GDPR CCTV MONITORING

By Tara Taubman-Bassirian https://Datarainbow.eu

CASE	DATE	SUMMARY
By Tara Taubman-Bassirian https://Datarainbow.eu		By Tara Taubman-Bassirian https://Datarainbow.eu
Court of Appeal - 2020/123	24 May 2022	The **Irish Court of Appeal**, in an appeal brought by the Irish DPC, ruled that personal data that was collected through CCTV for the purpose of crime prevention, could not be lawfully used for staff monitoring and disciplinary proceedings. This subsequent, secondary purpose, was incompatible with its original purpose.
VG Ansbach - AN 14 K 20.00083	23 Fev 2022	The **Administrative Court of Ansbach** held that the video surveillance of training areas in a gym was not lawful under Art 6(1)(b) GDPR and 6(1)(f) GDPR, therefore the DPA was entitled to require the controller to refrain from using video cameras. Data subjects had not given their prior consent by a clear and affirmative act. The mere acknowledgment of signs and the data protection notices are insufficient to comply with Art 6(1)(a) GDPR. The video surveillance was also compliant to Art 6(1)(b) GDPR. Contractual secondary obligations such as duties of consideration and protection may be covered by Art 6(1)(b) GDPR, but the continuous video surveillance in dispute went beyond these obligations. Therefore, the video surveillance was not necessary for the fulfilment of these secondary obligations as the recording of the training areas is not necessary. It is not in line with the general public's view to protect data subjects in gyms from assault and thefts through uninterrupted video surveillance or to make it easier for the controller to prosecute such incidents through video surveillance. The court also held that the video surveillance was not lawful pursuant to Article 6(1)(f) GPDR. The interest of the data subjects, namely their fundamental right to informational self-determination, prevailed. The continuous video surveillance in the gym on all training areas was a serious encroachment on this fundamental right of data subjects without any possibility of alternative space or time. Because of this lack of alternative for data subjects alone, their interests outweighed those of the controller. There were other, possibly not equally effective, but at least sufficiently effective measures available to the controller to protect its interests, such as an increase in staff. This was further aggravated by the fact that data subjects did not have to expectation of video surveillance in the gym. Even when considering the extent of the damages suffered, no other weighing of the interests was justified. The damage to property amounts to approximately €10,000 to €15,000 per year, while the income amounted to €200,000 in 2019. The

		legitimate interests of the data subjects themselves also did not justify a different result of the weighing as the ability to exercise in the gym without video surveillance overrides the interest in being protected from general risk of life by means of video surveillance.
BVwG - W274 2242638-1	20 Dec 2021	The **Austrian Federal Administrative Court** held that national provisions on video surveillance and image processing are inapplicable since the GDPR lacks an opening clause that would trigger them. Moreover, video surveillance to deter others from taking pictures of an estate is not justified under Art 6(1)(f) GDPR The court confirmed its view that special national provisions on video surveillance and image processing are inapplicable since the GDPR lacks an opening clause for them (cmp. BVwG W211 2210458-1/10 https://gdprhub.eu/index.php?title=BVwG_-_W211_2210458-1/10). The court held that the surveillance is not justified under Art 6(1)(f) GDPR. It was not clear for the court how image recordings could deter people from filing unjustified reports because people are in principle free to be in public traffic areas, even if it amounts to loitering, and free to file reports with the authorities on the basis of observations made in public traffic areas. Furthermore, the court reasoned that installing cameras could also not be an effective and therefore not an appropriate measure against the taking of photos by means of personally-held cameras, because they could in no way prevent such behaviour. Furthermore, the court mentioned that even if "the throwing of rubbish bags over the fence" were proven, the processing would not have been justified under Art 6(1)(f) GDPR since the captured space is exceeding the general recommendation of the DSB (Austria) which is a maximum of 50cm from the property line. FACTS : The data subjects and the controller are neighbours. The controller has its business located at the beginning of the street section whereas the data subjects' business is at the end of the dead end. They are entrenched in a neighbourly dispute for years. The controller installed two self-triggering cameras on its premises pointing towards the data subjects' business and capturing the street. The camera took pictures of the data subjects without their consent. The reasons given by the controller for installing the cameras were as follows: constant loitering of one of the data subjects around the premises of the controller taking pictures of the premises, numerous (about 300) complaints to the trade authorities concerni ng the business of the controller throwing of rubbish bags over the fence (which the court did not see as proven)

Rb. Amsterdam - AMS 20/3251	09 Nov 2021	The **Amsterdam Court of First Instance** held that a homeowner association lawfully installed new surveillance cameras in their apartment building because their legitimate interest in the protection of common property outweighed an individual resident's interest in the protection of their privacy (Article 6(1)(f) GDPR). First, the Court considered whether the measure was necessary by assessing the proportionality and subsidiarity of the measure. It held that the requirement of proportionality was met since the cameras do not allow the processing of biometrical data, and clear images of filmed people are justified by the fact that, in cases of damage, it needs to be clear against whom the charges are to be made. The requirement of subsidiarity was also met since the objective of the surveillance could be achieved in a less intrusive manner. Second, the Court conducted a balancing test of the interests of both parties. It considered that it is guaranteed that the data subject (and persons visiting her) will not be filmed more than necessary. Moreover, the Court noted that the controller had drawn up privacy regulations and had taken measures to limit the undesirable consequences of camera surveillance as much as possible: images would be deleted - in any case - after four weeks: the video recorder is password-protected; the recorder is placed a locked room; only a limited number of members of the Board of the VvE are allowed to check the images; and log files of the actions performed in kept a logbook. Lastly, the Court considered that people that pass by the camera, are informed about the camera surveillance (via a sign). Therefore, the Court concluded, with regard to the balancing test, that the interest of the controller in securing the communal property and that of the residents, and in being able to make a substantiated report if necessary, outweighed the data subject's interest of the protection of her privacy. Another issue on the applicability of national video surveillance and image processing provisions takes the Supreme Court of Austria (Oberster Gerichtshof - OGH) (see OGH 6 Ob 150/19f, However, the Supreme Court did not explicitly address this topic but rather implicitly affirmed the applicability.
Fairhurst v Woodard (Case No: G00MK161).	12 Oct 2021	A dispute between neighbours over the use of cameras for security purposes, the case gave rise to successful claims in harassment and data protection, and offers an important note of caution for those looking to install surveillance systems to protect their homes.

High Court finds use of CCTV evidence breached data rights in staff disciplinary investigation		A hospice employee has won a High Court appeal over the use of data from CCTV footage in a disciplinary investigation into unauthorised breaks and staff room graffiti saying "Kill all whites, ISIS is my life". Cormac Doolin, a craftsman's mate at Our Lady's Hospice and Care Service in Harold's Cross, Dublin, had appealed a Circuit Court decision that his data rights were not breached as a result of the use of information from CCTV footage for a disciplinary investigation into the graffiti and into the taking of unauthorised breaks in the hospice staff room.
VG Regensburg - RN 9 K 19.1061	06 Aou 2020	The **VG Regensburg** holds that Art 79 GDPR excludes further judicial remedies against controllers and processors. Therefore, actions for injunctive relief under §§ 1004 (1), 823 (2) German Civil Code (BGB) in the area of data protection should in principle no longer be possible. The applicant seeks an order tat the City of P. refrain from video surveillance of the "P.er K.-garten" and from recording it. The claimant argued that the installed video surveillance in a park is not necessary to prevent a.o. drug-related crimes. Moreover, the surveillance should not only be turned off entirely on market days, but also during other events which he would like to initiate. The court ruled: 1. Art 79 GDPR precludes further judicial remedies against controllers and processors, so that a general action for performance in the form of an action for an injunction pursuant to §§ 1004 (1) and 823 (2) of the German Civil Code is not permissible within the scope of the GDPR. 2. A distinction must be made between data processing that is (merely) contrary to the Regulation and a possible infringement of a person's rights with regard to the personal data relating exclusively to that person. 3. In the case of a mere unlawful data processing without any infringement of rights, the data subject has the right of appeal under Art 77(1) GDPR and subsequently the right of judicial remedy against the supervisory authority under Article 78(1) GDPR. Article 79 (1) GDPR provides for an individual right of injunction with regard to the violation of data subjects' rights (Article 13 to 20 GDPR).
RvS - 201903691/1/A3	26 Feb 2020	The **Dutch Council of State** issued a judgement on the processing of personal data by the means of two surveillance cameras, installed at a business' entrance gate for security purposes. The Court ruled that the surveillance cameras' use was lawful as there was a proper balance of interests between controllers' passers-by. Following on-site investigations, the surveillance camera position has been adjusted to be less visible for the public road. Thereafter, the area monitored corresponded to the plot boundary with the entrance gate and

