DIGITALEUROPE

9 SEPTEMBER 2019

Response to EDPB consultation on video devices

Executive summary

DIGITALEUROPE is pleased to provide its comments on the European Data Protection Board's (EDPB) draft Guidelines on the processing of personal data through video devices. The use of technology in this area has tremendous benefits for individuals and organisations, but also generates concerns in the public and uncertainty for businesses, particularly smaller ones. We therefore welcome the EDPB's work to clarify how the General Data Protection Regulation (GDPR) applies to various types of processing by means of video devices.

In our response, we highlight areas where we find application of the relevant GDPR provisions can be simplified in light of the letter of the text as well as existing case law. In particular:

- The household exemption should be more expansively interpreted in light of the clarifications brought about by the GDPR;
- Reliance on legitimate interest should be more clearly recognised, in particular when the purpose of processing is to protect property and physical integrity;
- Stricter requirements for special categories of data should be contained to areas that meet the relevant GDPR definitions, in particular that relating to biometric data applicable to facial recognition.

While our comments encourage the EDPB to avoid Guidelines that are unduly restrictive, DIGITALEUROPE does not support the unmitigated deployment of video devices and associated technologies across all use cases. Video technologies will only gain consumer support if they are trusted; in many scenarios, privacy mitigations are necessary and ethical. Our goal, therefore, is

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

to strike a balance that makes it possible to continue to innovate and benefit from these technologies while also protecting data subjects' rights and interests.

We hope our suggestions, read in light of the GDPR's substantive obligations to preserve data subjects' fundamental rights, can contribute to a positive deployment of present and future video technologies in Europe.

Table of contents

Household exemption

In illustrating a narrow interpretation of the household exemption under Art. 2(2)(c), the draft Guidelines refer to two pre-GDPR CJEU judgments that exclude such exemption in case of publication on the internet and where processing involves, even partially, public spaces.[1] Accordingly, the three examples listed of exempted activities always refer to situations where individuals never publish their recordings online and/or are either in a remote area or in a purely private space.[2]

However, the household exemption has changed in important ways under the GDPR compared to Directive 95/46/EC. In particular, Recital 18 now specifies that the exemption applies when there is 'no connection to a professional or commercial activity' and explicitly mentions 'social networking and online activity' in the context of an individual's personal or household sphere as being exempted.

These important changes should be reflected in the final Guidelines. The Article 29 Working Party (WP29) previously recognised that in an increasingly digitised society it would be illogical and impractical to subject individuals to full or even partial compliance with data protection law.[3] As highlighted by the WP29, doing so could not only inhibit other fundamental rights, such as freedom of speech and association, but also jeopardise a long tradition of respect for individuals' private lives, which should not be open to 'official' regulatory scrutiny.[4]

The WP29 also recognised that other laws than data protection are available and might be more suitable to protect individuals against damaging material posted online under the household exemption. These include laws on libel, harassment, malicious communications, threatening behaviour, incitement, persecution or

[1] In cases C-101/01 and C-212/13, respectively.

[2] Para. 14, p. 7 of the draft Guidelines. In light of the three examples provided, the relationship between the two CJEU judgments mentioned above is not clear. The first and second example concern cases that could be considered similar to case C-212/13, but the draft Guidelines arrive at the opposite conclusion relative to the CJEU judgment based a separate reading of case C-101/01: the tourist and biker are filming public places, capturing either numerous passers-by (the tourist) or not capturing anyone or very few people (the biker riding in a remote area), but because no upload to the internet is occurring (as required following case C-101/01) the household exemption is deemed to apply (while in case C-212/13 it doesn't – although Mr Ryneš in that case wasn't uploading videos to the internet, either).

