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. Furthermore, a 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 with the data subject by 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 procedures and mechanisms for exercising the rights of the data subject (article 12):
Procedures and mechanisms for providing information can easily 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 proportionate to the costs incurred for providing information.

On documentation requirements (article 28):
Documentations 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 an unrealistic burden on SMEs. According to the European Commission's own impact assessment the costs for a DPO are estimated at € 80 000[2]. DPO's as such do not pose any safeguards in mitigating risks related to the processing of data. SMEs should be given – on the basis of the Risk-Based-Approach – the responsibility to ensure themselves the safety of their data processing. On an optional and voluntary basis, SMEs should nevertheless have the freedom to seek external advice, or to appoint a DPO. In those cases, 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

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.