INFORMATIVE NOTE

PLMJ
ADVOGADOS, SP, RL

50 YEARS
By your side.

DATA PROTECTION

PERSONAL DATA PROCESSING AT WORK

On 8 June 2017, the Article 29 Working Party on data protection (the "WP29") approved an opinion on personal data processing at work (Opinion 2/2017). This opinion complements and updates a previous opinion on the matter (Opinion 08/2001) and a working paper on monitoring electronic communications from 2002.

On 8 June 2017, the Article 29 Working Party on data protection (the "WP29") approved an opinion on personal data processing at work (Opinion 2/2017). This opinion complements and updates a previous opinion on the matter (Opinion 08/2001) and a working paper on monitoring electronic communications from 2002.

The WP29 is a consultative body, made up of representatives from the data protection authorities of the European Union Member States. Even though the opinions of the WP29 are not binding, they are normally very useful documents, because they summarise the majority opinion of the data protection regulators on any given matter.

The topic of processing personal data at work is one that raises many doubts. This happens, above all, because of the lack of uniformity between the understanding of the regulatory authorities and even the employment courts, when called upon to decide on these matters. Against this background, any practical guidelines on this matter are clearly very welcome.

The main objective of this opinion is to update the understanding of the WP29 in face of the technological developments that have occurred since 2001. Opinion 08/2 the use of communication resources outside press 001 focused principally on the use of video surveillance systems, on monitoring email and the Internet, and on the use of location data. The tools available today make it possible to process the data of employees in multiple ways, and this is why the WP29 decided to review its position on the matter.

The Opinion addresses nine different data processing scenarios: (1) during the recruitment process; (2) monitoring employees' activities on social networks; (3) the use of communication resources in the press; (4) the use of communication resources outside the press; (5) control working hours; (6) the use of video monitoring systems; (7) the use of motor vehicles; (8) the disclosure of data to third parties; and (9) international data transfers.

Some of the key ideas we have identified in Opinion 2/2017:

- As a rule, the consent of the worker is not a legitimate ground to process some workers' data. This is because it has been established that, in the context of an employment contract, the worker is never truly free to refuse this consent.
- The most important ground is the pursuit of the legitimate interests of the employer, as established on a case-by-case basis. To be able to use this ground, the employer must ensure that data processing is strictly necessary for the purpose in question and that it is proportional in light of the needs of the business in question. The analysis of the proportionality of the data processing must look at whether all the data is necessary, whether the employees' right to privacy should not prevail over the legitimate interest, and whether adequate measures have been implemented to ensure a balance between the legitimate interest and the rights of the workers.

The workers must be informed about any data processing, and the WP29 recommends that policies on any monitoring carried out by the employer should be approved published.

- The workers must be informed about any data processing, and the WP29 recommends that policies on any monitoring carried out by the employer should be approved published. Whenever possible, the workers or their representatives should be involved in the preparation of these policies.
- The application of the principle of proportionality requires that the employer must always choose the least intrusive way of processing data.
- In the case of devices owned by the employees (Bring Your Own Device) permanent monitoring of communications is not allowed.
- The employer may not access health data collected by devices given or made available to its employees (including watches and other wearable devices).
- The use of facial recognition technologies to analyse the working environment is a form of processing that does not respect the principle of proportionality.
- The use of GPS in vehicles made available to employees must make it possible for it to be deactivated if the vehicle can be used for private purposes.

This Informative Note is intended for general distribution to clients and colleagues and the information contained herein is provided as a general and abstract overview. It should not be used as a basis on which to make decisions and professional legal advice should be sought for specific cases. The contents of this Informative Note may not be reproduced, in whole or in part, without the express consent of the author. If you should require further information on this topic, please contact **Daniel Reis** (**daniel.reis@plmj.pt**) or **Nuno Ferreira Morgado** (**nuno.morgado@plmj.pt**).