[3] See Annex 2 to the WP29 Statement on current discussions regarding the data protection reform package, February 2013, available at https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf

[4] Ibid., pp. 5-6.

discrimination. The role of these laws in defending individual rights should also be reflected in the final Guidelines.[5]

Legitimate interest

The draft Guidelines require a 'real-life situation of distress' in order for the legitimate interest legal basis to be met in case processing of video data to protect property.[6]

This means, based on the draft Guidelines' example, that a shop owner will not be able to install cameras unless she has suffered previous incidents of burglary, theft or vandalism –which the draft Guidelines require the owner to keep detailed proof of – or, at the very least, is able to present empirical and localised statistics showing high expectations of such incidents in the area.

In fact, there is no basis in the GDPR for such rigorous limits to controllers' reliance on the legitimate interest legal basis in situations where there are such clear interests at stake.

Any owner has a direct interest in protecting her property, irrespective of whether offences have already occurred or bear a high probability of occurring.[7] While legitimate interest does require a balancing test, we disagree that a case-by-case determination is necessary to establish the validity of legitimate interest for such uses.[8] More certainty is needed lest unnecessary and disproportionate effort is imposed in particular on SMEs.

On the other hand, we do agree that more complex determinations are required in relation to less straightforward cases. In practical terms, however, we believe these cases will be limited to those requiring a data protection impact assessment pursuant to Art. 35(3), particularly when monitoring on a large scale is concerned.

This does not detract from the need for processing in each specific case to be adequate, relevant and limited to what is necessary, nor does it impact the need for

[5] Ibid., pp. 6-7.

[6] Para. 20, p. 8 of the draft Guidelines.

[7] The draft Guidelines state that jewelleries and petrol stations, by reason of their being known targets for property offences, *may* count on legitimate interest as a basis for processing. These two examples shouldn't be stated as a mere possibility but should be clearly recognised as valid uses of the legitimate interest legal basis. We note that past incidents had been adduced by Mr Ryneš in case C-212/13 but the CJEU did not state anything with respect to their relevance in terms of establishing the legitimate interest legal basis. On the contrary, the Court held (para. 34) that 'the application of Directive 95/46 makes it possible, where appropriate, to take into account … legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the case in the main proceedings.'

[8] In relation to this, we also find problematic the example at para. 58, p. 13 of a shop owner who shares with the police material constituting a crime without there being an open investigation about such crime. We believe that reporting a crime should always be considered in the controller's legitimate interest.

the controller to implement technical and organisational measures minimising the impact on privacy and other fundamental rights (see next section of our response).

Necessity of processing

As stated in the Guidelines, there are various ways to protect property other than processing of video data. These include hiring security personnel and adopting physical protections and measures such as fencing, locks or lighting. This, however, does not imply that processing of video data is not a relevant and suitable measure.

With reference to necessity and the data minimisation principle (Art. 5(1)(c)), the draft Guidelines provide that video surveillance measures can only be deployed when and where 'strictly necessary.'[9] 'Necessity,' however, should be construed more expansively. The CJEU has held that processing that 'contributes to the *more effective* application' of legislation pursuant to Art. 6(1)(e) – and, by extension, to the more effective pursuit of the controller's legitimate interest under Art. 6(1)(f) – could be considered as necessary.[10]

Video devices can be valuable instruments, alone or in combination with other measures, to more effectively protect property and physical integrity. To the extent processing is in line and objectively linked with this purpose, we see no reason to ban the use of video devices, in itself, absent a detailed justification that no other means can be used in connection to the same purpose.[11]

This does not detract from the applicability of other GDPR provisions that require the controller to implement appropriate technical and organisational measures representing valid safeguards for the specific processing circumstances.[12] Some of these measures are mentioned in the draft Guidelines, including: blocking out or pixelating non-relevant areas; limiting use to more sensitive hours; or restricting access to the data to when an incident has occurred.

---

[9] Paras. 24 and 26, pp. 8-9 of the draft Guidelines.