		a section of the public road. In this regard, the AP found that the surveillance camera's owners had legitimate interests in installing the camera, as it was used for security purposes and that one incident already took place. For that purpose, the AP found that a limited part of the public road must be filmed and that it cannot be achieved by another less restrictive mean. In addition, the AP pointed out that the data controllers had implemented sufficient safeguards to inform the passers-by about the installation of the aforementioned camera. The AP concluded that the complainant's privacy interests did not outweigh those of the data controller. The complainant challenged the AP's decision before the District Court, which dismissed the appellant's claims as well. As a consequence, the appellant lodged an appeal against the District Court's decision before the Council of State.
EMPLOYEE VIDEO SURVEILLANCE: POSITION OF THE EUROPEAN COURT OF HUMAN RIGHTS		. On October 17, 2019, the European Court of Human Rights (ECHR) approved the installation of a Closed-Circuit Television ("CCTV") surveillance system which was used to monitor supermarket cashiers without informing those employees of the fact that it had been installed.
Deux décisions sévères contre la vidéosurveillance		A deux reprises, la CEDH vient de s'opposer à la vidéosurveillance, y voyant une ingérence tantôt illicite, tantôt disproportionnée. Même lorsque la surveillance a pour but d'identifier parmi les membres du personnel l'auteur de vols avérés, la Cour estime qu'il y avait moyen de mieux concevoir la mesure.
By Tara Taubman-Bassirian https://Datarainbow.eu		**DPA DECISIONS** By Tara Taubman-Bassirian https://Datarainbow.eu
DPAs DECISIONS		
		By Tara Taubman-Bassirian https://Datarainbow.eu
AZOP (Croatia) - Decision of 21 July 2022 - unknown car sales and service centre	**21 Jul 2022**	The **Croatian DPA** fined a car dealership approximately €4,000 for processing of personal data by a video surveillance system without prior notice. The DPA held that the controller violated Art 27(1) of the Croatian GDPR Implementing Act which provides for an obligation to clearly mark premises that are under video surveillance. This notice must be visible at the latest when entering the area in question. The DPA found that the controller did not put up a notice that its premises were under video surveillance and hence violated the Act.
	2022	**Italian DPA** fines Municipality of Policoro due to excessive retention of video footage / inadequate information signs / DPO conflict of interest € 26'000 for the use of a video surveillance system which served, among other things, to combat illegal wate disposal. Recordings were stored for

		longer than permitted. Lacked of transparency: signs did not contain all the required information. In addition, the recipient of the fine had appointed his lawyer as data protection officer, which in the opinion of the DPA constituted **a conflict of interest.**
Datatilsynet (Denmark) - 2020-832-0028	22 Jun 2022	The **Danish DPA** held that the Danish Football Association and Danish League could deny an access request seeking CCTV evidence in a suit against the police, but it reprimanded the two for conflicting statements on their joint controllership First, the DPA held that the DBU and the Divisionsforeningen were justified in refusing to facilitate **the data subject's access request** with regard to the CCTV footage. There are exceptions to the right of access. According to Art 22 of the Danish Data Protection Act, an access request under Art 15 GDPR may be denied if the **data subject's right is overridden by a vital public interest**, particularly that of state security and public safety. The DPA found that the data subject's right in this particular case was indeed overridden by the overriding considerations of public safety. However, the DPA also emphasized that restrictions on the right of access should only be made on the basis of a specific assessment of the information available at the time of receipt of an access request. This applies in particular in cases where the data subject provides a specific (and legitimate) justification for the access request. Second, the DPA held that DBU and the Divisionsforeningen's processing of personal data violated Art 5(1)(a) GDPR and therefore issued a reprimand against them. This was because throughout the communication with the data subject and the DPA, the DBU and the Divisionsforeningen gave different, contradictory information about who the controller was.
AEPD (Spain) - PS/00393/2021	07 Jun 2022	The **Spanish DPA** fined a restaurant owner € 3,000 for installing CCTV cameras to monitor the **public space** outside the restaurant which included a neighbour's front door. The DPA held that the cameras constituted excessive surveillance and imposed a fine of € 2,000 on the controller for violating the principle of data minimisation in Arti 5(1)(c) GDPR. The DPA fined the controller an additional €1,000 for failing to provide adequate signage in compliance with Art 13 GDPR. The DPA noted that it is the responsibility of the controller to make sure surveillance cameras are set up in a lawful manner. **Surveillance cameras must be oriented towards private property to avoid excessive recording;** recording public spaces is an exclusive competence of the Spanish state. Furthermore, cameras must be accompanied by signage indicating their presence, the purpose of surveillance, and the **identitiy of the controller**. This is true even in the

		case of a "simulation" camera which might lead to third parties believe that they are being permanently recorded.
ANSPDCP (Romania) - Fine against Asociația de Proprietari Aviației Park	27 May 2022	The **Romanian DPA** fined € 7000 a building owners association for keeping an extensive register of couriers entering the **residential complex** and for keeping video surveillance footage of the entrance longer than necessary for security purposes. The DPA fined the controller for violating Article 5(1)(a), (c), (e), (2) GDPR and Article 6 GDPR by processing the personal data without a legal basis, by violating the principles of data minimisation and storage limitation. € 2,000 (RON 9,885.80) of the fine was for the violation of Article 5(1)(a), (c) (2) GDPR and Article 6 GDPR by keeping the access register and €5,000 (RON 24,714.50) for the violation of Article 5(1)(e), (2) GDPR by **storing the video footage longer than necessary** for the purpose of monitoring the access to the complex. Additionally, the DPA ordered the controller under Article 58(2)(d) GDPR to bring is processing into compliance with the GDPR by: reviewing and updating the technical and organisational measures on the basis of a risk assessment, especially establishing a deadline after which collected data is anonymised and which is in accordance with the storage limitation principle. evaluating the processing carried out to implement the necessary measures to comply with the principles of Article 5 GDPR.
ANSPDCP (Romania) - Fine against LORIS FUEL SHOP SRL	12 May 2022	The **Romanian DPA** fined a gas station € 1,000 for not implementing **appropriate technical and organisational measures** against unauthorised access to video footage captured by its surveillance cameras. The DPA fined LORIS FUEL SHOP SRL €1,000 for violating Art 29 and 32(4) GDPR by not implementing the necessary technical and organisational measures to protect the video footage from unauthorised access. Furthermore, it instructed the controller to ensure compliance with the GDPR by implementing appropriate technical and organizational measures, especially in the form of training its employees, verifying access to the stored video recordings and implementing measures to rapidly detect, manage and report data breaches.
ANSPDCP (Romania) - Fine against Concordia Capital IFN S.A.	04 May 2020	The **Romanian DPA** fined a controller € 4,000 for installing video surveillance systems in its offices and monitoring its employees, without a legal basis in breach of Art 6 GDPR. The DPA started an investigation and found that: the purpose used to install surveillance cameras, and therefore to process its employees' personal data, was not justified and

		less intrusive measures could have been used to reach the same purpose (physical security); the controller processed the personal data without a legal basis in breach of Art 6 GDPR and without respecting the data processing principle stated in Art 5(1)(a), (b), (c) GDPR and 5(2) GDPR; the controller did not use the video surveillance systems according to the legal requirements of Art 5 of the national law no. 190/2018 which regulates the conditions of installing video surveillance at the workplace in conjunction with Art 6(1)(f) GDPR. As a result, the controller was fined approximately EUR 4,000 (RON 19,772.4).
Garante per la protezione dei dati personali (Italy) - 9777996	28 Apr 2022	The **Italian DPA** fined a public waste collection company (processor) €200,000 for installing video surveillance systems without prior authorisation of the Municipality of Taranto (controller) and for posting videos on Facebook with identifiable persons without a legal basis.
AZOP (Croatia) - Unknown energy company	08 Mar 2022	The **Croatian DPA** imposed a fine of approximately €120,000 against an energy company for a violation of Art 15(3) GDPR by failing to provide the video surveillance recordings requested by the data subject. The DPA found that the controller violated Art 15(3) GDPR, by denying him the right to obtain a copy of the video surveillance recording. The DPA decided to impose a fine on the controller. Considering that the controller gained a financial benefit from the violation, since it avoided the financial damage it might have suffered as a result of the consumer dispute with the data subject. The DPA emphasised that it cannot determine whether the data subject is entitled to compensation for damages in his consumer protection dispute. However, the DPA decided to impose a of HRK 940,000 (approx. €120,000), for the violation of Art 15(3) GDPR.
AZOP (Croatia) - AZOP (Croatia) - Decision of 8 March 2022 - Unknown supermarket chain	08 Mar 2022	The **Croatian DPA** imposed a fine of approximately €89,000 against a super market chain for lacking to implement appropriate security measures for the processing of personal data (in violation of several provisions under Article 32 GDPR) after an employee recorded video surveillance footage with their mobile phone and shared it on social media. The DPA found that the controller did not take appropriate measures to prevent its employee from filing the video surveillance with their phone. The DPA considered that the controller took certain organisational measures, such as the education of employees, and the adoption of internal acts that prescribed the authorisation of access to video surveillance. Moreover, the controller required employees to sign a confidentiality

