Hotrec Hospitality Europe

UEAPME

POSITION PAPER

27 July 2016

HOTREC and UEAPME joint position on the proposal for a Data Protection Regulation Trilogues Phase

HOTREC and UEAPME paid close attention to the approval of the Council general approach on the General Data Protection Regulation, at the Justice and Home Affairs Council of 15th June 2015.

HOTREC and UEAPME have also followed very closely the approval by the European Parliament of the plenary vote on the General Data Protection Regulation (12 March 2014).

Ahead of the trilogue negotiations starting on 24th June 2015 between the European Commission, the European Parliament and the Council of the EU on the topic, both organisations hereby highlight their priorities by embracing the decisions most favourable to SMEs and which have been decided by each one of the Institutions or proposed by the Commission.

Overall, HOTREC and UEAPME fully welcome the need to enhance the level of personal data protection for individuals and to increase business opportunities in the Digital Single Market. This is essential to stimulate economic growth, ensure employment and foster innovation. But both associations have comments on the following chapters:

- **Controller and Processor (chapter IV)**
- **Data protection principles (chapter II)**

1 - Controller and Processor (Chapter IV)

1 - Data Protection Officer

Option 1 – preferred option

The Council defends that the designation of a Data Protection Officer (DPO) shall not be compulsory for companies, except in cases where it is required by Union or Member State Law (art. 35/1).

The DPO is an example of a clear additional financial and administrative extra requirement that

would be asked to SMEs to comply with and require disproportionate costs
HOTREC and UEAPME fully welcome this balanced position of the Council.

Arguments:

- The **DPO should be compulsory only if the companies' core business is data processing** (this argument goes in line with the Commission position: art. 35/1 b and c);
- If a DPO is contracted only for some hours a year, the cost that such a figure would imply, would have a direct impact on SMEs. UEAPME and HOTREC would like to highlight the following estimates:
    - According to information provided by TÜV (Technical Supervisory Association) in Germany, the cost of an external DPO for SMEs could come to about 12.000 EUR in the first year (= 150 EUR per working hour, 10 working days needed per year, 8 hours per working day).
    - According to the impact assessment done by the European Commission an external consultant would be paid on average €250 per hour to develop and to implement his/her work[1];
    - The UK Ministry of Justice's impact assessment regarding the EU Data Protection Regulation proposal estimates that a DPO could cost anywhere between £30–£180 million per annum (in 2012–13 earnings terms) depending on the contractual hours of the DPO[2].

- If the company delegates the DPO tasks to an internal employee, the company would be facing an extra burdening, as this employee would need to learn the tasks performed by a DPO. And, it is important to insist that if a companies' core business is not data processing, there is no need for the company to have a DPO, especially if the company is an SME (Commission proposal – art. 35/1 b and c).
- In one person companies, which represent 50% of all enterprises in the EU, the task of DPO has to be taken up by the owner manager which work on average already more than 60 hours a week.

- HOTREC and UEAPME would encourage both Council and Parliament to work upon the text of the Regulation in order for companies to be able to well apply the legislation without the need of the DPO. Any piece of EU legislation should be clear, so that is **well understood by citizens.**

- **A DPO as such is not at all a guarantee for an effective data protection.**

Option 2

If option 1 does not find an agreement between Council and Parliament, than UEAPME and HOTREC

[1] Page 117, Annex 6 of the Impact Assessment on the Commission proposal on a General Data Protection Regulation SEC (2012) 72 final.
[2] UK Minister of Justice impact assessment.

would propose that both Institutions embrace the proposal presented by the Commission (art.35/1 a and b) which defended that companies employing less than 250 people were exempted from the obligation of designating a DPO, **as long as their core activities do not consist of data processing operations.**

Both associations consider that this approach takes into account SMEs concerns. A small hotel, whose core activity is to provide accommodation (and not data processing), should not have the additional burden of paying to a DPO. This approach aliens with the Commission willingness of rendering SMEs more competitive and of avoiding additional red tape.

2 – Risk Based Approach

Option 1 – preferred option

Overall, HOTREC and UEAPME fully welcome the **new risk-based approach** approved by the Council. Indeed this approach will decrease drastically the administrative and economic burdens that affect SMEs and the hospitality sector. At the same time, the Council's approach protects the rights and freedom of the data subjects in all circumstances of data processing. Consequently, the Council's approach is balanced and coherent.

In particular, UEAPME and HOTREC welcome the following outcome of the Council's approach:

- The controller should be compelled to implement appropriate measures and be able to demonstrate the compliance of processing activities with the Regulation. These measures should take into account the nature, scope, context and purpose of the processing and the risk for the rights and freedom of individuals (recital 60 and article 22);
- The likelihood of the risk should be determined in function of the nature, scope, context and purpose of the data processing. Risk should be evaluated by an objective assessment, based on whether data processing operations involve a high risk (recital 60b);
- High risk is a particular risk of prejudice of the rights and freedoms of individuals (recital 60b);
- Examples of high risk include cases where processing could give rise to discrimination, identity theft or fraud; financial loss, damage to the reputation or other social or economic disadvantage (recital 60b in conjunction with articles 28/4/b; article 31/1; article 32/1, article 33);
- Guidance for the implementation of appropriate measures, especially with regard to the identification of the risk, could be provided by codes of conduct, guidelines of the European Data Protection Board or by indications provided by the data protection officer (recital 60c and article 38);

In any case, data subjects are assured legal redressed:

- Every data subject shall have the right to lodge a complaint with a single supervisory authority (…) if the he/she considers that the processing of personal data relating to him

or her does not comply with the Regulation (art. 73/1);

- Moreover, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them (art. 74); or against a controller or a processor (art. 75).