[10] See case C-524/06, para. 62 (emphasis added). We note that a more restrictive interpretation of necessity with respect to Art. 6(1)(e) is required given that such article relates to the restrictions that Union or Member State law can impose on data subjects' rights, as evidenced by the GDPR's Art. 23. No such restrictions exist with respect to Art. 6(1)(f).

[11] Para. 126 of the draft Guidelines stipulates that unnecessary functions available in devices 'must be deactivated.' The examples listed include camera movements, zoom capability and audio recordings. Such capabilities, however, can be expected to be standard and widely available in devices. While due consideration should be given by controllers to how such functions are used, requiring deactivation altogether would fundamentally limit product design and development.

[12] Notably Art. 25 concerning data protection by design and by default.

Data subjects' reasonable expectations

The draft Guidelines adopt a presumption that, based on an 'objective third party' test, monitoring within public areas is likely not to meet the data subject's 'reasonable expectations.'[13]

It must be noted that people's expectations as to reasonable uses of video have changed since the introduction of the movie camera and can change in the future. A bank customer in the 1960s may not have reasonably expected that the bank would be fitted with cameras, yet the draft Guidelines now list this example as acceptable.[14]

This does not necessarily imply acquiescence to increased, intrusive processing of personal data, but may reflect a genuine shift in societal expectations and preferences. We suggest that a more circumstantial, case-by-case assessment is needed. For instance, video surveillance of parks, in particular where such surveillance is properly signalled to data subjects,[15] can be considered as reasonable in that it can substantially improve the safety and security of public spaces and of those who want to use them lawfully, similar to the parking area example.[16] Similarly, employees working in controlled environments such as warehouses or factories nowadays can reasonably expect that their workplace will be secured and equipped with video devices, in particular where clear information and notice are provided to them.

Again, this does not impinge on the application of broader GDPR provisions requiring the controller to minimise the impact of the specific processing operations on privacy and other fundamental rights.[17]

Data subject rights

We are particularly concerned with the draft Guidelines' statement that when a data subject objects to processing, the controller should be obliged to switch off the camera unless she demonstrates compelling legitimate grounds for not doing so.

---

[13] Para. 37, p. 11 of the draft Guidelines.

[14] Ibid.

[15] We disagree with para. 39, p. 11 of the draft Guidelines. The data subject's reasonable expectations are relevant in the context of the balancing test to determine whether the legitimate interest legal basis applies (Recital 47 of the GDPR). The presence of clear indications that video surveillance is deployed in a given area can certainly contribute to a data subject's objective expectation that video surveillance is present, although it will not in itself justify reliance on legitimate interest as a legal basis.

[16] P. 10 of the draft Guidelines.

[17] We also note that the use of video devices in public spaces will tend to have a link with Arts. 6(1)(c) and (e), as it may be specified in EU or Member State law. While the draft Guidelines include a short section on Art. 6(1)(e), they don't mention Art. 6(1)(c).

In line with our comments above,[18] we believe that the protection of property and physical integrity should always be considered compelling grounds, without the need for additional special circumstances or case-by-case assessments. Were this not the case, shoplifters or their accomplices could simply ask shopworkers to stop the processing and subsequently carry out their crimes.

The need to protect property, staff and customers as well as to prevent crime must be considered a 'compelling legitimate ground' despite any objections.

Special categories of data

We welcome the draft Guidelines' clarification that it is only when video is processed to deduce special categories of data that Art. 9 applies.

This implies that controllers actively pursue such deductions from the footage; by contrast, the fact that special categories can hypothetically be inferred does not suffice to trigger application of Art. 9. While this is clear in the example at para. 61, the first example at para. 63 suggests that the mere fact of observing a crowd would trigger Art. 9 because it is in theory possible to infer sensitive data. This should be rectified in the final Guidelines.

We are concerned with the draft Guidelines' blanket statement that facial recognition functionality will in most cases require explicit consent.[19] As explained at para. 75 of the draft Guidelines, the qualification of personal data as biometric data will require a case-by-case analysis to verify that the three cumulative criteria of Art. 4(14) are met. If one of the three criteria is missing, the processing of data will not be subject to Art. 9.

