Newsletter FEBRUARY 2019

MORE NEWS ABOUT PRIVACY AND PERSONAL DATA

The adjustment phase of the Italian post-GDPR legislation is characterised by continuous new developments. Among these, the recent pieces of legislation on employment relationships and artificial intelligence seem particularly significant. At the same time, the national supervisory authorities have also started enforcement of the new legislation, and the most important case is the sanction issued by the CNIL (the French Data Protection Authority) against Google.

1. Processing of special categories of data and employment relationships: the Italian Data Protection Authority identifies the requirements compatible with the GDPR in Decision No. 497/2018

1.1 The Decision revising the existing General Authorisations. With Decision No. 497 of 13 December 2018 (the "Decision"), the Italian Data Protection Authority (the "*Garante*") identified the requirements set forth in the existing General Authorisations Nos. 1/2016, 3/2016, 6/2016, 8/2016, and 9/2016, which are still compatible with the new European and Italian legislation for the protection of personal data (the "Requirements").

At the same time, the Decision was submitted for public consultation until 12 March 2019.

Once the above Requirements are definitively approved on conclusion of the aforementioned public consultation procedure, their breach, if any, will render the data processed unusable and will expose the offender to administrative fines of up to 20 million Euros or, in case of companies, up to 4% of their total annual worldwide turnover of the previous year, whichever is the greater.

1.2 Employment relationships and special categories of data. Among the five authorisations involved in the revision of the *Garante*, General Authorisation No. 1/2016 concerning the processing of "special categories of data" in employment relationships is of particular importance for companies.

1.2.1 Special categories of data. According to art. 9 of the GDPR, "special categories of data" means personal data (called "sensitive data" in the existing Privacy Code) that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, and data concerning a natural person's health or sex life or sexual orientation.

1.2.2 Who is required to comply with the Requirements. The Decision will apply to all those who, for various reasons, carry out processing activities for the purpose of establishing, managing and terminating employment relationships: employment agencies and other intermediaries, natural and legal persons, companies, including social entities, institutions, associations and bodies that are part of an employment relationship, joint bodies, employees' safety representatives, labour consultants, employers' associations in pursuit of legitimate statutory purposes, and competent doctors in any field that provide their services.

1.2.3 Data subjects covered by protection. The list of data subjects, i.e. those whose data must be processed in compliance with the Requirements of the *Garante*, is considerably wide and does not include only employees. In fact, the following are protected: candidates for employment, consultants and independent contractors, agents, representatives, self-employed individuals,

natural persons holding corporate or other positions in legal entities, institutions, associations and bodies, third parties damaged in the carrying out of the working or professional activities of the data subjects, and their family members or cohabitants for the issue of benefits or permits.

1.2.4 Legal basis of processing. The Decision specifies, among the lawful purposes of the processing: the application of laws and collective agreements on the establishment, management and termination of employment relationships, the application of laws and regulations on social security and health protection, including supplementary pension/health schemes, or on hygiene, health and safety at work, as well as on tax and trade union matters, the payment of contributions, salaries, allowances, bonuses, other emoluments, donations or accessory benefits, to safeguard the life and physical safety of employees or third parties, the guarantee of equal opportunities in the workplace, the defence of a right in court, administrative, arbitration and conciliation proceedings, and the pursuit of further purposes in relation to trade union matters.

1.2.5 Prohibitions. Specific obligations are imposed on companies before and after the employment of the data subjects.

(i) Prior to employment, special categories of data may be processed only for specified and legitimate purposes and to the extent necessary to establish the employment relationship.

In this respect, the Decision mentions only the data suitable to reveal the state of health and racial and ethnic origin of the candidates, establishing that they can be processed only if their collection is justified by specific and legitimate purposes and is necessary to establish the employment relationship. The list lacks references to other types of special data (e.g. those that may reveal political or religious opinions or beliefs of candidates); however, it does not seem possible to infer a processing regime for these data that is less restrictive than the others, given the prevalence of the principle of proportionality and necessity of processing provided by the higher European source of law (the GDPR). It follows that employers or intermediaries will in any case be prohibited from seeking information revealing the political or religious opinions or beliefs of candidates, unless it is strictly necessary for the establishment of the employment relationship.

The collection of data through questionnaires or curricula will be subject to the same "strictly necessary" requirements, even if these are spontaneously sent by the candidates: everything that is superfluous for the possible establishment of an employment relationship shall not be requested or, if provided, shall not be used.

Finally, the processing of genetic data of candidates, even with their consent, is absolutely excluded.

(ii) During the course of the employment relationship, without prejudice to the prohibition of processing of genetic data of employees, the Decision specifies that:

- data regarding religious or philosophical beliefs or membership in associations or organisations of a religious or philosophical nature may be processed only in the case of the use of permits on religious holidays or for the provision of canteen services or, in the cases provided for by law, for the exercise of objection of conscience;
- data regarding political opinions or trade union membership, or the performance of public functions and political offices, or trade union activities or offices, may be processed exclusively for the purposes of granting personal leave or leave of absence recognised by law or by collective agreements (including company agreements), as the case may be, as well as to allow the exercise of trade union rights, including the processing of data relating to

withholdings for the payment of membership fees to associations or trade union organisations; and

- in the case of participation of employees in electoral activities as list representatives, no data revealing political opinions should be processed (for example, the document designating the list representative shall not be required as the certification of the chairperson of the polling station is sufficient for this purpose).