		statement. However, according to the DPA, this was not enough. First, the controller did not supervise, test, evaluate and determine the effectiveness these measures (Article 32(1)(d) GDPR). Second, the controller did not ensure the ongoing confidentiality, integrity, availability of personal data (Article 32(1)(b) GDPR). Hence the controller did not take appropriate organisational and technical security measures that could have minimised the risk of the same, or a similar violation. Therefore, the DPA concluded that the controller violated Article 32(1)(b), Article 32(1)(d), Article 32(2), and Article 32(4) GDPR.
Garante per la protezione dei dati personali (Italy) - 9777996	28 Avr 2022	The **Italian DPA** fined a public waste collection company (processor) € 200,000 for installing video surveillance systems **without prior authorisation of the Municipality** of Taranto (controller) and for **posting videos on Facebook** with identifiable persons without a legal basis. The DPA held that the processor violated Article 28(2), as it did not notify the controller prior to contacting ITS about the video surveillance system. The DPA noted that public entities can lawfully process personal data for the fulfilment of a legal obligation or for the performance of a task in the public interest pursuant to Article 6(1)(c) and (e) GDPR. The DPA followed that even if the processing is lawful, it must also be in accordance with the principles laid down in Article 5. Since no indication of a legal basis for the placement of the videos on its Facebook page was found (Article 6 and Article 2-ter of Code Privacy), the DPA held that the processor violated the principles of "lawfulness, correctness and transparency" (Article 5(1)(a) GDPR). The DPA further held that the controller violated the principle of "purpose limitation" Art 5(1)(b). The DPA found no indication of any compatibility with the purposes for which the personal data was previously collected (detection of illegal activities) for further processing (publication on Facebook). Lastly, the DPA held that the processor violated Art 28, as it found that the processor had not appointed a data protection officer pursuant to Article 37.
Garante per la protezione dei dati personali (Italy) - 9773950	07 Avr 2022	The **Italian DPA** fined € 20,000 the municipality of Orte for operating photo-traps without adopting any compliance measures, for failing to provide information to the data subjects, and for failing to provide direct contact to their DPO. The DPA held that the controller failed to adopt a privacy policy and to implement technical and organizational measures to ensure compliance with the GDPR before installing the surveillance system. By doing so, the controller violated the principles of lawfulness, fairness and transparency, storage limitation and accountability of Art 5(1) GDPR, Art 24 and Art 25.

		The DPA clarified that information on video surveillance systems should be provided to the data subject through a layered approach. On this point the DPA referenced the EDPB Guidelines[1] as well as its own guidelines.[2] The DPA also held that the controller violated its duties of information under Art 12(1) and Art 13 by neglecting to inform the data subjects about the surveillance system, and to provide any information required under Art 13. Additionally, the DPA held that the controller violated Art 37(7), as it did not provide the DPA with direct contact information of their DPO. The DPA stated that supervisory authorities must be able to contact the DPO directly. The contact information must be specific to their DPO and distinct from the controller's. In this regard, the DPA referenced the Working Party 29 Guidelines[3] (as well as their own guidelines on DPOs in the public sector).[4] The DPA fined the controller for €20,000 and ordered it to provide new and direct contact information of their DPO.
ANSPDCP (Romania) - Fine against IAMSAT Muntenia SA	22 Feb 2022	The **Romanian DPA** issued a fine of approximately € 3000 on a company for not granting a former employee's right to object, and for **not informing its employees** about the video surveillance systems installed in its workplace. The DPA held that the company had violated Art 12(3) and 21 GDPR by not handling the **data subject's request** to exercise their right to object. It also held that the company had **not adequately informed** its employees on the processing of their personal data through video surveillance at the workplace, in breach of Art 12 and 13 GDPR. For the former violations, the DPA issued a fine of approximately € 1000 (RON 4.946,2) on the company, and for the latter, a fine of approximately € 2000 (RON 9.892,4). Additionally, as corrective measures, the DPA ordered the company to inform its employees about its data processing activities conducted through video surveillance in its workplace, as well as to reply and resolve the data subject's objection request accordingly.
Personvernnemnda (Norway) - 2021-20 (20/01648)	15 Fev 2020	The **Norwegian Privacy Appeals Board** upheld a DPA decision fining a beauty salon about €10,000 for unlawful camera monitoring that gave the general manager constant live access to images and sound via a mobile app on her phone, without informing the employees or customers. The Board agreed with the DPA that the installation of the camera was not discussed with the employees in advance, as claimed by the defendant, since there were no evidence of such discussions. The Board noted that **continuously montoring a workplace** is very intrusive for the employees, and also for the customers since there were no proper signage or information about the

		surveillance, and finds this to be a serious violation of the GDPR. The Board agreed with the DPA in that the defendant's actions are serious and criticisable, deserving of a sanction and which justified the level of the fine. This was further substantiated by the lack of technical and organisational measures for GDPR compliance in the company.
Garante per la protezione dei dati personali (Italy) - 9746047	27 Jan 2022	The **Italian DPA** fined a private club € 2000 for having security cameras pointing towards the public sidewalk without an appropriate information sign, violating Articles 5(1)(a), 5(1)(c) and 13 GDPR. The DPA noted that the use of video surveillance systems may result in the processing of personal data depending on the positioning of the cameras and the quality of the images captured. Furthermore, the Italian DPA stated that processing of personal data by video surveillance cameras must be carried out in compliance with the general principles contained in Article 5 GDPR, in particular with the principle of transparency. In the case of video surveillance cameras, this presupposes that "*the interested parties must always be informed that they are about to enter a video surveillance area*", and therefore the data controller must place appropriate information signs which convey this information to data subjects. The DPA held that the processing of personal data carried out by the club in this case was unlawful since it was not carried out in accordance with the principles of "lawfulness, fairness and transparency" and "data minimisation", in violation of Art 5(1)(a) and (c) GDPR, as well as in breach of the adequate information requirements under Art 13 GDPR.
AEPD (Spain) - PS/00224/2021	13 Jan 2022	The **Spanish DPA** fined an individual € 1500 for inadequately installing a video surveillance system, in breach of the data minimisation principle, as well as failing to provide sufficient information to data subjects on where to exercise their rights. After restating the law on installing video surveillance cameras, the DPA held the respondent violated Art 5(1)(c) GDPR and Art 13 GDPR by **intentionally or negligently positioning the cameras to record public areas without justified cause**, therefore processing data of identifiable natural persons, and by failing to provide sufficient information as to the identity of the controller and where data subjects can go to exercise their rights under the GDPR. As such, the DPA imposed a fine of €1500 on the individual and ordered them to move the cameras to comply with the GDPR.
CNPD (Luxembourg) - Délibération n° 47FR/2021	01 Dec 2021	The **Luxembourg DPA** fined a transport company € 6800 for failing to comply with the principle of data minimisation by not limiting the field of vision of its video surveillance

		systems as well as inadequately informing both its employees and third parties of their existence. First, the DPA assessed whether the company complied with the principle of data minimisation per Art 5(1)(c) GDPR. It started by affirming that only what is strictly necessary to achieve the pursued aims can be filmed, and that the processing operations cannot be disproportionate when assessed against their purpose. Companies seeking to lawfully install such systems are therefore required to set out the exact purposes of the processing prior to their installation. During the investigation, the company argued the systems were installed to protect its goods and access to facilities, as well as to safeguard users and prevent accidents. The DPA nonetheless held that three cameras did not comply with the requirements under Art 5(1)(c) GDPR. In particular, the camera aimed at the reception, which was unlawful because workers have a right to not be constantly monitored. The camera aimed at the "smoker's corner", which was unlawful because it monitored a space reserved to employees' leisure time. Finally, the camera aimed at the **public road** outside the office and neighbouring land, which was unlawful because it was disproportionate when assessed against the purposes of the processing. Second, the DPA assessed whether the company complied with its information obligations under Art 13 GDPR. It found that although the employees were notified of the existence of the video surveillance systems, visitors of the company's facilities had no access to this information. Thus, the Luxembourg DPA held that the company (1) failed to comply with the principle of data minimisation by not limiting the field of vision of its video surveillance systems, and (2) failed to adequately inform its employees and third parties of their existence.
DPC (Ireland) - DPC Case Reference: 03/SIU/2018	**09 Dec 2021**	The **Irish DPC** imposed an administrative fine of € 110,000 against a city council due to numerous failings in meeting data protection obligations in some of its smart city initiatives. The DPC identified a total of 48 issues in the course of the inquiry. The most important issues determined that the Council: a) had no lawful basis for the processing of personal data by CCTV cameras for traffic management purposes; b) lacked a lawful basis for a number of CCTV cameras used for the purposes of countering crime; c) lacked a lawful basis to carry out surveillance with CCTV cameras which employed Automatic Number Plate Recognition technology; d) infringed Art 15 GDPR by rejecting subject access requests in respect of CCTV cameras used for traffic management purposes;

