Newsletter OCTOBER 2019

THE EDPB ISSUES NEW GUIDELINES ON VIDEO SURVEILLANCE AND ONLINE SERVICES

The European Data Protection Board ("**EDPB**") has recently issued two new guidelines on the interpretation of the General Data Protection Regulation EU 2016/679 ("**GDPR**") and, in particular, on the legal bases for lawful processing of personal data.

The first guideline, still subject to public consultation, concerns the processing of personal data through video-surveillance devices; the second, adopted in final version, concerns the lawful processing of online service users' personal data as necessary for performing the on-line contract or taking steps prior to entering into that contract at the user's request.

1. Guideline 3/2019 on processing of personal data through video devices (version for public consultation)

1.1 The risks of video-surveillance. First of all, the EDPB guidelines recognize the importance of regulating video surveillance in order to prevent unauthorized uses, particularly in regard of: the enormous amount of personal data that may be processed, the new technological developments (such as smart cameras and video analysis software) and possible detrimental and discriminatory outcomes that video surveillance may implicate. Those risks are indeed recognized both by art. 35(3)(c) of the GDPR, which requires a data protection impact assessment in the case of systematic monitoring on a large scale of a public accessible area, and by art. 37(1)(b) of the GDPR, which requires the designation of a data protection officer in the case of regular and systematic monitoring of data subjects on large scale.

1.2 A purely personal or household activity. Art. 2(2)(c) of the GDPR sets out that the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. The EDPB has clarified the restrictive interpretation of this exemption, which shall cover only the private and family activities of the person; therefore, where the video devices operate, even partially, in a public space, they falls outside of such exemption.

1.3 Purposes of the processing. The EDPB has reaffirmed that the purposes of processing have to be documented in writing and need to be specified for every camera (also collectively if more cameras are used for the same purpose). A generic purpose of ensuring "security" is not sufficiently specific and it is contrary to the principle of transparency of the processing.

1.4 The legal bases for the processing. In principle, every legal ground under Article 6(1) of the GDPR can provide a legal basis for video surveillance. However, in practice, the provisions most likely to be used are Article 6(1)(f) of the GDPR - legitimate interest – and Article 6(1)(e) of the GDPR - necessity to perform a task carried out in the public interest or in the exercise of official authority. In rather exceptional cases Article 6(1)(a) of the GDPR (consent) might be used as a legal basis by the controller.

1.5 The legitimate interest. In order to assess the existence of a valid legitimate interest pursued by a controller or a third party it is necessary to carry out and document a balancing test taking into account the interests, rights and fundamental freedoms of the data subjects.

(i) The principle of accountability. In light of the principle of accountability, the EDPB requires data controllers to keep evidence and to document circumstances/events justifying the video surveillance (date, manner, financial loss). For instance, the EDPB

clarifies that statistics that provide evidence of vandalism in a certain area may justify the installation and use by a shop owner of a video surveillance system. This is also the case with shops selling precious goods (*e.g.* jewellers), or areas that are known to be typical crime scenes for property offences (*e.g.* petrol stations).

(ii) The principle of data minimisation. The EDPB reiterates the importance of examining whether other alternative, less intrusive means can fulfil the desired purposes (*e.g.* fencing the property, security locks, tamper proof doors, providing better lighting, etc.). In general, video surveillance should be limited to private premises only; the monitoring of outdoor spaces must always have its own specific justification.

(iii) Making case-by-case decisions. In carrying out the balancing test, the controller has to evaluate the risks on the data subject's rights. The legitimate interest needs to be real and actual, it must not be theoretical or speculative. Each decision has to be taken case-by-case, taking into account the reasonable expectations at the time and in the context of the processing. For instance, an employee in his/her workplace is in most cases not likely expecting to be monitored; on the other hand, the customer of a bank might expect that he/she is monitored inside the bank or by the ATM. Signs informing the subject about the video surveillance have no relevance when determining what a data subject objectively can expect.

1.6 Consent. Such legal basis shall be used very carefully. In most cases employers should not rely on consent when processing personal data, as it is unlikely for the controller to prove that the consent was freely given. A context in which the data subject may feel pressured into giving consent, affects the consent itself (*e.g.* athletes may be asked consent to monitor the whole team; in such case the individual athletes may feel pressure into giving consent by the rest of the team, therefore no valid consent would serve as a legal basis).

