage the establishment of data protection certification mechanisms and of data protection seals and marks runs the risk that such certification can easily lead to a *de facto* mandatory certification requirement for businesses.

This is especially true if such certification gives the impression to the public that only the certified processes, technologies, products or services meet a certain data protection level.

Furthermore, certification requirements could result in a competitive advantage for large and financially strong businesses compared to SMEs which cannot afford costly measures.

19. Right to lodge a complaint and to engage in court proceedings (Articles 73, 76)

The Regulation now extends the right to lodge a complaint and engage in court proceedings for any individual, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data..

We believe that the right for e.g., civil society associations to engage in, or pursue, legal proceedings along with supervisory authorities would lead to a confusing co-existence of roles and more legal uncertainty.

20. Sanctions and fines for breaches of data protection law (Article 79)

The fines for breaches of data protection legislation have increased significantly under the proposed Regulation. General fines of up to 0.5%, 1% or 2% of annual worldwide turnover of the company are foreseen, compared to e.g., German Law which foresees fines of up to 300.000 Euros (which can only be exceeded if this amount does not exceed the economic advantage of the offender).

This increase is unjustified, especially with regard to some of the provisions which foresee fines in case of a breach (e.g. insufficient compliance with the extensive information requirements in Article 79(5)(a)).

The obligations are also often provided by general clauses or formulations which leave room for wide interpretations. This couldlead to a situation that companies cannot oversee all their duties and obligations in an acceptable and manageable manner. The uncertainty created by Article 79 as regards legal obligations, combined with the significant amount of the fines, amounts to a considerable and unacceptable risk for companies.

21. Exemption for processing of data for journalistic purposes (Article 80)

An exemption for journalistic data processing is essential to ensure that journalists and publishers can continue fulfilling their democratic mission as regards investigating, reporting, writing and publishing editorial content without any obstacle, and to ensure that sources are adequately protected. Even though the Commission proposes to retain the existing exemption for journalistic data processing, it has to be ensured that with the change to a Regulation the level of protection will not be lowered:

a) The **chapters referred to in Article 80 must be immediately and without further modification excluded from applying to journalistic data processing**. The Commission proposal continues to leave it up to the Member States to provide for such exemptions. The current national exemptions in force in the Member States would no longer be applicable under the new Regulation and it cannot be foreseen whether all Member States will introduce new robust exemptions without hesitation. Any implementation of this provision by Member States carries the risk of restrictions to the existing standards of protection of editorial press freedom.

b) Furthermore, the **exemption should be extended to Articles 73, 74, 76 and 79** of Chapter VIII (on Remedies, Liabilities and Sanctions). This is because they include elements such as complaints to the supervisory authority, which are not suitable considering that the exemption for journalistic purposes is supposed to avoid supervision. We also believe that the current wording of Article 80, by listing the titles of each chapter before each chapter number, could lead to a misinterpretation that it is not the chapter as a whole which is to be excluded from the application but only some parts of the

chapter (e.g. only the general principles in chapter II rather than the whole of the chapter entitled "general principles").

c) It should be underlined that this direct application of the exemption is **consistent with the subsidiarity principle**. The journalistic activities which are foreseen to be excluded from the data protection Regulation via the exemption for journalistic data processing, can still be covered by media, libel and privacy laws. These are mainly characterized by national laws and are therefore covered by Member States' fundamental rights. This means they are thus open to legal action via Member States' constitutional courts.

d) It should also be noted that the proposal suggests that activities are "journalistic" if 'the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes' (see recital 121). It **must be ensured, however, that the protection of the editorial processing of the press is not weakened** as a result of these non-journalistic expressions of opinion also be covered in the definition.

22. Relationship with the E-Privacy Directive (Article 89)

Article 89 now clarifies that the E-Privacy Directive takes precedence over the Data Protection Regulation for those cases regulated in it. It is an important step that it is has been made clear that the Data Protection Regulation introduces no duties other than those that are envisaged in the E-Privacy-Directive. Nevertheless, the wording of the Article must not inadvertently undermine the aim of the Regulation in this regard by conferring additional rights to individuals. In addition, not all data processing processes relevant for digital business models fall under the E-Privacy Directive, in which case the Data Protection Regulation would apply. Therefore, it is quite likely that this might lead to further restrictions.

23. Delegated acts

Delegated acts are not the proper instrument to regulate or to specify the right of privacy. In particular, discussions in and with the European Data Protection Committee cannot replace the democratic process.

Data protection legislation has to achieve the sometimes difficult balance between the legitimate interests of the individual and the communication needs of a modern economy. The result of this balancing process can have far-reaching effects on consumers and businesses, and should therefore not be left to a single institution.

In addition, due to the use of numerous general clauses and the reservation of the adoption of delegated acts at various points of the proposed Regulation, it is practically impossible for companies to predict which obligations will actually be implemented. This entails not only the risk of further restrictions, but also leads to significant legal uncertainty for businesses.

CONTACTS:

Sophie Scrive
ENPA Deputy Director
Sophie.scrive@enpa.be
+32 (0)2 551 0197

Catherine Starkie
EMMA Senior Legal Adviser
Catherine.starkie@magazinemedia.eu
+32 (0)2 536 0602