20.

Ref. Ares(2017)2518464 - 17/05/2017

BUSINESSEUROPE [redacted]

ANNEX

1. Guidelines on the right to data portability

- *Intention of Article 20 of the GDPR*

Data subjects are offered a new right of data portability within the GDPR to strengthen the control they have over their data and avoid digital lock-in. The original intention was to enable this right on the basis of a request from a subject. The draft Guidelines should be strengthened in this regard to reflect this intention. They should clearly state that the subject must have a legitimate interest in when making that request. Only data that is provided to the controller by the subject is covered under this right. That includes data controlled and accessed by the subject during the performance of the contract but not data automatically generated by the service offered during that performance.

The right to portability is designed to enable people to switch services with greater ease. However, not all information provided to one service is relevant to another. The draft Guidelines should clarify the ability of determining this choice. Controllers should be able to offer people technical means of selecting which information they want to transfer to another controller rather than offering an all or nothing solution. Receiving businesses may decide to not process all data they receive via a transfer from another controller (e.g. the information is not relevant in the consumer request to switch services).

The draft Guidelines should also state specifically that the right to portability only exists when the subject has a legitimate interest in transferring it to another controller (eg. this would not concern employees' personal data (except application documents) as no legitimate interest to transfer data collected within the employment relationship). This would not only violate confidentiality interests under Article 20(4) but would be unpractical as human resources data is processed in a format unreadable by subjects.

The draft Guidelines should not widen the intention of this right to allow subjects' access to manage and reuse personal data. The current draft Guidelines should not include data which the subject never possessed or was aware of in order to fulfil the condition of data "provided by" the data subject. Including this data as personal data and therefore including them in the portability request would require controllers to port observed data that was machine generated with little user interaction or generated during the provision of a service. Just as inferred or derived data, observed data is proprietary and should be out of the scope. Widening the scope to observed data (eg. when controlling movements of employees or monitoring behaviour of website users) is too wide and is not in line with the GDPR. Including it would create legal uncertainty in practice. It could also incentivise reliance on alternative legal bases to process it.

Further to this, taking an overly broad interpretation could also force sharing commercially sensitive data with competitors. The draft Guidelines should explicitly state that the right to data portability is narrower than the right to access, and subjects may not need or want to port all data available to them. It would be useful for the guidelines to further clarify that Article 20(4) should be interpreted in conjunction with recital 63, and therefore the data portability right should not adversely affect the

controllers' rights, (e.g. confidentiality, IP). The controller should only be requested to transfer data directly provided by the subject not impacted by these concerns.

Portability should be read as excluding data that is passively collected from users. It will also be technically impractical as most service providers do not have a separate database containing only raw data that can be separated easily from data generated by a service provider (e.g. algorithms).

It is also worth realising that some national laws include portability rights for observed data also ensure that it is accessible online. Whereas data that is not accessible to users in the context of the original service should not be considered eligible. Therefore, the draft Guidelines should only include observed data that is accessible to users online where subjects have asked for its transfer. It should not include personal data of third subjects.

- *Controllership*

It will be difficult for a receiving controller to ensure data in practice is relevant and not excessive with regard to new processing requests. The draft Guidelines create additional burdens which will place unacceptable legal risks on receiving controllers in practice. Often, these controllers are not legally allowed to have knowledge of the data subject via the service they offer. Also, beginning to analyse data for this purpose would mean saving it. If this processing takes place without consent of the data subject that inspection of data is already non-compliant. In order to ensure legal certainty for the receiving controller without creating additional requirements, the draft Guidelines should state clearly that the subject is responsible for the lawfulness of processing third party data provided on their behalf to the receiving controller. This being said, determining which data is not relevant for processing will still be complicated in practice.

The draft Guidelines should also stipulate that the data provided by the subject is communicated by the controller in its existing state without further need for verification or updates. Consequentially, the controller who transmits data of the subject cannot be held liable by receiving controllers. The receiving controller should also not need to identify lawfulness of processing of third party data (e.g. a legitimate interest when the household exception applies). The draft Guidelines should ensure the receiving controller is not burdened with this requirement when it was not required by the original controller.

Article 20 does not determine methods by which controllers must provide or receive data. It leaves it to controllers to determine the means that are most suitable for their specific services. But the draft Guidelines suggest that all controllers should implement tools to enable subjects to select the relevant data and exclude (where relevant) other subjects' data. Additionally, they should implement consent mechanisms for other data subjects involved to ease transmission when parties give consent. These practices need to be determined by the market. Companies should be free to build their own mechanisms to benefit their users and to achieve a competitive advantage. Many companies already provide tools to select and exclude their data or other subjects' data from being ported to other services. But this should not be forced.

- *Data portability tools*

Controllers will offer a direct download opportunity to transmit subjects' data to another controller. But the Guidelines should not prescribe that method of data portability. The draft Guidelines currently note the use of an API (application programming interface) but this limits other tools that could be used to transfer data through electronic means. It must remain the discretion of the controller to determine the means of transfer. At the same time, referring solely to the licensing constraints of alternative methods disregards the costs data controllers incur when attempting to agree on an interoperable format .

The draft Guidelines also present the best practice of controllers offering recommendations on which formats or encryption measures could be used to enable the subject to secure data storage. This should in no way place responsibility of this nature on the controller in practice.