		e) did not fulfil its transparency obligations under Art 13 GDPR by failing to erect signage in respect of its CCTV processing operations ; f) infringed Art 12 GDPR by failing to make its CCTV Policy more easily accessible and transparent. The DPC exercised the following corrective powers: a) A temporary ban on the processing of personal data with CCTV cameras at a number of locations used for the purposes of criminal law enforcement until a legal basis can be identified. b) A temporary ban on the processing of personal data with CCTV cameras used for traffic management purposes until a legal basis can be identified. c) An order to the Council to bring its processing of personal data into compliance taking certain actions specified in the decision. d) A reprimand in respect of a number the Council's infringements. e) An administrative fine of € 110,000.
CNPD (Luxembourg) - Délibération n° 44FR/2021	09 Nov 2021	The **Luxembourg DPA** fined a car dealership €1500 for failing to comply with the principle of data minimisation by not limiting the field of vision of its video surveillance systems as well as inadequately informing both its employees and third parties of their existence. First, the Luxembourg DPA assessed whether the company complied with its information obligations under Art 13 GDPR. Companies seeking to lawfully install such systems are therefore required to set out the exact purposes of the processing prior to their installation. During the investigation, the DPA found no information as to the existence of the video surveillance system had been provided by the car dealership. Additionally, the employees were never notified of the existence of the video surveillance systems. The owner of the dealership argued they were not aware of the obligation to provide such information and had only installed these to ensure customers would not have to wait if one of the receptionists were ever missing. The DPA nonetheless held the car dealership breached Art 13 GDPR by failing to provide information on the existence of the video surveillance systems. Second, the DPA assessed whether the car dealership complied the principle of data minimisation per Article 5(1)(c) GDPR. DPA pointed that only what is strictly necessary to achieve the pursued aims can be filmed, and that the processing operations cannot be disproportionate when assessed against their purpose. The dealership stated the images captured by the camera were not recorded, but simply transmitted onto a screen for the owner to check whether customers were dealt with in time when the reception was not

		occupied. The DPA's inspector found that the field of vision of the cameras essentially allowed the constant surveillance of employees working at the reception, which they held to be disproportionate as said employees could feel constantly observed. As such, the DPA held the car dealership contravened Art 5(1)(c) GDPR because the cameras could be replaced with less invasive means to achieve the purpose pursued, such as a counter which welcomes customers. Thus, the DPA held that the company (1) failed to comply with the principle of data minimisation by not limiting the field of vision of its video surveillance systems, and (2) failed to adequately inform its employees and third parties of their existence. It fined the dealership €1500 for these violations of the GDPR.
CNPD (Luxembourg) - Délibération n° 35FR/2021	06 Nov 2021	The **Luxembourg DP**A imposed a fine of € 5300 on a company for using a video camera surveillance system on its premises and tracking devices in some of its employees' vehicles in breach of the information obligation set out in Art 13 GDPR and in breach of the principle of data minimisation set out in Art 5(1)(c) GDPR. The DPA carried out an audit on the premises of a company to verify whether the latter was complying with the GDPR with respect to the installation of video surveillance cameras in the building and of geolocation tracking devices in the vehicles of some of its employees During the audit carried out by the CNPD, the CNPD found that the Company had failed to comply with several obligations relating to the principles of transparency and data minimisation. First, the DPA found that the Company had violated the principle of data minimisation as well as the obligation to properly inform data subjects about the processing. According to the DPA, the principle of data minimisation in the context of video surveillance implies that (i) the Company should only record what appears **strictly necessary to achieve the purpose(s) of the processing**, i.e. protecting the Company's assets and securing access to the building and (ii) that the processing operations must not be disproportionate. In this case, the DPA found that one of the cameras had been installed in such a way that the field of vision included the staff dining hall potentially monitoring employees during their free time. The DPA considered that installing cameras and filming the employees in places designed for private use **disproportionate**. In particular, the DPA pointed that the **fundamental rights and freedoms of the employees** (including their right to privacy) were prevailing over the legitimate interests of the employer to use video surveillance cameras foe security purposes. The DPA further found that the outdoor camera's field of vision included **part of the public street as well as an**

		adjacent site (i.e. the parking lot and the entrance of a shop located in front of the Company's building). The DPA admitted that, depending on the configuration of the premises, it is sometimes impossible to limit the field of vision of the camera to private premises only. Sometimes, a small portion of the street or of the surrounding is also being recorded. In such a case, however, the DPA considers that the data controller should implement masking or blurring techniques in order to limit the field of vision of the camera to its private property. In view of the above, the DPA concluded that the Company had been acting in breach of the principle of data minimisation Art 5(1)(c) GDPR. Violation of the obligation of information Informing the data subjects about the processing of their personal data is an essential element of the principle of transparency. The DPA noted during the on-site audit that the existence of the video camera surveillance system was not notified to visitors. Furthermore, the employees were not duly informed about all the points listed in Art 13 GDPR. After the on-site audit, the Company adopted several measures in an attempt to remedy that breach, such as displaying stickers with a warning sign and an information sheet at the entrance to the building about video camera surveillance. The DPA found however that these measures were not sufficient to fully comply with Art 13 GDPR. In this respect, the DPA recommended to adopt a ***"multi-layer communication approach"***: (i) the first layer of information (e.g. a warning sign accompanied with a short text) should generally convey the most important information, such as the **existence of a processing, the purpose of the processing, the identity of the controller, etc, as well as the way to obtain further information** ; (ii) the second layer of information, which must include the rest of the elements listed in Art 13 GDPR, should be made easily accessible to the data subject, for example in the form of a comprehensive information sheet available at a central location (e.g. information desk, reception or cashier) or displayed on an easy accessible poster. As mentioned above, the first layer of information should clearly refer to the second layer of information. Based on these elements, the DPA found that the Company had violated Art 13 GDPR. On the use of geolocation tracking devices During the on-site audit, the DPA found that the employees were not informed of the presence of geolocation tracking in some of the Company's vehicles, except in some instances orally. The DPA referred to the guidelines of the Article 29 Working Group on the transparency principle, and in particular to the fact that to controllers should always keep a

		written record of the measures that they have adopted, so that they are able to prove compliance with the obligation set out in Art 13 GDPR. because the Company was not in position to prove that all its employees had been duly informed about the use of geolocation tracking device, the DPA found that the Company had violated Art 13 GDPR. Considering the severity and extent of those violations, the DPA imposed a fine of € 5300 on the Company. The DPA also issued an injunction against the Company to adopt corrective measures in order to bring its processing operations into compliance with the GDPR within a period of two months. in particular, the Company was ordered to: (i) modify the field of vision of the cameras, (ii) inform third parties in a clear and precise manner about the video surveillance system by providing them with all the information set out in Art 13 GDPR, (iii) inform employees individually in a clear and precise manner about the video surveillance system and tracking devices in their cars by providing them with the information set out in Art 13 GDPR.
Personvernnemnda (Norway) - 2021-13 (20/01874)	04 Nov 2021	The **Norwegian Privacy Appeals Board** first reduced a fine for unlawful camera surveillance from €20,255 to €10,127, and then repealed it entirely due to the fact that the Norwegian DPA had not handled the case within a reasonable period of time. The PVN agreed with the DPA that the Company had infringed Art 6(1)(f) GDPR because of the **absence of a valid legal basis for the processing** of personal data through the installation of surveillance cameras. However, the PVN considered that the breach of Art 6 GDPR as not as serious as the DPA had found. In the opinion of the PVN, the breaches of Art 13 and 24 GDPR were more serious. After an overall assessment, the PVN concluded that the amount of the administrative fine for such violations should be limited to €10,127 (NOK 100,000). After considering the length of the procedure, however, the PVN decided to annul the fine altogether due to the DPA's long case processing time (i.e. in total, almost three years).
Persónuvernd (Iceland) - 2021010073	02 Nov 2021	The **Icelandic DPA** issued an injunction against a private individual to stop monitoring some shared and public areas around a multi-family house through video surveillance cameras, and to delete all the recorded material. The DPA first recalled that the monitoring of a private property via surveillance cameras could fall outside of the scope of the GDPR in line with Art 2(2)(c) GDPR (i.e. processing of personal data "by a natural person in the course of a purely personal or household activity"). In the case at hand, however, the field of vision of the three cameras covered some **shared spaces** (such as the common garden of the house) and some public areas (such as the sidewalk in

