Position Paper

UEAPME[1] position on the proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (COM(2012) 11 final)

1) General remarks

1.1

UEAPME, the European Association of Craft, Small and Medium-sized Enterprises, welcomes the European Commission's intention to establish a new framework for data protection at European level. As stated in our previous papers[2], UEAPME identifies the necessity to adapt the current directive to the challenges and needs linked to new technological developments. We underline that in order to be future-looking all new legislative proposals at European level have to meet the requirement of being technology neutral.

In this respect, we would like to make reference again to UEAPME's most important general views with respect to personal data protection:

- Need for adaptation of the current data protection framework to the new technical developments, especially to the challenges of the online world;
- A high level of consumer protection is needed and has been already ensured by the current framework;
- The balanced approach should lead to the avoidance of inappropriate administrative burdens for SMEs;
- Need for proper and clear worded rights and obligations for the data subject, controller, processor and data protection officers;
- In order to avoid additional administrative burdens on SMEs clear, understandable and user-friendly provisions are from outmost importance;
- In addition, information campaigns on personal data protection backed by EU funding should be carried out at European, national and regional level in partnership with representative SME organisations.

[1] UEAPME subscribes to the European Commission's Register of Interest Representatives and to the related code of conduct as requested by the European Transparency Initiative. Our ID number is 55820581197-35.

[2] http://www.ueapme.com/IMG/pdf/110114_pp_personal_data_protection.pdf
http://ueapme.com/IMG/pdf/091218_pp_data_protection.pdf

1.2

UEAPME welcomes the European Commission's approach to adapt the proposal to the needs of small- and medium sized enterprises. In order to do so, several provisions make reference to SMEs and through concrete exemptions administrative burdens and extra costs should be eliminated. This shows how seriously the European Commission is taking its intention to strengthen the economic position of SMEs, which are in fact the backbone of the European economy. In order to achieve the necessary positive effect, it is important to align the whole proposal with the original intention of the European Commission on SMEs. Part II of this position paper (specific remarks) lists the issues where UEAPME sees the need for further steps in this respect.

Further to the aforementioned general principles, UEAPME has identified some other points which would need further consideration during the forthcoming legislative procedure.

In general, the form of a regulation is qualified to provide a coherent system of provisions throughout all Member States. It also ensures the same rules without running the risk of legal fragmentation because of the different implementations in the Member States. However, with respect to this proposal, the form of directive would also achieve the aim of the review of the data protection framework. It has to be borne in mind that in general the currently existing framework is considered as well functioning. The necessity to review is linked to the new technical developments and challenges. In order to adapt, there is no need to change the form of the legislative act.

In this respect, the extended use of delegated acts has to be mentioned as well. On one hand, it is understandable that in such a complex topic, where further criteria and requirements have to be reflected on, the Commission is going back to this instrument. In this way, it could be ensured that the legislator can react quickly on the legal challenges of the technical developments. However, through this extensive use we see the danger that no legal certainty will be provided and the user-friendliness of the proposal for all parties may be jeopardised. The approach gives the impression that the European Commission would like to ensure in this way the flexibility of the future regulation. According to UEAPME, this will also lead to less transparency. Moreover, this means that this process can lack of appropriate stakeholders' input and involvements. It really has to be evaluated whether all delegated acts proposed for the future directive would indeed be necessary and where it would make more sense to have from the beginning clear rules instead of making use of delegated acts later on.

UEAPME doubts that it will be at all possible for SMEs to follow when and in which respect the European Commission makes use of delegated acts. The necessary flexibility could also be provided through a directive, where Member States would have a broader room of manoeuvre. In this respect, the right balance has to be found during the ongoing legislative procedure.

Although the proposal is exclusively dealing with the protection of individuals and their personal data, UEAPME sees the need to make reference also to the protection of legal persons. It should be borne in mind that the data protection of enterprises in respect to their trade and industrial secret is at least as important as the data protection of individuals. Particular attention has to be given to the relation between SMEs and big enterprises in this case. Concerning this question, there is a demand for subsequent improvement. Moreover, the question of the missing distinction between private and public field regarding data protection would need detailed analysis and consideration.

