

Portuguese Supervisory Authority Launches Public Consultation on DPIA

CRA – Coelho Ribeiro e Associados, SCARL

Mónica Oliveira Costa

Ana Carolina Santos

1 August 2018

Portugal



The Portuguese Supervisory Authority (CNPd) just launched a public consultation on the list of the kind of processing operations that require a Data Protection Impact Assessment (DPIA). The end date to submit any views and concerns shall be 30 days after this list project is published on the National Official Journal, which shall occur soon, and can be done by e-mail (consulta.publica@cnpd.pt) or by post to the new CNPD's address at Av. D. Carlos I, 134, 1.º, 1200-651 Lisboa.

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) establishes on its Article 35.1 the obligation of the controller carrying out a DPIA, where, taking into account the nature, scope, context and purposes of the processing (and in particular those using new technologies), it is likely to result in a high risk to the rights and freedoms of natural persons.

No. 3 of the mentioned Article provides an illustrative list of cases, in which carrying out a DPIA is mandatory, such as:

- a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- b. processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences;
- c. a systematic monitoring of a publicly accessible area on a large scale.



The European Data Protection Board (EDPB), former Article 29 Working Party, has also issued guidelines (wp248rev.01) on DPIA and determining whether processing is “likely to result in a high risk” under the GDPR as well as providing examples of processing operations for which a DPIA is mandatory.

Nevertheless, the GDPR also creates (articles 35.4 and 57.1 k) a duty for national supervisory authorities to establish and make public a list of the kind of processing operations which are subject to the requirement for a DPIA. As a result, CNPD launched a public consultation concerning the referred list through the Draft of Regulation no. 1/2018¹, which, nevertheless, is a non-exhaustive and dynamic list that will be updated whenever deemed necessary. Thus and in addition to the processing operations stated in Article 35.3 of the GDPR, the Portuguese Supervisory Authority determines that the following processing operations are subject to a mandatory DPIA:

- a. Processing of special categories of personal data (article 9.1 GDPR) as well as personal data relating to criminal convictions or offences (article 10 GDPR) for other purposes than those for which they were collected (ex: for archiving purposes in the public interest, scientific research purposes or statistical purposes), unless such processing is authorised by law and provided that a DPIA is carried out;
- b. Processing of information resulting from the use of sensors or other electronic devices that transmit, via communication networks, personal data, with legal effects concerning the data subjects or significantly affect them in a similar way, namely those allowing to analyse or predict data subjects’ location and movements, tastes or personal interests, consumptions or other behaviours and health (e.g., medical devices implanted or applied);
- c. Interconnection or combination of personal data or processing that links special categories of personal data (article 9.1 GDPR);
- d. Processing of personal data where such data have not been obtained from the data subject, where it is not possible or feasible to ensure the right to information under article 14 GDPR;
- e. Processing of personal data involving or consisting on large-scale profiling;
- f. Processing of personal data that allows tracking the location or behaviour of data subjects (e.g. workers, customers or just passers-by), except the processing is necessary for the provision of services specifically required by clients;
- g. Processing of biometric data for unambiguous identification of the data subjects, unless such processing is authorised by law and provided that a DPIA is carried out;

¹ Draft Regulation No. 1/2018, concerning the list of processing operations for which a DPIA is mandatory available at https://www.cnpd.pt/bin/consultapublica/Projeto_regulamento_1-2018.pdf



- h. Processing of personal data using new technologies or new use of existing technologies;
- i. Significant change in the architecture of the information system on which the processing of personal data is carried out.

This list falls short of expectations due to, save very few exceptions, the broadness of the processing operations enumerated. Controllers call from their Supervisory Authorities for real effective guidelines, i.e., specific, clear and unambiguous, with much more (and less confusing) examples, rather than further vague and undetermined concepts, repetitions and/or small variations of those foreseen in the GDPR. Regrettably, it does not bring, as it should, the waited and desired legal clarity and certainty on when a DPIA is mandatory.