		front of the house). As a consequence, the processing of personal data was not covered by the household exemption set in Art 2(2)(c) GDPR, and had to comply with the rules and principles of the GDPR. The DPA then considered whether such processing could be justified on the basis of Art 6(1)(f) GDPR (i.e. processing is "necessary for the purposes of the legitimate interests pursued by the controller (...), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (...)). After balancing the legitimate interest of the neighbour to monitor the shared property with the right and freedoms of the Complainant, as well as any other individuals who could have been filmed by those cameras, the DPA concluded that **the neighbour had failed to demonstrate the need to monitor the covered areas**. As a consequence, the DPA considered that the processing of personal data through the surveillance cameras was unlawful. In view of the above, the DPA issued an injunction against the neighbour to stop the electronic monitoring of these areas, to delete all the recorded material, and to confirm that these instructions had been followed no later than 26 November 2021.
AEPD (Spain) - PS/00377/2021	18 Oct 2021	The **Spanish DPA** warned a Municipality for failing to meet its information obligations to its employees regarding the placement of video surveillance cameras that also record audio. First, the recording of personal conversations is an invasion of privacy. This is therefore strictly forbidden and can lead to a violation of Art 5(1)(c) GDPR. Second, the cameras must be limited to the purpose for which they are intended. Also, the way of capturing and processing this data must be proportionate in relation to this purpose (surveillance/security). Third, the DPA recalls that, in order to comply with Art 12 GDPR, a clear sign must be placed in a visible area (e.g. access door) indicating that it is a video-monitored area, and it must indicate: . the existence of the processing. . the identity of the data controller. . the possibility of exercising the rights provided for in Art 15 to 22 GDPR. Absence of clear information leads to the violation of Art 13 GDPR. Respondent had failed to install and show a clear sign that provided this information. Moreover, the purpose of security had not been known to the legal representatives of all the public employees of the aforementioned entity, although they must be aware of the purpose(s) of the images obtained. Hence, this constituted an infringement, attributable to the respondent, for violation of Art 5(1)(c) and 13 GDPR.

		Therefore, the DPA (1) imposed a warning on the Municipality and (2) ordered respondent to: Place information signs duly approved to the current GDPR at the main entrances to the Town Hall within one month of the decision. Inform all public employees of the measures adopted, in particular those related to the purpose(s) of the processing. To place the entrance camera so that it is used for the security function of the Town Hall, but avoids capturing the work area of the employees exclusively, disabling the audio option if necessary.
Datatilsynet (Denmark) - 2020-31-3586	06 Sep 2021	The **Danish DPA** held that an insurance company breached Art 15 GDPR by refusing to give an insured person access to a surveillance report which the company had compiled about them. The company could not restrict the data subject's access right because the report might be used in litigation against i After reviewing the facts of the case, the Danish DPA found that the insurance company had infringed Art 15 GDPR, as implemented by section 22 of the Danish Data Protection Act. In particular, the DPA recalled that the right to access of the data subject could only be restricted on the basis of "*decisive considerations*" pertaining to prevailing interests of the data controller or another party. According to the DPA, this exception only applies when there is an "*imminent danger*" that the interests of a private party will suffer "*significant damage*". In this case however, the insurance company would have not suffered a significant damage from handing over the surveillance report to the data subject. In particular, the Danish DPA considered that the fact that the surveillance report may have been used, by the complainant, as evidence in a litigation against the insurance company did not constitute a "*decisive consideration*".
Datatilsynet (Norway) - 20/01648	14 Jul 2021	The **Norwegian DPA** fined a beauty salon approximately €9,473 (NOK 100,000) for unlawfully installing camera surveillance that gave the general manager constant live access to images and sound via a mobile app on her phone, without informing employees or customers. Following an appeal, the Norwegian Privacy Appeals Board upheld the DPA's decision. The Norwegian DPA held that the controller had breached Art 5(1)(a) and (c), 6, 12(1) and 13 GDPR and for this fined the controller NOK 100,000 (approximately €9,473). The fine was reduced from NOK 150,000 because the business had a reduced turnover following the circumstances around COVID-19. The DPA emphasized in particular that:

		The camera had a wide-angle lens capable of capturing 130 degrees. The camera was angled towards the reception area and the area towards the treatment room. The camera was able to record sound. The general manager had remote access through a mobile app on her mobile phone. The camera was enabled and the surveillance was active at all times, including with motion sensor. Further, the DPA commented that the controller should have conducted a Data Protection Impact Assessment (DPIA) before installing the camera and considered other, less invasive ways to achieve the claimed purpose.
IP (Slovenia) - 0611-10/2021/11	15 Jun 2021	The **Slovenian DPA** held that a bar owner does not have a legitimate interest in monitoring the various rooms and outdoor terrace of the bar with video surveillance, but does have a legitimate interest in monitoring the bar counter and bar entrance. Accordingly, the DPA gave the bar fifteen days to adjust the viewing angles of its surveillance cameras to record only the counter and entrance. The DPA explained that video surveillance is the processing of personal data (Art 4(2) GDPR) and the operator of video surveillance is responsible for complying with the principles set out in Art 5 GDPR, including data minimization, purpose limitation and storage limitation. In assessing the adequacy of procedures and measures to ensure an adequate level of security of personal data, the bar must also comply with Art 32 GDPR, which provides that controllers and processors shall ensure a level of data security appropriate to risks to the rights and freedoms of individuals by, for example, endeavouring to maintain the confidentiality of data subjects. According to national law (ZVOP-1), video surveillance of a business premises may be carried out for the safety of people or property, to ensure control of entry into or exit from or from business or business premises, or if, due to the nature of the work, there is a possibility of endangering employees. Thus, the bar has a legitimate interest, as recognized in Art 6(1)(f) GDPR, in processing data limited to those purposes. In contrast, there is no provision allowing for the general surveillance of employee workplaces, such as server rooms, if the protection of people in these workplaces can be achieved by milder means. The interest of the bar manager in securing the bar rooms also does not outweigh the interests and freedoms of bar guests. The IP thus concluded that there is no legitimate interest, based in a need for data processing, for video surveillance of spaces where guests are located and where employees work.

CNPD (Luxembourg) - Délibération n° 21FR/2021	11 Jun 2021	The Luxembourg DPA fined a controller €7600 for failing to comply with the principle of data minimisation and for failing to provide data subjects with required information about their video surveillance system. Regarding the video cameras, the NCPD held that non-compliance with Article 5(1)(c) GDPR in respect of the two above-mentioned cameras was established on the day of the on-site visit, even if the controller changed the range of vision to make it compliant afterwards. In the same way, the CNPD considered that non-compliance with Article 5(1)(c) GDPR in respect of the six other cameras was established too. Regarding the information of the cameras, the CNPD held that the pictogram did not contain the required elements of the first level of information (essential information) for either employees or third-parties, since it only informed about the recording but did not provide any more of the information required by Article 13 GDPR. Furthermore, the CNPD held that the document entitled "Information to workers - Privacy protection" did not contain all the information required by Article 13 GDPR. Therefore, the CNPD concludes that at the time of the on-site visit of the CNPD officers, the company was not compliant with Article 13 GDPR. The CNPD held that the controller infringed Article 5(1)(c) GDPR and Article 13 GDPR and decided to: - impose an administrative fine of €7,600 on the controller, - issue an injunction to the controller to bring the processing into compliance with the provisions of Article 13 of the RGPD, within a period of two months following notification of the decision, with proof of compliance to be sent to the CNPD at the latest, within this period.
ANSPDCP (Romania) - Fine against Glove Technology SRL	23 Sep 2021	The **Romanian DPA** fined a controller approximately €5,000 (RON 24,745) after it used CCTV systems to surveil its employees, record their conversations and use the recordings against them, in breach of Art 5(1)(a) and Art 6(1) GDPR.
DSB (Austria) - DSB-D123456	10 Aug 2021	CCTV camera pointed at the office over the street. Controller argued that using the street is consent to CCTV. Austrian DPA held, that walking on the street is not unambiguous consent.
AEPD (Spain) - PS/00120/2021	23 Jul 2021	The **Spanish DPA** fined Mercadona, a supermarket chain, € 3,150,000 (reduced to €2,520,000) in relation to its video surveillance system that **used biometric data** to identify individuals who had previously committed crimes at its store and who were banned from entering. On Art 6, 9 and 5(1)(c) GDPR Special categories of data

		The DPA started by confirming that the data processed by Mercadona was included in the special categories of data from Art 9 GDPR, since it is biometric data that is used for the purposes of biometric identification (as opposed to biometric authentication). As remarked by the DPA, facial recognition systems are identification systems that are very intrusive for rights and freedoms. The DPA also noted that the processing was carried out at a distance, continuously, and it was **automated, and used algorithms to create the patterns**, what derived in a extreme risk, as it may lead to an indiscriminate and mass surveillance. Therefore, the controller should have relied on a valid exception from Art 9(2). According to the DPA, the controller could not have relied on the exception from Article 9(2)(g), regarding public interest, since such interest must be set by national law, that shall also specify the circumstances, limits, rules, and measures for applying the exception and relying on a public interest and be proportionate. Since there is no national law allowing this type of processing, the controller could only have relied on explicit consent. The DPA also remarked that all the persons that entered any of the shops of the controller were the system was used were treated as convicted subjects, since the controller's justification to use the system was to control and prevent only the entry of convicted persons. The judgments allowed for the use of electronic means to implement the system, as requested by the controller; in some cases even mentioning facial recognition, in accordance with the measures allowed by the Spanish Criminal Code. The DPA concluded that such measure may only affect the (rights of the) convicted persons. Additionally, not all judgments talk about facial recognition. And, particularly, the DPA noted that the use of such system **should take into account the nature and context of the situation that leads to the processing, including the seriousness, probability and depth of the potential harm and consequences to rights, guarantees and freedoms of all the affected persons,** including the convicted persons. Also, the judgment allowing the use of such means should have included the necessary and proportionate conditions and guarantees to be implemented, what they did not actually do, leaving it to the discretion of the controller. In this regard, the DPA also considered important that the controller had tried to prepare in advance the legitimacy to carry out such processing by directly requesting the courts to allow them to use a facial recognition system to control the entry, and that this had been done without carrying out in advance a data protection impact assessment (DPIA), an analysis of the (extreme) risk and a prior consultation to the AEPD, as they should have done. This, that should had been

		done before requesting the permission of the court, should have led the controller to determine the unacceptability of the risk. Additionally, the DPA stated, the electronic means used by the controller shall only had affected the convicted persons to which the judgments concerned, not third persons such as Mercadona clients and workers. Legal basis The DPA also remarked that the controller did not have an appropriate basis form Art 6 to rely on. In the same way as what the DPA noted regarding the exception from Art 9(2)(g), the public interest legal basis from Art 6(1)(e) needs to be defined by law, including a mention to affected interests, restrictions to its use, limits and conditions. This will pose a limit for public powers, as well as ensure the principle of legal certainty. However, in this case, there is no real connection between the security measure the system used for and public interest; it only pursues the private interest of the controller. The DPA also differentiated between activities that are connected to a public interest, so they benefit the society as a whole, and where a judge or court should assess its proportionality, against an activity in which public interest is used to legitimise the massive processing of the data of every person, so everyone is treated as a convicted person. The DPA argued, in line with the previous judgment, that there is **no such public interest**, since the company was only pursuing a private interest. Analysis of the legal bases and exceptions In its analysis about legal bases and exceptions, the DPA differentiated between three types of processing: the processing of convicted persons data, the processing of potential clients, the processing of Mercadona workers. With regards to the data of the convicted persons, Mercadona alleged the use of the exception from Art 9(2)(f), regarding the processing of data for legal claims. However, the DPA concluded that the use of this exception was not valid. In this case the legal claims had already been exercised or defended. Additionally, the existence of a legal claim does not entitle the controller to process such data per se; other conditions must be met. In accordance to Recital 52, this shall be done exceptionally and when it is necessary. It also requires adequate guarantees. Therefore, the interpretation of the legal text must be done in a restrictive way. In this sense, the AEPD compared this exception to Article 10 GDPR, that also requires, for the processing of criminal data, to be under the supervision of a public authority; in this case, the processing was not supervised, only potential consequences deriving from it (such as the non-compliance with the judgment). The DPA also remarked here that, for example, if it was the court that would be the one to carry out the

		processing, they could only process data of the convicted persons, since the measures contained in the judgment can only affect convicted persons. Therefore, what a court cannot do should not be allowed for a private actor to do. With regards to the legal basis from Article 6, the DPA stated, as already explained, that the basis from Article 6(1)(e) needs, firstly, to be defined by law and, mainly that such public interest did not exist, since the company was only pursuing a private interest. With regards to the data of potential clients, Mercadona tries to rely also on the exception from Article 9(2)(f), which as explained is not valid. The DPA explained again that the court can only establish measures in its judgment that affect the rights of convicted persons; third persons cannot have their rights affected. This third persons include children, minors and vulnerable people. This totally disproportionate measure, as the DPA remarked, violates the spirit of the GDPR. The DPA concluded that, even if the exception from Article 9(2)(f), the measure, that is a taken in the framework of a criminal procedure, can only affect the persons affected by the judgment; otherwise, it would indirectly mean massively imposing a criminal measure on non-related third persons. This would generate a perverse effect, that would be translated in practice to the establishment of a large scale facial recognition system, highly intrusive in people's rights and freedoms, that would pose an unacceptable risk. Although it is true that the Spanish law, both the Data Protection Act, in its Article 22, and the Private Security Act, in its Article 42, allow for video surveillance systems, this does not include facial recognition systems, that pose a much bigger risk and are more intrusive, and are not meant to be used for private interests. With regards to Mercadona workers, the AEPD concluded that they were not taken into account in the DPIA carried out by the controller, even when they were specially affected. In accordance with the Opinion from the A29WP, the controller should have carried out an evaluation between legitimate interests of the controller and the reasonable privacy expectations of the employees by outlining the risks posed by this technology and by undertaking a proportionality assessment, what was not done at any moment. The use of the technology was clearly disproportionate, also as there is a risk that it may result in an indirect control of the workers. The DPA also made reference to the new provision implemented in the Spanish labour law, providing for algorithmic transparency of artificial intelligence systems that affect workers, as they found a lack of transparency regarding the functioning of the system. This is also connected with Articles 5(1)(a), 12, 13, and 14 GDPR, and Article 89 of

		the Data Protection Act, that provides for a privacy right for workers. In conclusion: a measure that affects only a very small number of persons that have been convicted does not legitimize the use of this technology. There is no legal basis, nor any exception from Article 9, that can legitimize the processing. Therefore, Articles 6 and 9 had been violated. Proportionality assessmenteditedit source Data processing requires a proportionality assessment. The assessment must entail three requirements: adequacy assessment, necessity assessment and proportionality assessment in a strict sense (rights and freedoms balance). The assessment must additionally be carried out at the right moment, i.e. before actually carrying out the processing. Also, it will require a detail look when dealing with biometric data, that pose a higher risk. Whether the the resulting loss of privacy is proportional to any anticipated benefit must be weighed. The processing must be essential to fulfill the need. This also means that if there is a less intrusive way to achieve the pursued end, it shall be followed. Therefore, the processing must not just be useful, but strictly necessary to achieve the purpose. According to the DPA, the processing was neither proportionate, since it affected the rights of every potential client and the employees when it should only affect convicted persons, nor necessary, since there are less intrusive ways of achieving the purpose, such as having the photographs of the convicted persons in every premise, for the security staff to know them. The AEPD also remarked that, in this case, this system may not even be adequate for the purposes, since it would be easy for the convicted persons to fool it, using, for example, a mask, so it may be neither useful nor effective. This is also linked with Articles 5(1)(c) and 25(1) GDPR. The fact that the processing is authorized by a judgment does not make it necessary; specially since it does not provide for any safeguards, what should be hence done by the controller, that is responsible for the compliance, in accordance with the accountability principle too. The controller still has to comply with the data protection rules. The DPA also remarked that it was not proven that the controller had adopted any technical measures to avoid the transfer of data to third parties, including international transfers of data. Minimization principleeditedit source With regards to Article 5 GDPR, the DPA also noted that the minimization and purpose limitation principles shall be respected; particularly the minimization principle from Article 5(1)(c) GDPR. However, the own nature of facial recognition systems leads it to a massive processing of biometric data -

		that shall entail reinforced guarantees, also because of the high number of affected data subjects. The processing activity at stake is, additionally, not proportionate, since it could be argued that it is adequate but it is neither necessary nor strictly proportionate, since there are less intrusive alternatives and as the rights and risks are not properly balanced. Therefore, the processing is exercise; the controller is processing data of every potential client and employee only for the purpose of controlling a small number of convicted persons. Therefore, the minimization principle was infringed, so there had been a violation of Article 5(1)(c) GDPR. Personal data of childreneditedit source The AEPD put special emphasis in the fact that the controller should have carefully considered the risks that the processing of personal data from children and vulnerable persons entail, in accordance with Article 28(2) of the Data Protection Act. Conclusioneditedit source Hence, the DPA concluded that there is no possibility of relying on the exception from Article 9(2)(g), there is no valid legal basis from Article 6(1), and that the necessity, proportionality and minimization principles had not been respected. Therefore, Articles 6(1), 9(1) and 5(1)(c) GDPR were violated.
CNPD (Luxembourg) - Délibération n°24FR/2021	29 Jun 2021	The **Luxembourg DPA** fined a controller €12,500 for violating the data minimisation principle by recording **public areas** and permanently monitoring employees with its video surveillance system, and for failing to provide the necessary information regarding the processing of data by the system.
IMY (Sweden) - DI-2018-22697	09 Jun 2021	The **Swedish DPA** fined a fire department € 34,555 (SEK 350 000) for installing CCTV cameras that monitored firefighters in a way that was more intrusive than necessary First, the DPA examined whether the CCTV cameras required a permit. The Swedish Camera Surveillance Act (kamerabevakningslagen), which contains supplementary rules to the GDPR, sometimes requires a permit for the use of CCTV. 7 § of the Camera Surveillance Act requires a permit if the surveillance is carried out by a public authority and if the surveillance is of a "place to which the public has access". The DPA concluded that a fire station is not a place to which the public has access and that the Rescue Service did not need a permit for CCTV. Was there a legal basis? The DPA considered whether there was a legal basis in Art 6(1)(e) GDPR for processing data for the performance of a task carried out in the public interest. On the one hand, the DPA found that the monitoring of the staff who are in a vulnerable position, in this case was **constant, intimate, and**