On some points, UEAPME is under the impression that the proposal is not meeting one of its main challenges, namely to establish a framework in line with new technical developments. For example, the question of how SMEs should be able to verify the identity of the data subject in relation to the use of internet was left out of the proposal. In this respect, obligations are often put on the controller, but the practical feasibility was not taken into account (e.g**. article 8** and **article 11** and related obligations). Also, **article 7** on the condition for consent is

MAISON DE L'ECONOMIE EUROPEENNE - RUE JACQUES DE LALAINGSTRAAT 4 - B-1040 BRUXELLES
TEL +32 (0)2 230 75 99 - FAX +32 (0)2 230 78 61 - E-MAIL info@ueapme.com

not taking at all the issue of "cookies" into account. We urge the European Parliament and the Council to adapt the provisions to these relevant questions.

It also must be ensured that SMEs have flexibility when it comes to the transmission of information to the data subject. The decision of how and in which way required information by the data subject is delivered has to be left to the controller (e.g. **articles 11, 15 and 18**). This is also important to avoid administrative burdens for SMEs. UEAPME has some doubts that the proposal will not meet this requirement. Some examples of these aspects can be found more in detail further below, **article 13 and article 33, 34**. There is also a need for transitional provisions in order to ensure legal certainty between old and new facts of a case.

2) Specific remarks

The European Commission has chosen to follow a very broad approach concerning the definition of "personal data" according to **article 4(2).** This way is for several reasons doubtful. UEAPME sees the danger that on the one hand it would increase burdens on SMEs involved on e-commerce, *inter alia* because of a possible inclusion for example of IP addresses. There is a need for clarification also concerning **recital 24** of the proposal, which states that there is no need to identify "identification numbers, location data, online identifiers or other specific factors as such" as personal data "in all circumstances". This approach is welcome and should be put forward.

Besides these specific remarks, the definition should reflect the nowadays characteristic trends when it comes to the use of personal data by the data subject. To publish these data and make them accessible on an unsolicited way on the internet in general and especially on the so called social networks is a normal behaviour of data subjects nowadays. Because of the broad definition of the proposal, any kind of information related to the data subject could be interpreted as personal data. For this reason, UEAPME calls for a more realistic and future looking approach in this respect, which takes the technical developments and social behaviour of data subjects into account.

Article 4(8) is dealing with the definition of the **"data subject's consent"**. According to this provision, there is the *"explicit indication"* required by the data subject, *"either by a statement or by clear affirmative action signifies agreement to personal data relating to them being processed"*. UEAPME has been advocating for a detailed analyses of this approach in order to see if there will be any added value by this. According to our view the issue on the "explicit indication" can burden the future looking characteristic of the proposal. One of the European Commission's aim, which is fully supported by UEAPME, to establish a coherent framework in all policy fields for the new technologies, especially for the growing importance of the online world. Especially for this reason the issue on the "explicit indication" is getting even more important for these fields. According to **article 7**, the controller bears the burden of proof on whether the consent was given by the data subject or not. This would make the situation difficult especially for websites and would require the registration of the data subject for every website. It would also slow down and burden innovative possibilities for this field. Moreover, for SMEs this would mean enormous administrative and financial burdens to fulfil to obligation of getting the "explicit consent" of the data subject according to the requirement of the proposal. Because of protective measures,SMEs would have to archive the explicit consent of the data subject. The experience of our members shows that this can have a cost of thousand of euros.

According to our understanding, **article 10** on the "processing not allowing identification" is aiming to solve the aforementioned problems, mentioned under 4(8). UEAPME thinks that this collection of provisions is not understandable for SMEs and asks for clearer rules. There are several solutions which in our opinion would more suitable to regulate this problem while still ensuring security for the data subject. It would be possible for instance to establish an opt-out system when it comes to the consent of the data subject. There are also examples which make the distinction between sensible and non-sensible data. In these cases the consent of the data subject could be linked to the sensible data of the data subject.