1.7 Disclosure of video footage to third parties. Any disclosure of videos to third parties needs to have an autonomous legal basis. Additional purposes of data processing may be considered only if compatible with the initial ones for which the personal data were at first obtained. For example, a video taken for the purposes of avoiding damages to private property (in the context of a legitimate interest) may be shown to the lawyer to pursue an action for damages.

1.8 Processing of special categories of data. Video surveillance may entail the processing of data belonging to special categories. In order to assess whether a specific legal basis pursuant to art. 9 GPPR is necessary, it shall be addressed if processing of particular categories of data is the objective of the data controller. Taking a video of the inside of a shop and occasionally filming customers who may wear glasses or using a wheel chair is not considered per se to be a processing of special categories of data. Conversely, the use of video surveillance devices to monitor patients' health conditions in a hospital shall be considered as a processing of special categories of personal data (and shall be subject to the additional legal rules pursuant to art. 9 GDPR).

1.9 Transparency and information obligations. A layered (multi-level) approach shall be followed by data controllers in informing data subjects. The first layer should be the warning sign itself that a video camera is installed in a certain place; further mandatory details and information may be provided with the privacy information notice, at the second layer.

(i) The warning sign – the warning sign should be positioned at a reasonable distance from the places subject to monitoring. The data subject shall have the chance to easily recognize the circumstances of the surveillance before entering the monitored area. The sign should convey the most important information: the purposes of the processing, the identity of the data controller, the existence of the data subject's rights, a reference to where to find more information on the processing, and any other information, regarding specific circumstances, that is material to the data subject.

(ii) The privacy information notice – the full information notice on the processing of data must also be made available at a place easily accessible or displayed in a not monitored area. The EDPB recommends the use of technological means (*e.g.*: a QR code on the sign).

1.10 Storage and security. Eventually, the guidelines, reaffirm the obligation to keep video surveillance images only for the time strictly necessary for the pursued purposes (ideally suggesting a few days at most) and the importance of providing technical and organizational measures to minimize the processing.

2. ECHR's judgement dated October 17, 2019 on video surveillance at work

2.1 It seems appropriate to mention the recent judgment of October 17, 2019 of the European Court of Human Rights in applications nos. 1874/13 and 8567/13 (Lopez Ribalda and others v. Spain). The applicants alleged, *inter alia*, the infringement of Article 8 of the European Convention on Human Rights('ECHR'), which lays down the right to respect for private and family life. In particular, the applicants claimed that they had been filmed by means of hidden cameras, therefore without their knowledge, by their employer, in their workplace. Such recordings had led to their dismissal and had been used as evidence in the subsequent proceedings. The applicants, having exhausted internal means of appeal against the alleged unfair dismissal, filed a case against the Spanish Government before the European Court of Human Rights.

2.2 Margin of appreciation. The Court observes that under Art. 8 of the ECHR, States benefit of a margin of appreciation and that such article ensures only that the processing must be proportionate and be accompanied by adequate and sufficient safeguards against abuse, weighing up conflicting interests; i.e., on the one hand, the applicants' right to respect for their private life and, on the other hand, the possibility for the employer to ensure the protection of its property and the smooth operation of its company.

2.3 The decision. The Court concludes that "hidden" video surveillance is allowed only as a last resort, with spatial and time limitations that restrict as much as possible the monitoring on workers, taking into account legal remedies, reasons justifying use of video surveillance and legal safeguards to limit the processing of such data.

In the present case, the Court has found that the installation of hidden cameras was legitimate because: (*i*) there were reasonable grounds for suspecting theft committed by the workers; (*ii*) the areas being filmed were rather limited; (*iii*) the cameras had been in operation only for a limited period of time; (*iv*) no alternative solutions were feasible; and (*v*) the footage was only used in evidence in the consequent proceedings.

In Italy, the judgment is relevant in relation to the interpretation of the legality of employers' defensive checks under Article 4 of the Italian Workers' Statute of Rights (L. 300 of 1970).