In particular, it must be stressed that the definition of biometric data implies processing for the specific purpose of uniquely identifying a given natural person. If processing doesn't result in such unique identification, the definition does not apply.

Facial recognition technology can in fact process data without uniquely identifying a person. Templates do not necessarily enable unique identification of an individual. The individual is uniquely identified only when the template is correlated with a pre-existing template connected to identifying information held by the controller. In the absence of this other template and information, the individual cannot be uniquely identified from the newly acquired template.

Consistent with paras 79 and 80 of the draft Guidelines, processing of a face template that is used only to detect matching faces should not fall under Art. 9. By contrast, Art. 9 does apply if biometric templates linked to uniquely identifying information are built and stored.

---

[18] See the 'Legitimate interest' section of our response, p. 4.

[19] Para. 76, pp. 15-16 of the draft Guidelines.

In some cases, facial recognition may be deployed with the aim to simply determine that two face templates are the same and others are different, with no interest in identifying who is behind each template. Examples of such uses include:

- The counting of how many people enter a controller's premises and to ensure the same person is not counted twice;
- Queue measurement;
- Calculation of how long it takes to move from the start to the end of a queue.

In other cases, facial recognition may be deployed to uniquely identify a person for whom the controller owns a biometric face template connected to identifying information. In such cases, the system is neither able nor seeking to uniquely identify every other person who steps in front of the camera just by capturing her face through intermediate templates.

In light of the above, we disagree with the draft Guidelines' assertion that on-the-fly processing falls under Art. 9, thus requiring explicit consent from anyone captured by the camera. As a consequence, we urge the EDPB to reconsider the two examples contained in para. 84 of the draft Guidelines.

Suggested measures

Section 5.2 of the draft Guidelines, entitled '*Suggested* measures to minimise the risks when processing biometric data,' appears to signify obligations on the part of data controllers, rather than suggestions. For instance, para. 87 states that in a controlled environment such as delimited hallways or checkpoints, templates 'shall be' stored in certain ways; likewise, para. 89 requires that controllers 'must' explore noise-additive measures. We urge that these and similar references should be softened. Requirements to follow unvarying prescriptive steps can actually undermine privacy by deterring usage of protections that may be more appropriate to a given set of circumstances. They also run counter to the GDPR's risk-based approach, which allows both controllers and processors to adapt their security measures to the actual risks.

Transparency and information

We believe that the first-layer information described in the draft Guidelines contains unfeasible requirements. The sample warning sign at para. 114, in particular, is overly crowded and ignores the majority of signs that have already emerged in compliance with Directive 95/46.

We believe that a feasible layered approach to informing data subjects must necessarily imply a very basic first layer of information that clearly signals the video

processing, provided by the sign, and additional information available in the second layer, in digital and/or physical format. In this context, we urge the EDPB to reconsider its position that the second-layer information should always also be provided in a non-digital format, as in most cases this will only generate increased burden without improving data subjects' access to the relevant information.

Use of alternative solutions to access services

The draft Guidelines require controllers to always provide an alternative to biometric solutions, in particular for authentication for the use of a service. While in principle agreeing with this approach,[20] we believe consideration should be given to situations where biometric processing may be inherent to a given service. For example, the video technology used in a frictionless store will be quintessential to the convenience of the service, which simply cannot be provided without it.

In addition, when facial recognition is used for security, authentication and identification purposes, having to provide alternative solutions may undermine the whole purpose of the processing. Requiring the controller to always offer an alternative way to access the building such as through badges or keys could lower the building's level of security. This is particularly problematic in the financial sector, which uses video ID verification products for know-your-customer and anti-money laundering purposes.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

[20] We note that such requirement may be needed for compliance with Directive (EU) 2019/882, which lays out accessibility requirements for products and services.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK