Data Protection: reform for SMEs, not at their expense

MEPs will soon be asked to vote on the EP position on the General Data Protection Regulation. This is a big responsibility. **European SMEs look to the EU for the benefits of one set of rules across our continent, ensuring their on-going investments in European jobs and innovation.** To make sure EU SMEs do not get hurt in the process of modernising DP rules, here are a few suggested positions you may want to take – come the 2014 elections, SMEs will be grateful.

Exempt non-data driven EU SMEs from disproportionate documentation requirements.

The EC proposal holds size-based exemption. A more relevant, desirable and feasible approach would be a risk-based exemption. Let mainstream 'brick and mortar' SMEs focus on job-creation, rather than overburdening them with unnecessary and costly extra requirements.

Exempt EU SMEs from DPIAs that add no proven value but are costly and burdensome.

There is no tangible evidence that DPIAs (data protection impact assessments) add value, but we *do* know that they are a costly and burdensome exercise – especially for SMEs. For a truly risk-based approach, SMEs that process data as an ancillary activity, or not at all, should be exempted from this DPIA obligation.

Ensure EU SMEs spend money on workers that create value, not on Data Protection Officers.

For on- and offline SMEs, every day since the crisis hit is a struggle to survive and pay wages. How can we ask them to spend what they cannot afford? The EC's impact assessment estimates the average annual cost of a DP Officer at EUR 80 000. Even if outsourced, these would be valuable resources that should be spent on real worker wages.

Do not punish EU SMEs for failing to understand complex legislation, but help them and give warnings before imposing fines.

When the new DP rules come into force, there is a fair chance that most SMEs will not be immediately aware of how to apply them. Authorities should provide SMEs with clear and simple checklists for compliance.

Keep the Access Request Fee!

The costs for a business of responding to an Access Request are estimated at €60-€120. The current Directive allows Member States to instate a fee for each access request, thereby preventing frivolous requests. This option should be maintained under the new Data Protection Regulation: support amendment 1146.

There are more than 19 million SMEs in Europe. Many at present do business online. Many others want to use the internet to take advantage of the benefits of the Single Market. In 2013, you can make sure EU SMEs are not afraid to do business online or handle data.

Data Protection: reform for SMEs, not at their expense

On the data subject's consent (article 4 - paragraph 1 – point 8):
The definition of consent needs to take into account the practicalities of the interaction between individuals and business. Consent should be defined as freely given specific, informed or unambiguous indication of the wishes by which the data subject signifies agreement to personal data relating to them being processed.

On principles relating to data processing (article 5):
ESBA recognises the potential to include a more elaborate set of principles in this article, in particular in order to be able to base any further regulatory requirements on these principles. A suggested threshold of 5000 data subjects is however still very low. We think, any number of data subjects does not make a distinction between ancillary activity vs. core activity or high vs. low risk.

On the lawfulness of processing (article 6 – paragraph 1 – point e/f):
In cases where there is no direct contact between the data subject and the SME, it should be explicitly clear that lawful processing follows from a task necessary to be carried out by a third party. Furthermore, lawful processing should be established when data are collected from public registers lists or documents accessible by everyone or when necessary to ensure the legitimate interests of third parties.

On conditions for consent (article 7 – paragraph 4):
The wording "significant imbalance" between the position of the data subject and the controller is too broad and even misleading. It may be assumed that in various business relationships there may be a "significant imbalance" from a legal point of view (i.e. client/lawyer or patient/physician). In these cases, consent should no longer be the basis for legal processing of data. For purposes of legal certainty, paragraph 4 should be deleted.

On procedures and mechanisms for exercising the rights of the data subject (article 12):
Procedures and mechanisms for providing information lead to overregulation. Information to the data subject by the controller should be provided without undue delay by means of any medium. In order to protect SMEs from 'manifestly excessive data requests' – something that could be used against SMEs for competitive reasons – SMEs should be allowed to charge a fee for information requests.

On documentation requirements (article 28):
Documentation requirements as such do not ensure any safeguards in mitigating risks related to the processing of data. Instead they pose a heavy burden on SMEs. The responsibility of safeguarding data should be established by means of principles on processing. It should be left to the individual businesses how they establish appropriate procedures to implement these principles.

On data protection impact assessments (article 33):
Data protection impact assessments (DPIA's) are very heavy regulatory measures. According to the European Commission's own impact assessment the costs for a DPIA are estimated at € 14 000[1]. DPIA's should only be required when data is processed as a core activity of a business. Moreover, as most business fail within their first three years, a business should only be required to perform a DPIA after the first three years of incorporation.

On data protection officers (article 35):
Data Protection Officers (DPO's) pose a disproportionate burden on SMEs. According to the European Commission's own impact assessment, the costs of a DPO are estimated at € 80 000[2]. Any mandatory appointment of a DPO should incorporate the Risk Based Approach and only be required if an SME processes data as a core activity. In cases that a DPO is appointed, other regulatory requirements should be lowered.

On sanctions (article 79):
SMEs that process data only as an ancillary activity may make initial unintended compliance errors, because their resources are scarce. For this reason, a "three strikes, you're out" rule (i.e. administrative sanctions are not imposed until the third case of non-compliance) is a more proportionate way to ensure SMEs' compliance with the Regulation.

[1] Commission Impact Assessment accompanying the proposals for a Regulation and for a Directive. SEC (2012) 72, p. 70. http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf
[2] Commission Impact Assessment accompanying the proposals for a Regulation and for a Directive. SEC (2012) 72, p. 110. http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

Proposal for a Regulation
Article 28 – paragraph 4

Text proposed by the Commission	*Text proposed by the rapporteur (AM 189, 190)*	*Amendment*
4. The obligations referred to in paragraphs 1 and 2 shall not apply to ***the following controllers and processors:***	4. The obligations referred to in paragraphs 1 and 2 shall not apply to a natural person processing personal data without a commercial interest***.***	[retain text proposed by the Commission]
(a) a natural person processing personal data without a commercial interest***; or***		
(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	***(deleted)***	

Justification

Unless a risk-based exemption solution is in place (e.g. suggested article 33), the original Commission proposal is the best alternative. As the Commission proposes, SMEs[1] ***that do not process data as their core activity*** *should be allowed to focus on innovation and job creation instead of wasting resources on burdensome and unnecessary documentation obligations. Therefore, amendments 189 and 190 should be rejected in order to retain the SME exemption in Article 28(4)(b).*

[1] "The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million." Commission Recommendation 2003/361/EC, Annex, Article 1.
< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF >

Proposal for a Regulation
Article 33 – paragraph 4a (new)

Text proposed by the Commission	*Text proposed by the rapporteur*	*Amendment*
		4a. The obligations referred to in paragraphs 1 to 4 shall not apply to:
		(a) an SME that processes data only as an activity ancillary to its main activities;
		(b) an SME that processes data as its core activity, for the first three years after the SME was founded.

Justification

The "risk-based approach" to data protection reform[2] should also be extended to the obligation to carry out a Data Protection Impact Assessment (DPIA). The Commission's impact assessment for the reform package calculates the cost of even a small-scale DPIA at EUR 14 000.[3] For SMEs that only process data as an activity ancillary to their main activities, such a cost is highly disproportionate and they should therefore be exempted. Most SMEs fail within their first three years of business, due to cost of business, lack of access to finance and administrative and regulatory burden. Even for SMEs that process data as their core activity, the cost of a mandatory DPIA will prove to be prohibitive for many companies during these crucial and highly vulnerable start-up years, which would stifle innovation and growth. For this reason, the exemption should be extended to all SMEs during the first three years after they are founded. Safeguards against the "specific risks" mentioned in Article 33(1) are provided by Article 30 on the security of processing.

[2] Speech by Viviane Reding, Vice-President of the European Comission and EU Justice Commissioner: 'The overhaul of EU rules on data protection: making the single market work for business', 3rd Annual European Data Protection and Privacy Conference, Brussels, 4 December 2012.
< http://europa.eu/rapid/press-release_SPEECH-12-897_en.htm >

[3] Commission Staff Working Paper: Impact Assessment [accompanying the proposals for a Regulation and for a Directive]. SEC(2012)72, p. 70.
< http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf >

Proposal for a Regulation
Article 35 – paragraph 1

Text proposed by the Commission	*Text proposed by the rapporteur (AM 223, 224, 225)*	*Amendment*
1. The controller and the processor shall designate a data protection officer in any case where:	1. The controller and the processor shall designate a data protection officer in any case where:	1. The controller and the processor shall designate a data protection officer ***only*** where:
(a) the processing is carried out by a public authority or body; or	(a) the processing is carried out by a public authority or body; or	(a) the processing is carried out by a public authority or body; or
(b) the processing is carried out by ***an enterprise employing 250 persons or more; or***	(b) the processing is carried out by ***a legal person and relates to more than 500 data subjects per year.***	(b) the processing is carried out by an enterprise employing 250 persons or more; or
(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.	(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring ***or profiling*** of data subjects.	(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.
	(ca) the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1).	

Justification

The Commission's impact assessment calculates the average annual cost of a full-time data protection officer (DPO) at EUR 80 000.[4] Even if SMEs would not need a full-time DPO, and even if the DPO could be shared among multiple SMEs, the compliance costs are simply too high for the average small company. The Commission has acknowledged this fact in its proposal, but the lead rapporteur's amendment replacing the SME exemption with the arbitrary threshold of 500 data subjects would result in significant burdens for many SMEs, even for those companies where the processing is ancillary to their main activities. The threshold of 500 data subjects is not based on any research or impact assessment – contrary to the principle of evidence-based policy-making. For these reasons, the exemption for SMEs that do not process data as their core activity should be retained and underlined.

Proposal for a Regulation
Article 52 – paragraph 1 – point k (new)

Text proposed by the Commission	*Text proposed by the rapporteur*	*Amendment*
		1. The supervisory authority shall:
		(k) provide SME processors and controllers with a comprehensive list of their responsibilities and obligations in accordance with this Regulation;

Justification

A solid information strategy is key to the implementation phase of EU legislation. While the new Regulation's unified rules for the entire EU would provide welcome clarification, SMEs do not have the resources to familiarise themselves with all the relevant provisions of the new legislation. In order to prevent unintentional non-compliance, each national Data Protection Authority (DPA) should, in its role of one-stop shop for data protection issues, provide compliance checklists to all relevant companies and organisations.

[4] Commission Staff Working Paper: Impact Assessment [accompanying the proposals for a Regulation and for a Directive]. SEC(2012)72, p. 110.
< http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf >

Proposal for a Regulation
Article 79 – paragraph 3

Text proposed by the Commission	*Text proposed by the rapporteur*	*Amendment*
3. In case of a first and non-intentional ***non-compliance*** with this Regulation, a warning in writing may be given and no sanction imposed***, where:***	3. In case of a first and non-intentional ***breach of*** this Regulation, a warning in writing may be given and no sanction imposed.	3. In ***the first two cases of*** non-intentional non-compliance with this Regulation, a warning in writing ***shall*** be given and no sanction imposed, where:
(a) a natural person is processing personal data without a commercial interest; or		(a) a natural person is processing personal data without a commercial interest; or
(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.		(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.

Justification

Whereas large companies and even smaller data-driven companies should be able to allocate the necessary resources to ensure compliance with this Regulation, SMEs that process data only as an ancillary activity may make initial unintended compliance errors, because their resources are scarce. For this reason, a "three strikes, you're out" rule (i.e. administrative sanctions are not imposed until the third case of non-compliance) is a more proportionate way to ensure SMEs' compliance with the Regulation.

The European Small Business Alliance (ESBA) is a non-party political European group, which cares for small business entrepreneurs and the self-employed and represents them through targeted EU advocacy activities. Through its direct membership, associate membership and cooperation agreements, ESBA today represents more than one million small businesses and covers 36 European countries.

CEA-PME is an ideologically neutral and non-party confederation of national business organisations. It represents the interests of small and medium-sized enterprises of all branches and professional groups towards the European institutions and aims at giving SMEs a voice commensurate to their importance for the European economy.

The Federation of Small Businesses (FSB) is the UK's leading business organisation. It exists to protect and promote the interests of the self-employed and all those who run their own business. The FSB is non-party-political and, with around 200,000 members, it is also the largest organisation representing small and medium-sized businesses in the UK.

The Association for Competitive Technology (ACT) is an international grassroots advocacy and education organisation representing more than 5 000 small and mid-size app developers and information technology firms. ACT is also a part of the Industry Coalition on Data Protection; this document should be seen as complementary to, not *in lieu* of, positions ACT supports through the ICDP.