		intrusive. However, given the particular role that society has given to the Rescue Service and the need for the command centre to be able to effectively manage and organize a response to an emergency, the DPA found that there was a legal basis for the processing. Fairness and data minimization The DPA considered whether the monitoring complied with the principle of lawfulness, fairness and transparency under Art 5(1)(a) GDPR. The DPA referred to the preparatory work of the Swedish GDPR Implementation Act when it noted that the legislator intended that **the proportionality of the monitoring must be assessed by balancing the conflicting interests,** even if a legal basis exists. The DPA recognised that the employer had very strong reasons justifying the surveillance. Nevertheless, the DPA considered that the surveillance was **too wide-ranging**. Firefighters were monitored in places where they changed clothes, without censorship or demarcation. The DPA also investigated whether the Rescue Service had practiced data minimisation under Art 5(1)(c) GDPR. The DPA found that the purposes of the monitoring were legitimate, but that the means chosen were **too intrusive and breached the principle of data minimisation**. The DPA considered that the monitoring was unfair and breached Art 5(1)(a) GDPR, as well as the lack of data minimisation practice to breach Article 5(1)(c) GDPR. For these two violations, the DPA imposed a fine of SEK 300 000. Was the data sufficiently protected? Finally, the DPA assessed whether the monitoring data was adequately protected. The CCTV were monitored live from the command centre. The command centre had 29 staff, 6 of whom held the position of inner command and were authorised to view the camera footage. The Rescue Service stated that it was possible for any employee present in the command centre to view the camera footage and witness what was going on at a particular fire station. The Rescue Service had **also not issued any guidelines** regarding the monitoring of the CCTV. The DPA acknowledged that it is sometimes warranted to allow a wider range of command centre staff to view the CCTV. However, given the nature, scope, and intrusiveness of the monitoring of the CCTV, the DPA held that the Rescue Service was at fault for not issuing guidance. The DPA stated that the more sensitive the processing, the higher the data protection requirements. The **lack of policies** could have led the staff of command center to monitor firefighters more than was necessary and lawful. The DPA found that the Rescue Service had breached Art 32(1) GDPR and Art 32(4) GDPR by failing to take the necessary organizational measures. For this, the DPA imposed a fine of SEK 50 000.

AEPD (Spain) - PS/00261/2020	03 Jun 2021	The **Spanish DPA** fined a company € 26,000 (reduced to €19,600) for recording images of their employees' resting room and for not offering up-to-date information about the use of video surveillance at the workplace. The DPA concluded, in the first place, that even if there might had been an infringement in the storage of the images for more than a year, the violation was already prescribed, according to the former Spanish Data Protection Act, as more than two years had passed since the moment in which the controller handled the images to the court. On the other hand, the DPA found that the controller had violated Art 5(1)(c) GDPR when recording part of the employees' resting room. Even if the Spanish Workers' Statute allows under its Art 20(3) the employer to use different methods of control and surveillance, the Spanish Data Protection Act regulates the use of videocameras in the workplace. Its Art 89 allows for the use of videocameras, but specifically prohibits the recording of images of resting places for employees. Therefore, the controller illegally recorded such images, and hence violated Art 5(1)(c) GDPR, for processing inadequate and irrelevant personal data of its employees. The DPA suggested that, if they needed to record images of the door providing access to the room, they could either move the camera, so the angle was the appropriate one, either mask the part of the image that was filming the resting room, other than the door. The DPA fined the controller €20,000 for the violation of Art 5(1)(c) GDPR, reduced to €16,000 due to early payment. Additionally, the DPA found that the informative signs regarding the video cameras were not up-to-date, as they only mentioned the former Spanish Data Protection Act. The DPA considered that the controller had had enough time to update the signs since the publication and the entry into force of the GDPR, and that therefore the controller had violated Art12 GDPR, by not fulfilling their information obligations. The DPA fined the controller €6,000 for the violation of Art 12 GDPR, reduced to € 3,600 due to the recognition of responsibility and early payment.
AEPD (Spain) - PS/00389/2021	21 May 2021	The **Spanish DPA** fined € 1500 a bar for installing video surveillance cameras pointed towards a public street, violating the data minimisation principle under Art 5(1)(c) GDPR. The DPA stated that the installation of this type of device must be accompanied by a mandatory information sign, indicating the purposes and the person responsible for the processing of personal data, if applicable. In any case, the cameras must be oriented towards private areas, to avoid **intimidating neighbourhoods** with this type of device, as well as monitoring public transit areas without a justified cause. **The**

		DPA held that this type of device cannot be used to obtain images of public space, as this is the exclusive competence of the State Security Forces and Corps. The DPA considered that, in accordance with the evidence available in the procedure, the defendant had two video-surveillance cameras that affect a public traffic area without a justified reason. Therefore the DPA imposed a fine of € 1500 on LA OFICINA BAR for violating the data minimisation principle under Art 5(1)(c) GDPR.
APD/GBA (Belgium) - 57/2021	06 May 2021	The **Belgian DPA** states that a separate and clearly defined purpose is necessary for transfer to a third party. Multiple, different processing can take place for the same purpose, but each requires a legal basis. Legal basis of legitimate interest The defendant states that non-sensitive personal data can be processed based on legitimate interest for different purposes: - conducting computer tests; - monitoring the quality of service; - training of personnel; - monitoring and reporting; - storing recordings of video surveillance for the statutory period; and - compiling statistics from coded data, including big data. For each of these purposes, a balancing test was done. The DPA recites the requirements for relying on Art 6(1)(f), namely purpose test, necessity of the processing and a balancing test. As regards the first condition (the so-called "purpose test"), the DPA considers that the processing purpose as described by the Respondent must be considered as carried out in view of a legitimate interest. The interest pursued by the Respondent as the data controller can in itself be regarded as legitimate, in accordance with **recital 47** of the GDPR. In order to satisfy the second condition, it must be demonstrated that the processing is necessary for the achievement of the purposes pursued. This means checking whether the same result could be achieved by other means without processing personal data or without an unnecessarily intrusive processing for data subjects. In order to verify whether the third condition of Art 6(1)(f) - the so-called "balancing test" between the interests of the controller, on the one hand, and the fundamental freedoms and fundamental rights of the data subject, on the other hand - can be met, the reasonable expectations of the data subject must be taken into account in accordance with recital 47 GDPR. More specifically, it should be evaluated whether "*the data subject may reasonably expect, at the time and in the context of the collection of the personal data, that processing may take place for that purpose.*" Conducting computer tests

		The DPA holds that this satisfies the first, second and third criteria. It does state that the data subject could be more informed about the tests. Monitoring the quality of service and compiling statistics from coded data, including big data This topic has three parts: "statistics and quality tests", "satisfaction questionnaires" and "quality tests operations", each legitimate interest basis was assessed by the DPA: Statistics and quality tests All criteria have been fulfilled. Satisfaction questionnaires All criteria have been fulfilled. Quality tests operations All criteria have been fulfilled. Training of personnel The first criteria has been fulfilled. The necessity test has not been fulfilled, as it is not necessary to use client data in order to provide training cases for personnel, this is a breach of data minimisation of Article 5(1)(c). The balancing test is also not fulfilled as it is not within the reasonable expectations of a person taking an insurance for their information to be used as an example. Monitoring and reporting The first criteria have been fulfilled. The second criteria have been fulfilled as a minimum of data is necessary to fulfil legal obligations. Said legal obligations however, did not foresee in an explicit legal basis for the processing. The third criteria has also been fulfilled as it is a reasonable expectation of a data subject that the insurance company must fulfil its legal obligations. Storing recordings of video surveillance for the statutory period The first and second criteria have been fulfilled. The third criteria have not been fulfilled as a data subject signing an insurance contract cannot reasonably expect that their data will be used for video surveillance. This falls under the Camera law of 21 March 2007, including the obligation to put up pictograms to inform the data subjects. Model of balancing test The defendant states that all these balancing tests scored less than 30 on the model that they used, which means legitimate interest can be used as a legal basis. The DPA holds that this is purely instrumental, and no legal value can be given to a model. Legal basis for transfer to third parties The defendant claims that transfers to third parties is not a processing purpose, but a form of processing within the meaning of Article 4(2). The DPA states according to Article 5(1)(a), personal data must be processed for a specific purpose and the processing