3. Guideline 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects

3.1 Article 6(1)(b). Among the legal bases for processing, Article 6(1)(b) of the GDPR provides that processing is lawful to the extent that it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract. In its guideline, the EDPB has clarified the interpretation of this requirement in relation to online services.

3.2 Definition of online services. The EDPB, firstly, has clarified what shall be meant by "online services", defining them as any service provided at a distance, by electronic means and at the individual request of the recipient of the services, even if not paid for by the person who receives them (such as services funded through advertising).

3.3 The concept of "necessity". The guideline adopted by the EDPB focuses on the "necessity" requirement, as it applies to processing which is "necessary for the performance of a contract" or " for the performance of pre-contractual measures". In this respect, the EDPB states that the use of such legal basis must be limited to personal data objectively necessary for the performance of the contract or in order to take pre-contractual steps at the request of the data subject. Such concept must be interpreted restrictively: if there are less intrusive alternatives, in line with the principle of minimisation, the processing is not "necessary".

(i) The assessment of what is necessary. The assessment of "necessity" must be carried out independently from what is permitted or foreseen in the general terms and conditions of service ("T&Cs"). Processing which is useful but not objectively necessary for performing the service or for taking relevant pre-contractual steps at the request of the data subject cannot be "necessary".

(ii) The irrelevance of the T&Cs. The contractual terms and conditions cannot expand the categories of personal data needed for the performance of the contract. The concept of "necessary for the processing" does not depend on the contractual clauses: processing may be necessary even if not provided therein, or vice versa. In practice, this legal basis does not cover cases where processing is required by the data controller for the execution of the contract.

(iii) The perspective of both parties. The contractual purpose that shall be taken into consideration must be the mutually understood purpose; this depends not just on the controller's perspective, but also on the reasonable data subject's perspective when entering into the contract.

(iv) Assessment criteria. In order to carry out the assessment of whether Article 6(1)(b) is applicable, the following questions can be of guidance:

- What is the nature of the service being provided? What are its distinguishing characteristics?
- What is the exact rationale of the contract?
- What are the essential elements of the contract?
- What are the mutual perspectives and expectations of the parties?

(v) The incidents in the performance of the contract. The "necessity" has to be interpreted net of any "incidents", *i.e.* any actions that may be necessary in the event of non-

compliance, or incorrect performance of the contract. That said, it is possible to take into account certain actions which may be reasonably foreseen and necessary within a normal contractual relationship, such as sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract.

3.4 Examples. The guideline provides some examples. Specifically:

(i) processing for service improvement – in most cases, collection of organisational metrics relating to a service or details of user's engagement, cannot be regarded as necessary for the provision of the service, as the service could be delivered in the absence of processing such personal data. Nevertheless, a service provider may be able to rely on alternative lawful bases for this processing, such as legitimate interest or consent.

(ii) processing for behavioural advertising – as a general rule, processing of personal data for behavioural advertising is not covered by such legal basis; the fact that the online service funds the provision of the service by such advertising remains not sufficient to establish that it is necessary for the performance of the contract at issue.

(iii) personalisation of content – eventually, the EDPB acknowledges that personalisation of content may (but not always) justify a processing necessary for the performance of the contract. This is the case when personalization of content is an intrinsic aspect of online services, falling within the user's expectations. This is not the case when personalization of content is intended to increase user's engagement. The EDPB provides an example: such legal basis would not be applicable to an online booking search engine that monitors past bookings or past searches of users in order to provide future suggestions.

Newsletter OCTOBER 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 OCTOBER 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 around 250 lawyers, working in its Milan, Rome, London and New York offices, and has a diverse and extensive practice covering the following areas: Corporate Finance; Banking; Energy, Project & Infrastructure; Debt Capital Markets; Equity Capital Markets; Financial Intermediaries Regulation; Investment Funds; Litigation and Arbitration; Restructuring and Insolvency; EU, Antitrust and Regulation; Employment and Industrial Relations; Tax Law; Administrative Law; Real Estate; Compliance; Shipping, Aviation and Transportation Law; Intellectual Property; TMT (Technology, Media, Telecommunications); Environmental Law; Insurance; Food Law; Data Protection. For more information, please visit our website: www.legance.com.