34.

sopra steria

JUST-ARTICLE29WP-SEC@ec.europa.eu
presidenceg29@cnil.fr

DG Justice and Consumers

Oslo, 31. January 2017

Subject: **Guidelines from the Article 29 Group – Data Protection Regulation (GDPR)**

Dear Sir or Madam,

Sopra Steria is a global company that is present in more than 20 countries. Sopra Steria is a European leader in digital transformation, and provides end-to-end service offerings on the market: consulting, systems integration, software development, infrastructure management and business process services.

Our services include giving advice regarding privacy and information security, including on the new General Data Protection Regulation (GDPR). We are therefore following the advice published by the Article 29 group closely, to make sure we are able to help our clients be compliant with the new regulation from 2018.

From our Scandinavian branch, we have read and discussed your three statements regarding DPOs, data portability and identifying a controller or processor`s lead supervisory authority, and have a few questions/comments we hope you can elaborate on in future guidelines.

Guidelines on Data Protection Officers (DPOs)

In Norway, it`s already common practice for bigger companies and public agencies to have a DPO. In your statement, you especially emphasise the necessity for the DPO to be competent and impartial. We would, however, like to get your input on whether the DPO would be impartial and able to perform his/hers duty if the role as DPO is held by the same person as Chief Information Security Officer (CISO). We see both advantages and disadvantages if these two roles are kept by the same person:

- In many smaller companies, the current competent person that could perform the task of a DPO might be the CISO. Many smaller companies might not have the resources to employ different persons in these two roles, even if the tasks are performed on a part-time basis.
- The CISO is in charge of performing risk assessments and making sure the results are followed up on. Sometimes, it would be best from a security perspective to introduce new measures that would be invasive from a privacy perspective, security monitoring of employee activities online being one such example. If these two roles are kept by the same person, this can create a conflict of interest.

Sopra Steria AS
Biskop Gunnerus' gate 14A - P O Box 2 - N-0051 OSLO - Norway
Registered Number: 910 909 088

- Some of our clients combine these two roles today. This may sometimes lead to more informed decisions, since both aspects are then duly taken into account and given the same importance. But this would of course vary depending on the person holding the positions.

In your written opinion, you discuss the possibility of the DPO being external and not an employee. We believe that appointing a DPO not under employment of the Controller or Processor could reduce the DPO's ability to perform its tasks, as it is expected that the DPO performs tasks on its own discretion. Having an external entity issuing claims for activities performed not directly ordered by the Controller or the Processor might be a source of conflict e.g. because of the economic incentive for the DPO, reducing the DPO's ability to perform its tasks. This is an aspect that could have been raised in your opinion. On the other hand, an external DPO would always remain objective, and also using a professional DPO could be a good alternative particularly for smaller companies, giving them access to competencies they cannot maintain within their own organisation.

We in Sopra Steria Scandinavia would like to hear your opinion on these two issues in the future.

Guidelines on the right to Data Portability

We are positive towards the right to data portability for the data subject. However, we see that this right will create uncertainties as to what constitutes a "structured, commonly used and machine-readable format", see GDPR article 20 (1). Today, we work with a lot of clients on data transfer, and we see that data transfer can be challenging to do in practice. We therefore support your statement regarding the need for more interoperable standards and formats, and would like to see more work on this in the future.

After reading your opinion, we believe there is still a need for clarification on the obligation to hand over information on the best possible level of granularity. This can end up exposing trade secrets, and we therefore believe that the balance between the right to protect trade secrets and the right to data portability needs to be clarified.

With regards to ensuring information security while processing requests for data portability, we recommend issuing advice on implementing authentication procedures even if no such mechanism is in place for the normal consumption of the service. We consider the potential risks related to confidentiality, availability and identity theft to be higher when requesting a large volume of structured data to be exported compared to the normal use of data while consuming the services.

Best regards,

On behalf of Sopra Steria Scandinavia,