MAISON DE L'ECONOMIE EUROPEENNE - RUE JACQUES DE LALAINGSTRAAT 4 - B-1040 BRUXELLES
TEL +32 (0)2 230 75 99 - FAX +32 (0)2 230 78 61 - E-MAIL info@ueapme.com

According to **article 5 (f)**, the controller is obliged to "*demonstrate*" that each processing operation is in compliance with the proposal. Beside of the fact that this provision will add burdens for SMEs it is also the question how far this provision can comply with the erasure of personal data.

Article 6.1 (b) will heavily burden SMEs in contractual relations. According to this, the use of personal data is only considered as lawful if it is happening *"in order to take steps at the request of the data subject prior to entering into a contract*". However, it is not clear enough what should be considered as a request. The fulfilment of any pre-contractual obligations by law cannot depend on any kind of *"request*". UEAPME sees the danger that this provision will cause difficulties when it comes to the application of the recently adopted Consumer Rights Directive[3]. According to the directive, in case of consumer contracts the trader is obliged to provide to the consumer a bundle of pre-contractual information. It is not clear how the mentioned provision of article 6.1 (b) will comply with the Consumer Rights Directive if the trader is sending the pre-contractual information via email to the consumer, since this email address is considered as personal data. We would like to underline that the too extensive involvement of the data subject in this request would cause even more burdens for SMEs.

Article 6.1(f) is stating with respect to the **lawfulness of the processing** that the processing of personal data is considered lawful if the *"processing necessary for the purposes of the legitimate interests pursued by a controller"*. UEAPME considers this requirement as too vague and would like to ask for more clarification on it. In this respect, we also would like to draw to attention that the requirement of article 7(f) of Directive 95/46 is missing as well. According to this article "*personal data may be processed only if (...) the processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed"*.

Article 7.4 states that in case of a significant imbalance of the position of the controller and data subject, the consent is not considered as a legal basis. However, when and under which circumstances such an imbalance exists is unclear. In order to avoid legal uncertainty, UEAPME sees the need to revise the concept of article 7.4.

With respect to **article 8**, processing of personal data of a child, it is important to highlight the well known problem of the use of internet and the age of children. According to our observation, the proposal has missed to provide a future looking solution to the question of what happens if the child has not provided his real age in the online world (e.g. what kind of legal consequences does it have for a contractual relation etc). We urge to deal with this problem and related legal questions more in detail.

Article 9.2(b) is a crucial provision from the SME point of view. We welcome that the processing of personal data is permitted if it is necessary in the field of employment law. We would like to draw to attention that at national level the issue is already settled in well working manners, and heavy efforts were done in order to establish these good practises in all parties' interest. It would not be useful if the already existing good practices in this field would not apply any longer.

With respect to **article 12.2**, the one month period in order to give requested information by the controller to the data subject is considered as far too short. UEAPME asks to extend the general period up to eight weeks to give SMEs sufficient time to deal with those requests. We take reference to the "Think Small First" principle and remember the legislator that SMEs, which represents 99.8% of all enterprises, have in general limited human resources. For this reason, it is necessary to establish a legal framework which meets at every place the characteristics of SMEs.

As it stands in **article 12.4 "***manifestly excessive*" needs more clarifications, since there is no clear indication of what is meant in this respect. Moreover, the obligation to provide free of charge the information requested by

[3] Directive 2011/83/EU of the European Parliament and of the Council

MAISON DE L'ECONOMIE EUROPEENNE - RUE JACQUES DE LALAINGSTRAAT 4 - B-1040 BRUXELLES
TEL +32 (0)2 230 75 99 - FAX +32 (0)2 230 78 61 - E-MAIL info@ueapme.com

the data subject without any restriction is imbalanced. There are more reasonable ways and solutions which could be followed and would on the one hand ensure the free access to the requested information for the data subject, but would not on the other hand mean extra burdens for SMEs.