- *Security*

Rather than solely focussing on the timing of fulfilling portability requests, the draft Guidelines should also focus on the security of transfers. Data portability features pose significant security concerns as temporary unauthorised access to an account can be leveraged to permanently copy information. Companies need the ability to offer protection to control the subjects' ability of disabling portability features and delay fulfilment of requests in order to authenticate the subject invoking the right. Companies should retain a margin of manoeuvre to determine the circumstances in which they need to authenticate users, based on a reasonableness standard. The Guidelines should acknowledge that strict security measures are necessary and not obstructive in nature. These measures should include the ability to disable portability mechanisms or delay the provision of data upon a portability request if there are valid reasons to believe an account might be compromised in order to verify the identity of the subject making that request.

Controllers are risking great financial and administrative burdens as they are obliged (not the subject) to make a wholly secure data transfer, particularly as they cannot remain fully protected against all potential trade secret or copyright abuses.

2. Guidelines on Data Protection Officers (DPOs)

- *Designation*

A legal person can only be appointed as a DPO when conditions below are met and specified in the corresponding service contract:

- the tasks of the DPO are carried out by a DPO team
- a clear allocation of tasks within the DPO team is defined
- each individual member of the DPO team fulfils all relevant requirements of the GDPR
- a single individual is assigned as a lead contact and person in charge for each client
- thorough knowledge of the actual business sector the controller is operating in

While the draft Guidelines specify that the requirements of external DPOs can be assigned to several individuals working in a team we believe that for legal certainty and practical application, the draft Guidelines should also state that this ability also applies to internal DPOs. Particularly as it may not always be possible in practice to locate one individual fulfils all the skills required.

The draft Guidelines imply significant financial and organisational requirements in order for a fully functioning DPO to comply with the GDPR. But it will be very complicated to engage more than one DPO in one organisation due to the lack of appropriate persons on the market. This number of skilled people is limited further due to the application of rules regarding possible conflict of interests. Ensuring wide ranging DPO independence creates a new position of an upper-employee. The draft Guidelines even doubt whether it is possible to terminate an internal contract with a DPO (e.g. for inappropriate working results).

With regard to the need for a DPO if the core activities of the controller and processor consist of systematic and regular monitoring of subjects, Article 37 of the GDPR should not be interpreted in such a wide-reaching manner to cover instances where the data processing is not a core activity. We do not regard the current example of a hospital processing patients' data as its core activity. Instead the core activity should be defined as the main element and objective of the controller or processor. In this case it would in fact to provide health care – not process data.

Article 38 of the GDPR permits DPOs to fulfil other tasks and duties other than those relating to their position as the DPO if they do not result in a conflict of interest. While this can only be determined on a case by case basis, following current draft Guidelines would apply this provision too broadly as it would include tasks the DPO has to carry out such as informing and advising controllers or processors of their obligations (Article 39(a)). We believe that a conflict of interest cannot arise just because the DPO was carrying out its core duties to fulfil the GDPR. Practically, it may also be difficult at some organisations to appoint a knowledgeable DPO that is completely free of financial, marketing, medical, executive, human resources or IT links to the organisation. Whereas the accumulation of activities to designate an in-house DPO would be desirable particularly for SMEs.

The draft Guidelines correctly explain that establishing a DPO among a group of undertakings may take place electronically rather than physically. This should also refer to the possibility of establishing a DPO in various regions to execute tasks over a whole group of undertakings as it shall be practically impossible for a DPO to be designated in several establishments throughout a group of undertakings across various regions that is available for each subject or authority in every language. Further explication concerning the accessibility and language of the DPO is needed. Particularly as the draft Guidelines go further than the GDPR placing greater duties on controllers and processors stating that the DPO has to be accessible via hot-lines, dedicated contact forms or addressed through the organisation's website.

- *Tasks*

The DPO should report to the highest management level. Yet the draft Guidelines are ambiguous about what level that is. Clarification is needed so that the reporting requirements can be met with legal certainty. The tasks of the DPO should be made

clearer in the draft Guidelines on the whole, particularly as Article 39(1)(b) is ambiguous. For example, existing national laws include training as a core DPO task yet the draft Guidelines are silent on these examples.

Elaboration on when the controller should seek advice from the DPO is needed within the draft Guidelines. In some circumstances, a DPO may be best placed to not only give advice on a data protection impact assessment (DPIA) but even conduct it on behalf of the controller. Particularly when extra costs are posed by carrying out a DPIA externally or internally through another source.

It is highly welcome that the draft Guidance enables DPOs to prioritise activities and focus efforts on issues presenting higher data protection risks. But the approach reached in Article 39(2) of the GDPR still remains unclear. Instead of relying upon what is ideal and secure in terms of risk to prioritise work, DPOs will also have to conduct an assessment based on the nature, scope, content and purpose of the respective processing.

Further information is needed in the draft Guidelines to clearly describe what the creation and holding the registers by enterprises will mean in practice. What administrative and financial requirements will this represent and how should this be achieved in practice?

3. Identifying a Controller or Processor's Lead Supervisory Authority

- *Borderline cases*

The draft Guidelines exceed the GDPR's scope by presuming that a decision on a borderline case cannot be made solely based on statements by the organisation under review. Yet as the burden of proof is placed on controllers and processors, they should make an objective assessment of the facts and determine their main establishment. This assertion can be rebutted. Supervisory authorities should only rebut upon an objective examination of these relevant facts.

- *Supervisory authority concerned*

The GDPR only provides for limited cooperation with respect to lead and supervisory authorities reaching mutually acceptable decisions on procedural matters. This cooperation applies when a lead supervisory authority and the other supervisory authorities concerned agree to dismiss or reject parts of a complaint and act on other parts of that complaint. This does not include decisions about issuing a warning or press statement. But when a procedural decision is made to dismiss or reject parts of the complaint that decision should prevail.

* * *