1.2.6 Methods of processing. From a practical point of view, the employer will have to follow the following processing methods:

- as a general rule, the data must be collected from the data subject. It follows that, except in special cases (e.g. the assumption of top management or senior roles for which special investigations may be required by law or collective agreements), the use of information contained in databases for so-called "background checks" does not seem to be allowed;
- communications, including electronic communications, containing special categories of data must be individualised, i.e. the most appropriate measures must be taken to prevent unjustified knowledge of personal data by parties other than the recipient (e.g. by forwarding paper documents in closed or stapled envelopes; by using double authentication systems for access to electronic communications, etc.);
- documents containing special categories of data must contain only the information necessary for the performance of the internal function or office to which they are transmitted, without attaching, where not strictly necessary, complete documentation or including excerpts within the text (for example, to manage an absence it may be sufficient to communicate the fact without attaching medical certificates proving it; or, in the case of leaves used for participation in elections, as candidates or list representatives, it may not be necessary to circulate documentation certifying the candidacy in a specific list or the representation of a list at the polling station); and
- the employer must not explain, even through acronyms, abbreviations or otherwise, the reasons for the employee's absence from which it is possible to infer the knowledge of special categories of personal data (such as trade union leaves, health data), even when for reasons of work organisation, and in the context of the preparation of shifts, data relating to attendance and absences from work are made available to parties other than the data subject (including other colleagues).

2. French Data Protection Authority (CNIL) imposes €50 million Euro fine on Google

2.1 The decision and the reasons behind. On 21 January 2019, the French Data Protection Authority, CNIL (*Commission nationale de l'informatique et des libertés*), imposed a fine of €50 million on the American company Google following complaints lodged by the associations None Of Your Business (NOYB) and Quadrature du Net (LQDN). This is the first sanction against Google under the **GDPR**.

The CNIL examined both the privacy documents published by Google and the browsing procedure that users must follow to configure an Android mobile device. At the end of the investigation, the following was found:

(i) Lack of transparency, as Google was found to disseminate information about the processing operations across several pages and documents, not easily accessible except through 5 or 6 clicks;

(ii) Lack of a valid legal basis for the processing, since the consent collected by Google was considered to be lacking the "specific and explicit consent" requirements provided by the GDPR, given that the box of consent to ads personalisation was pre-ticked, and moreover, the company collected a single expression of consent for a plurality of purposes (ads personalisation, speech recognition, etc.).

2.2 Territoriality and competence. The American company tried to defend itself by claiming the lack of competence of the CNIL and, instead, the competence of the Irish Data Protection Authority, on the assumption that it had identified its main establishment in Dublin. However, thanks to the application of Article 4(16) in conjunction with Recital 36 of the GDPR, the CNIL was also able to consider itself as competent and to apply the penalty accordingly. The French Authority pointed out that, at the time of the violation of the GDPR provisions, the Irish headquarters of the company could not be classified as a "main establishment", not only because of the lack of formalisation to that effect, but also because it lacked the power to make decisions on the purposes and means of processing the personal data acquired as a result of the use of the Android operating systems.

The Google case was the first test of the new rules on cooperation between supervisory authorities and on the so-called "one-stop-shop" mechanism, according to which the authority competent to make decisions against groups with different establishments in the European Union, in the case of cross-border processing operations, is that of the country in which the main establishment is located, which for Google is Dublin.

3. Artificial Intelligence and personal data protection: European guidelines arrive on the Data Protection Day

On 28 January 2019, the official Data Protection Day, the Advisory Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") published a text containing guidelines on data protection and artificial intelligence (AI).

In particular, the Committee offers a series of recommendations both to developers of AI solutions and to public decision-makers. Among the recommendations addressed to developers of AI solutions, it is particularly important to consider in advance any potential adverse effects of using AI on the rights of individuals, through impact assessment procedures that also involve independent committees of experts and academic institutions, but noteworthy are also the sections dedicated to the need to design algorithms so that developers do not make decisions conditioned by prejudice or based on an unnecessary amount of data. The latter problem can be solved by using so-called "synthetic data" in the "training" phase of the algorithm, i.e. a particular category of data anonymized by computer processing. In addition, developers are also recommended to maintain a "human rights by design" approach, of continuous vigilance over the algorithm, and to guarantee the right of data subjects not to be subject to decisions based on fully automated processes.

The Committee calls on governments, and public decision-makers in general, to ask participants in public calls for special forms of transparency on algorithms, but also guarantees regarding the carrying out of preventive impact assessments on personal data. Data protection should therefore become one of the main criteria for allocating public resources to AI. Finally, particular emphasis is

also placed on the need to prepare training and "digital literacy" programs in order to spread awareness among the population on the potential and the limitations of AI.

Newsletter FEBRUARY 2019

The Data Protection Department of Legance is available to provide any clarifications, also in respect of any specific situation which may be of interest to you.

For further information:

Andrea Fedi

Partner

T. +39 06.93.18.271

afedi@legance.it

Lucio Scudiero

Senior Associate

T. +39 06.93.18.271

lscudiero@legance.it

or your direct contact at Legance.

Newsletter FEBRUARY 2019

THE FIRM
Legance is an independent Italian law firm with expert, active and result-oriented lawyers, with a strong team spirit that has permitted a flexible and incisive organisational model that, through departments active in all practice areas of business law, offers the right balance between the specialist and the lawyer as a global consultant. Legance comprises more than 230 lawyers, working in its Milan, Rome, London and New York offices, and has a diverse and extensive practice covering the following areas: M&A and Corporate; Banking; Project Financing; Debt Capital Markets; Equity Capital Markets; Financial Intermediaries Regulation; Investment Funds; Litigation and Arbitration; Restructuring and Insolvency; EU, Antitrust and Regulation; Labour and Employment; Tax; Administrative Law; Real Estate; Energy, Gas and Natural Resources; Compliance; Shipping, Aviation and Transportation Law; Intellectual Property; TMT (Technology, Media, Telecommunications); Environmental Law; Insurance; Law & Technology; Food Law; Data Protection. For more information, please visit our website: www.legance.com.