January 17, 2019

The European Data Protection Board
Rue Montoyer 30,
B-1000 Brussels

RE: Comments for EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)

Dear Members of the European Data Protection Board,

On behalf of the National Association of Professional Background Screeners (NAPBS), whose members include companies around the globe, we write to you to with our comments regarding the current EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). As a nonprofit organization with chapters in the United States, Europe, Canada and APAC and consisting of over 900 small and large background companies engaged in the background screening profession, NAPBS has been dedicated to providing the public with safe places to live and work since 2003. The NAPBS member companies conduct millions of employment-related background checks each year, helping employers, staffing agencies, and nonprofit organizations make more informed decisions regarding the suitability of potential employees, contractors and volunteers.

We thank you for this opportunity, and would offer the following for your consideration:

- Comment 1: Where a Controller or Processor has no establishment in the EU per 3(1), and is not covered under the targeting criterion set forth in 3(2), but the Controller or Processor accesses an internet-based portal hosted in the EU by a Processor established in the EU, is it a correct interpretation that the only obligations to the non-EU based Controller or Processor would be contractually imposed by the EU-based Processor?
    - Example: A US-based background screening company uses a EU-based subprocessor to conduct checks such as verification of employment or education, criminal record checks, etc. The US-based screening company has no establishment in the EU. The US-based screening company logs on to a web portal of a EU-based screening company hosted in the EU. It is expected that the EU-based processor would need to implement appropriate safeguards for transfer of data to the US-based screening company. Would the accessing of the web portal in any way be considered to be processing in the EU by the US company such that the US company would be directly subject to the GDPR?
- Comment 2: Where a Controller or Processor has no establishment in the EU per 3(1), and is not covered under the targeting criterion set forth in 3(2), but the Controller or Processor contacts sources in the EU directly, such as employers and universities, is it a correct interpretation that the only obligations to the non-EU based Controller or Processor would be contractually imposed by the EU-based Processor?
    - Example: A US-based background screening company has no establishment in the EU. The US-based screening company conducts searches such as verification of education, employment and reference checks where the source of the information, e.g., the employer or school, is located in the EU. None of these services involve special

categories of data, nor do they involve criminal records data. Is it correct to interpret that this company will have no direct applicability of GDPR and will also NOT be required to appoint a representative, per the derogations in 27(2)?

- Comment 3: The Guidelines imply that "monitoring" requires the collection of personal data along with "subsequent behavioral analysis or profiling techniques involving that data." It is understood that the one-time aggregation of data related to suitability for employment would not amount to "monitoring." Is this a correct interpretation?
    - Example: A background screening report gathers data to confirm the accuracy of a data subject's CV, such as verification of employment and education credentials, and also checks such information as criminal record history. This information is gathered a single time and collated into a final report, provided to the potential employer. Our understanding is that this does NOT constitute "monitoring" as defined in 3(2). Can you please confirm if this correct?
- Comment 4: Would the interpretation supplied in Comment 2 change if the background report were updated at regular intervals?
    - Example: A data subject is hired for position requiring regular driving, such as a delivery driver. Their driving record is checked as part of the pre-employment background check as well as during the employment period as requested by the employer. Our understanding is that this does NOT constitute "monitoring" as defined in 3(2) as it is related to the employee's continued eligibility for employment and not "profiling," as that term is defined by the GDPR. Can you please confirm if this correct?
- Comment 5: Is the GDPR's application to processing that is "related to...the offering of good or services…to such data subjects in the Union" in 3(2) limited to circumstances under which the controller or processor in question offers goods or services directly to the data subject, with the term "related to" implying goods or services offered by the controller or processor? In other words, would an offering of business to business services, which services include the collection and sale of personal data on individuals in the EU, be covered, assuming such controller or processor is not otherwise directly subject to the GDPR?
    - Example: Background screening services are offered to a potential employer regarding information about a data subject. The service is not offered directly to the data subject. Our understanding is that the data subject is not being targeted and thus this specific provision of territoriality does not apply. Is this correct?
- Comment 6: Can more clarity be provided regarding the derogation of mandatory designation of a representative cited in 27(2)(a)? Specifically, it is not clear if the derogation intends to say that EITHER large scale, processing of special categories of data as referred to in Article 9(1) OR (any) processing of personal data relating to criminal convictions and offences referred to in Article 10 prevents derogation; OR if the derogation intends to say processing on a large scale of special categories of data OR processing on a large scale of criminal convictions and offences.
    - Example: If a US-based screening company not established in the EU, but otherwise covered under the territorial scope of the EU, that conducts several hundred criminal record checks per annum in the EU be exempt from the requirement to provide a EU-based representative?
- Comment 7: Can more clarity be provided on what constitutes "large-scale" processing?
    - Example: Most screening companies process thousands and sometimes tens of thousands of background checks per annum where the background check includes data regarding EU-based data subjects. The largest companies might process > 100,000 checks per annum where the background check includes data regarding EU-based data subjects. In all cases, the processing is done on an individual basis, with each data subject's data being processed individually, on a transaction basis. Would this constitute large-scale processing?

We thank you for taking the time to hear our concerns and appreciate the opportunity to provide this commentary to help further improve these regulations. NAPBS and its members are prepared to discuss any questions you may have and look forward to working with you further. Please feel free to contact me directly with any questions via email at Melissa.sorenson@napbs.com.

Sincerely,

Melissa L. Sorenson
NAPBS Executive Director