Article 14, information to the data subject and **article 15,** right of access for the data subject, contain a far too extensive list of obligations for the controller. These two articles are following the practice that the more information is dealt with the more security and knowledge is ensured in favour of the data subject or consumer. The fact that the amount of information is not and cannot be followed by the data subject, or in other cases by the consumer, and put unnecessary burdens on SMEs is not taken into account. It would be necessary to understand that quality goes before quantity of information. Also a more practical approach is needed, since for example **article 14.1(c)** is obliging the controller to give the data subject information about "*the period for which the personal data will be stored*". However, this provision is not taking into account that it is often very difficult for the controller to foresee the exact period. For this reason, a lighter wording which provides on the one hand the information and security for the data subject, but also gives the necessary flexibility for the controller in order to put forward his economic activity without burdens, is needed.

According to UEAPME's position the issue of **article 17**, right to be forgotten and erasure, is far too difficult and challenging to follow for SMEs. For example, **article 17.3** is stating that the controller has to "*carry out the erasure without delay"*. What "*delay"* in this respect exactly means is not clear. It is also necessary to mention that delays are sometimes not related at all to the controller. We see the need to rethink the concept of this article in order to make it practically feasible for SMEs.

With respect to **article 19.1** on the right to object, in order to avoid legal uncertainty UEAPME asks to put forward the already applicable and well established provision in this respect[4] which takes reference on the particular situation of the data subject instead of taking reference on the "*compelling legitimate grounds*".

According to **article 19.2 of the right to object**, when it comes to direct marketing the data subject shall be offered *"to object free of charge to the processing of their personal data for such marketing."* UEAPME does understand the practical intention of the European Commission to protect data subjects from the overload of advertisements and marketing offers. UEAPME would welcome if the in several Member States already existing and working system would be maintained. This allows the data controller to send direct mailings for commercial purposes to its **customers** (and for legal persons/companies) without their consent, unless they opt-out. Getting consent from the recipient for every direct mailing or providing an opt-out every time (also for direct mailings to customers) would pose disproportional burdens on SMEs for gathering the proof of consent. It also needs more clarification how often the right to object should be provided to the data subject. Is it enough if the controller processing the personal data is offering the right to object once, or does s/he have to provide it regarding every direct marketing undertakings?

Chapter IV Section 1 is laying down the **General Obligations** of the controller and processor. In general **article 22**, responsibility of the controller is introducing a series of excessive measures in order to be in line with the provisions. Nevertheless, UEAPME welcomes in general that with respect to the documentation responsibility of the controller (**article 22.2(a)) article 28** is excluding SMEs if they *"processing personal data only as an ancillary* "to their main activities. However, we are wondering if the absence of any documentation in line with **article 28** would not have an effect if it comes to the application of **article 30** on the Security of Processing and in this relation to **article 31**, Notification of a personal data breach to the supervisory authority. It is important that all the elements of article 31, notification of a personal data breach to the supervisory authority can be fulfilled without having documentation according to article 28. In this respect UEAPME sees the need to clarify the situation in case of breach of data security. Although article 30 is mainly following the

[4] Article 14, Directive 95/46/EC

MAISON DE L'ECONOMIE EUROPEENNE - RUE JACQUES DE LALAINGSTRAAT 4 - B-1040 BRUXELLES
TEL +32 (0)2 230 75 99 - FAX +32 (0)2 230 78 61 - E-MAIL info@ueapme.com

approach of the current directive, a clear distinction between the duties of the processor and the controller in respect of the security of the processing would be welcomed. See our detailed remarks further below.

The controller's responsibility contains according to **article 22** the performance of a data protection impact assessment as well. Here again, we see a link to the issue of the documentation. In practice, impact assessment should take place before the processing operation. In case an impact assessment is required because of the nature of the processing activity it should contain, according to **article 33.3** *"at least a general description of the envisaged processing operation".* This article comes to application in general in case of "*specific risks to the rights and freedoms of data subjects*" which are than further in paragraph 2 specified. If an impact assessment is required, then the exclusion from the documentation obligation (**article 28.4.b**)) could be confusing for an SME. UEAPME also sees the need to rethink the concept of article 33 as such. In general, we consider this provision too vague and burdensome with respect to the constantly changing and improving technical circumstances. Unnecessary and costly delay of the data use/application can be expected. Should the concept of the provision be kept, it would be necessary to exempt SMEs from this obligation.

The same comments can be made to **article 34,** on the prior authorisation and prior consultation. If it isgoing to take place, according to paragraph 6 of the article, impact assessment should be provided for the supervisory authority and any other information as well. We think that the range of any other information is quite broad and in cases where is no documentation the SME which is acting as a controller or processor can face difficulties. In order to avoid any confusion in this respect, clarification is needed.

Regarding **article 28**and **article 35.1**, the European Commission has rightly identified that SMEs needs to be exempted in order to avoid administrative burdens of financial and human nature. This approach should be put forward consequently also in respect to article 33, impact assessment and article 34, prior authorization and prior consultation with the supervisory authority.

UEAPME welcomes the exclusion of SMEs from the designation of a data protection officer. Further in the paper we will deal with this issue more in detail.

UEAPME welcomes that according to **article 22.4** the European Commission is "*empowered to adopt delegated acts"* in order to consider specific measures for micro, small and medium-sized-enterprises. Nevertheless, the issue on the responsibility of the controller is considered as a core responsibility. For this reason, UEAPME would prefer to have in this case a way which can be more followed and monitored by the representative stakeholders, especially when it comes to specific measures for micro, small and medium-sized-enterprises. Because of the significance of this article, it is more than crucial that representative stakeholders are involved and consulted id it comes to the application of this provision. We also take reference to our remarks concerning the delegated acts in the general part.

It should be considered whether it would not be useful to delete **article 23.3**. It has to be borne in mind that technical standards are easier to be targeted by "hackers". However, if the article is going to be maintained those technical standards should be plain, unequivocal and easily realisable.

Article 26.4 on the role and responsibilities of processor if the personal data is processed by him differently than instructed by the controller needs further clarification.

With respect to **article 30** on the security of the processing, it would be ideal to have more clear provisions concerning the responsibilities of the controller and processor. Especially **article 30.1** could be harmful for SMEs. According to this article both the controller and the processor are responsible for the implementation "*appropriate technical and organizational measure to ensure a level of security appropriate"*. The main question is how far can a controller, for example an SME, control if the technical measures provided by the processor in order to fulfil article 30.1 are appropriate and sufficient? UEAPME's opinion is that it can happen that in case of

MAISON DE L'ECONOMIE EUROPEENNE - RUE JACQUES DE LALAINGSTRAAT 4 - B-1040 BRUXELLES
TEL +32 (0)2 230 75 99 - FAX +32 (0)2 230 78 61 - E-MAIL info@ueapme.com

an SME the necessary human and technical resources are missing to control the processors technical compliance. We see the need to establish the right balance in this respect.

Article 31, notification of personal data breach to the supervisory authority, foresees in case of personal data breach that the controller notifies without undue delay, and so far it is possible within 24 hours after having gained knowledge about the breach, the supervisory authority. UEAPME fears that, although the "24 hours rule" is not exclusive, it can be difficult to clarify under which conditions the requirement "where feasible" is fulfilled and what this exactly means. We are worried that the interpretation in this respect will lead to legal uncertainty. For this reason, UEAPME advocates for the deletion of the "24 hours rule" and is in favour of following the "undue delay" approach, which would be also in line with the e-privacy Directive (2002/58/EC amended by 2009/136/EC).

We welcome the European Commission's intention to lay down standard formats in the specific case of notifications of data breach to the supervisory authority. In order to have user – and SME-friendly – standard form in this respect, we encourage the European Commission to consult for the drafting the representative stakeholders. The same applies with respect to **article 32.4,** communication of a personal data breach to the data subject.

UEAPME welcomes that enterprises with 250 or less employees are not obliged, according to **article 35.1 (c)** to designate a data protection officer. Nevertheless, we have some doubts regarding this comma. In this point, the proposal is dealing with the designation of a data protection officer in case the "*core activities (…) require regular and systematic monitoring of data subject"*. In practice, there are often cases when this requirement would be fulfilled, e.g. payment by instalments etc. However, through article 35.11 the Commission is empowered by delegated acts for further specification concerning the criteria and requirements if core activities. Because of this reason, any kind of consequences for the practice are uncertain.

Chapter VI contains provisions regarding the Independent Supervisory Authority and **article 52** is listing in detail the duties of it. Looking into these duties, one can observe that these authorities will have at the end a possible monopolistic position on data protection questions and issues. We also fear that the authorities will not be able to deal with all the tasks the proposal foresees for them, and this will have at the end a negative effect on SMEs.

Article 73, on the right to lodge a complaint with a supervisory authority is giving in paragraph 2 the possibility to "*any body, organisation or association*" dealing with data protection "*on behalf of one or more data subjects*" "*to lodge a complaint with a supervisory authority in any of the Member States*" in case infringement of the data subject's right is considered. Paragraph 4 is giving the same possibility in case a "*personal data breach has occurred*". **Article 76.1** is also giving to "*any body, organisation or association*" the same rights when it comes to judicial remedy against a controller or processor in case of a supposed infringement because of non-compliance with the Regulation according to **article 75**.

UEAPME understands that data subjects need support regarding data protection and this support is given by various organisations and bodies. Nevertheless, we think the supportive role should stay in the focus. It should not lead to the situation that these bodies are taking over the lead and bundle data infringements or personal data breaches of the data subjects. Otherwise, we could easily face the situation, which has been already experienced by UEAPME members, that the core activity of these organisations is financially based on these kinds of cases and they will use these situations for profit making. This again can cause significant problems for SMEs. They can easily find themselves involved in court cases or in an enquiry by the supervisory authority. SMEs do not have the human and financial resources to deal with these kinds of organisations. We fear that this possibility given by article 73-75 will be abused by "*any body, organisation or association which aims to protect data subjects' rights*".

MAISON DE L'ECONOMIE EUROPEENNE - RUE JACQUES DE LALAINGSTRAAT 4 - B-1040 BRUXELLES
TEL +32 (0)2 230 75 99 - FAX +32 (0)2 230 78 61 - E-MAIL info@ueapme.com

Article 78 on the penalties is following the minimum harmonisation approach and giving the different Member States the possibility to lay down different rules. We do not see coherence behind this intention. If the European Commission has decided to use the form of a regulation, the establishment of different penalty systems can go against the vision of the European Commission to have a coherent framework for personal data protection throughout Europe. In this context, we take reference on our remarks in point 1.2 concerning the form of a directive.

UEAPME ask for the deletion of **article 77.2**, which foresees a joint liability in case of those damages where more controllers or processors are involved into the processing.

The provisions of **article 79.3** which is providing SMEs (not dealing with data processing as main activity) an exclusion from the sanctions of this article "*in case of a first and non-intentional non-compliance*" is to welcome. The correct conclusion is made, since the complexity of the new proposal towards the currently applicable data protection directive cannot be questioned. In order to get acquainted with all the new provisions, time will be needed and it can easily happen that an SME does not comply non-intentionally with the future regulation. Besides this paragraph, the amount of sanctions from the SME point of view is considered as quite high. We would also advocate in these cases more for an approach linked to diligence instead of the strict liability of negligence.

Article 81 is dealing with the processing of personal data concerning health. It is already predictable at this stage that the requirement of article 81.1(a) that the data processed has to be undertaken "*by a health professional subject to the obligation of professional secrecy or another person*" equivalent will cause administrative burdens for SMEs.For instance, orthopaedics, opticians, dental technicians etc. will be affected by this. For this reason, UEAPME asks for the deletion of this article.

Brussels, 26 April 2012

For further information on this position paper, please contact:

Dora Szentpaly-Kleis
Adviser for Legal Affairs
Rue Jacques de Lalaingstraat 4
B-1040 Brussels
Tel: + 32 2 230 7599
Email: d.szentpaly@ueapme.com