Therefore, **only when processing operations represent a high risk**, the following activities should be developed by the controller:

- Communicate the personal data breach to the supervisory authority (recitals 67; 68; 68/a; 69 and article 31 and 32);
- Carry out an impact assessment (recital 66a; 70a; 71; 74 and articles 33);
- Consult the supervisory authority prior to the processing of personal data, where a data protection impact assessment, as provided for in Article 33, indicates that the processing would result in a high risk in the absence of measures to be taken by the controller to mitigate the risk (recitals 66a in conjunction with article 34).

Proposal for a compromise text on the definition of high

Council's General approach – recital 60b	HOTREC and UEAPME proposal of amendment
"(…) A high risk is a particular risk of prejudice of the rights and freedoms of the data subjects.	"(…) A high risk is a particular risk of prejudice of the rights and freedoms of the data subjects. **High risk applies to companies' when their core business is data processing**".

Justification

In order for companies to better access weather their activities imply high risk or not, some more detail could be given to the definition. Only if a companies' core business is data processing, then there are sufficient grounds that justify the connotation of "high risk" attributed to a company. This goes in line with the Commission proposal (art.35/1 a and b). For instance, a small craft shop deals with credit card data processing on a daily basis. But as its core business is not data processing, it should not imply high risk.

The same amendment should be included in all the articles that touch upon high risk (e.g.: articles 31, 32, 33, 34).

Option 2

HOTREC and UEAPME would also welcome the Commission proposal with regard to the communication of the data breach (art.32) – as long as the deadline of "undue delay" proposed by the Parliament and estimated to take place within 72 hours would be adopted. We believe that this proposal would be sufficient to allocate both consumers and businesses interests.

UEAPME and HOTREC could as well support the development of an impact assessment (art.33) as proposed by the Commission, as in this case, the nature, scope and purposes of the data being processed are taken into account.

HOTREC and UEAPME's position on the threshold of 5000 Data Subjects – Parliament's approach

Above all, **HOTREC and UEAPME strongly disagree with the idea that the threshold of 5,000 data subjects, for which no impact assessment has been developed, should be the reference that obliges a company to follow or not certain obligations foreseen in the proposed Regulation,** according to the Parliament approach, namely:

- Designation of a DPO (art.35);
- Presumption that the company is likely to present specific risks (art. 32/a/2/a)
- Obligation of developing an impact assessment (art.33)

A one-size-fit all approach shall not be applied on a general basis. Instead, a case by case risk analysis should be developed in order to access the risk. HOTREC and UEAPME insist that the nature, scope, purpose of the activities developed by the companies should be criteria to judge whether there is a risk when processing data.

In fact:

- **No justification has been provided with regard to the chosen threshold**. Even though both associations have called for the European Parliament to **develop an impact assessment, no study has been put forward**; Because of the high importance and long lasting impacts of the future legislation of data protection for SMEs these aspects must be given the necessary attention.
- The threshold is still clearly too low, as the vast majority of SMEs, including micro-enterprises, already process data related to more than 5,000 data subjects a year. In fact, **with an occupancy rate of 55%, any small hotel with only 25 rooms would fall under this category**;
- It is difficult for a company to anticipate the number of clients whose data will be processed per year. In any case, an estimation by the SMEs representatives could as well not be provided without an impact assessment.

For these reasons, UEAPME and HOTREC consider the threshold of **5,000 data subjects' critical value as unnecessary burdensome (in economic and administrative terms)** and, therefore, **disproportionate**.

Data Protection Principles (Chapter II)

1 – Lawfulness of processing

HOTREC and UEAPME welcome that, provided that the interests or the fundamental rights and freedoms of the data subjects are not overriding, the **processing of personal data for the purpose of direct marketing** for own or similar services should be presumed as carried out for the legitimate interest of the controller. In this way, former clients could be contacted by the hospitality businesses for marketing purposes (e.g.: promotions, newsletters, client loyalty programmes, etc.), without

needing to receive an explicit consent by former clients.

In this sense both associations welcome one of the following options:

- The Council's approach (recitals 38, 39, 57 in conjunction with articles 6/1/f , 19/2; 79a/2/de; **or**
- The European Parliament's approach (recital 39b in conjunction with art. 6/1/f)

2 – Deletion of the right to data portability

The possibility for the data subject to obtain from the controller a copy of data undergoing processing in an electronic and structured format, where personal data are processed by electronic means, would bring costs to entrepreneurs. In fact, the electronic systems of companies would probably need to be upgraded to produce electronic forms for the data subjects so that the electronic data could be transferred.

UEAPME and HOTREC would like that **only companies whose core business is data processing would be obliged to deal with the right to data portability.**

Brussels, 18 June 2015

CONTACTS:

HOTREC: Marta Machado; marta.machado@hotrec.eu; 0032 (0) 2 513 63 23
UEAPME: Luc Hendrickx; l.hendrickx@ueapme.com; 0032 (0) 2 230 75 99

*

* *