		must be legitimate within the meaning of Article 6(1). It is possible to do multiple processing for the same purpose, but this must be done in compliance with the above. As the defendant is not able to state a specific and separate purpose for the transfer to a third party, and in light of the transparency principle within the meaning of Article 13(1)(c), there is a breach of the GDPR. Transparency principle Notwithstanding Art 13(1)(d) regarding transparency of its legitimate interests, the defendant claims that they fulfilled the requirements by merely stating in the privacy notice that the personal data will be processed based on its legitimate interest without indicating what those interests are. Those legitimate interest are not public as they contain company sensitive information and the documents are very 'heavy', not suited for a privacy notice. As the defendant is not able to state a specific and separate purpose for the transfer to a third party, and in light of the transparency principle within the meaning of Art 13(1)(d), there is a breach of the GDPR. And even if the defendant does not want to share sensitive information, they must at least provide more information to its data subjects in a clear and transparent way. Sharing company sensitive or 'heavy' documents on their own is not required for this. Based on the above, the first decision, and the appeal, the fine for the insurance company is reduced to €30.000 (from €50.000)
NAIH (Hungary) - NAIH-1006-3/2022	21 May 2021	The **Hungarian DPA** imposed a fine of approximately €1,300 on a car repair shop. The DPA held that the shop violated Art 5(1)(a) , 6 and 13 GDPR by failing to appropriately inform its employees about CCTV surveillance and for using it in areas intended for work breaks.
AEPD - PS/00151/2020	14 Apr 2021	The **Spanish DPA** fined a landlord € 3000 for violating Art 5(1)(c) and 13 GDPR in relation to a video surveillance system in an **apartment building**. The Spanish DPA considered that the surveillance system installed was violating the minimization principle: the fact that some of the apartments in the building are dedicated to tourist activities does not legitimize the recording of the common areas, unless by agreement of the board of owners. The DPA imposed therefore a fine of € 2000 for violation of Art 5(1)(c) GDPR. Regarding the obligation to provide information to the data subjects, as there is no informational poster that informs the people affected about the data processing, the identity of the controller and the possibility of exercising their rights, there is a clear breach of the duty of information as per article 13

		GDPR. The DPA imposed thus a fine of € 1000 for violating **Art** 13 GDPR.
ANSPDCP - S.C. Tip Top Food Industry S.R.L	14 Avr 2021	The **Romanian DPA** fined a company € 5000 (RON 24,362.50) for violating the data minimisation principle. The DPA held that CCTV surveillance in a workplace is excessive and does not respect the data minimisation principle when employees are recorded in spaces like cloakrooms or dining areas. Additionally, consent given by employees for such processing cannot be considered freely given. The DPA found that there has been a violation of Art 5(1)(b), 5(1)(c), 5(2), 6 and 7, considering that recording employees in spaces like cloakrooms, or dining areas was not necessary for the purpose pursued, and the same result could have been achieved through other measures less intrusive in the employees' private life. In addition, the DPA found that **consent cannot be considered a valid legal base in the context of the imbalanced relationship between employer-employee.** Consequently, the controller was not able to prove the lawfulness of the processing. Finally, a fine of RON 24.362,50 (approx €5000) was imposed, together with two corrective measures: - the controller must implement the data minimisation principle in its data processing activities; - the controller must adjust the monitored area in order to prevent surveilling the employees in the cloakrooms, or dining areas.
AEPD (Spain) - PS-00436-2021	21 Avr 2021	The **Spanish DPA** declined to sanction a local pub for failing to post signage warning of video surveillance. The pub's signs had been stolen and replaced at least three times, including once on the same day the complaint was filed. The DPA noted that, in cases of video surveillance, Art 22.4 LOPDGDD provides that the duty of disclosure in Art 12 GDPR may be fulfilled by placing a sign near surveillance cameras that identifies the existence of data processing, the identity of the controller, and the possibility of exercising the rights forseen in Art 15 to 22 GDPR. Failure to provide this information constitutes a "*serious infraction*" per Art 83.5 GDPR. However, the DPA held that the controller could not be sanctioned per Art 28.1 of Law 40/2015, of October 1, on the Regime Legal of the Public Sector (Responsibility), which requires that only parties responsible for an adminstrative infraction by way of fraud or negligence be subject to sanction. The DPA argued that because the controller had failed to comply only as a result of repeated acts of vandalism and had quickly acted to remedy the infraction after each incident, there was no fraud or negligence on the part of the controller.

NAIH (Hungary) - NAIH-3748-1/2021	25 Mar 2021	The **Hungarian DPA** held that CCTV monitoring is only necessary **when less intrusive measures are not available**. Further, the relevant data protection documentation (especially the privacy notice) must detail how the CCTV monitoring takes place and how the related recordings are processed by the controller. The holding of the DPA in this case was that the above reasons generally do not necessitate the operation of a CCTV system and that the operator monitored the performance of employees and the life of the occupants unlawfully. Disputes among occupants and concerning personnel could be settled with measures less invasive of the privacy and private life of data subjects. DPA also highlighted in this respect that payments could also be proven by written declaration instead of a CCTV recording and that in case of an accident or injury necessitating immediate assistance, analysing the recordings before acting would be unreasonable. DPA further suggested that the anti-corruption cause for monitoring the office of the head of the retirement home was too evasive (especially considering that the CCTV system did not record sound). In addition to the above, consent as a legal basis was not applicable, since the data subjects were not in a position to effectively give and withdraw consent. The data protection documentation concerning the CCTV system was also contradictory or missed certain details (i.e. the privacy notice did not specify the persons having the right to access the recordings or the exact data protection rights of the data subjects).
AEPD - PS/00191/2020	22 Feb 2021	The **Spanish DPA** imposed a fine of €2,000 against Ripobruna 207, S.L. (defendant) for the alleged violation of Article 5(1)(c) GDPR for the unauthorised use of two video surveillance cameras that also recorded parts of the public road without any justified cause. The original fine of €2,000 was reduced for voluntary payment to €1,600. The DPA held, that the actions of the defendant constitute an infringement of Article 5(1)(c) GDPR " Data Minimisation principle". The DPA further noted that: - Those responsible must ensure that the installed systems comply with current legislation, proving that it complies with all the requirements of the regulations in force. - The installation of this type of device must have the mandatory information notice, indicating the purposes and the responsible for the processing, where appropriate, of the personal data. - With reference to its Resolution R/00818/2012, the capture of images of public spaces by private surveillance cameras must be limited to what is strictly necessary, applying in any case the principle of proportionality. - Security cameras installed in private spaces will not be able to capture images of public spaces, the security function of

		public spaces corresponds exclusively to the State Security Forces and Bodies. The DPA imposed an initial fine of €2,000 which was reduced for voluntary payment to €1,600 in accordance with Article 85 (2) LPACAP).
AEPD - PS/00054/2020	19 Feb 2021	The **Spanish DPA** issued a warning sanction on a private individual for the installation of a video surveillance system without informing the subjects who may be recorded of the data processing, in violation of Article 13 and Article 5 (1) (c) GDPR. The DPA held that the video surveillance system was excessive in relation to the purposes alleged by the defendant. It issued a warning and ordered that the system should only be operational when the defendant or his family were living at the address where the camera was located. Given that the defendant is a natural person, that there is no evidence of recidivism and that, furthermore, he has shown cooperation with the DPA in repairing the possible damage caused, it was decided to impose a warning sanction.
IP - 07121-1/2021/563	22 Mar 2021	The **SLOVENIAN DPA** decided that covert video surveillance of employees is not permissible in any manner or under any circumstances. An employer first installed a surveillance camera in a visible place with markings, operated by the security service after requesting written consent of employees. The complainant however noticed another hidden camera. Employees must be informed in writing prior to the use of video surveillance within the work premises. The DPA reminded that in any case, employees cannot consent to video surveillance, as the basis for such video surveillance is in the law (Article 77 of ZVOP-1), but they must be informed in writing in advance, which legally restricts video surveillance of workplaces.
IP - 07121-1/2021/597	26 Mar 2021	The **Slovenian DPA** stated that video surveillance performed by an individual from his private facility or from his private property to the neighbour falls under the exception of "personal use". Therefore, the DPA has no jurisdiction under the GDPR as the processing of personal data for personal / domestic activity, except in the case when it also records public areas or space that is not owned by the individual who performs video surveillance.
Datatilsynet (Norway) - 20/01777	17 Mar 2021	The **Norwegian DPA** fined a controller € 3430 (NOK 35,000) for sharing a CCTV recording of a data subject vandalising its property with the data subject's employer, without a legal basis.

		he DPA held that the company lacked legal basis for the disclosure to the data subjects's employer and was therefore in violation of Articles 5(1)(a) and 6(1) GDPR. The recordings had already been handed over to the police and the further disclosure to the data subject's employer was unnecessary for the (legitimate) purpose of preventing vandalism or resolving the case.
HDPA (Greece) - 23/2021	17 Fev 2021	The **Greek DPA** fined an employer €15,000 for the illegal installation and operation of a video surveillance system. It held that a CCTV surveillance system is active and operational even if its camera feeds have been disabled via software, because these camera feeds can be easily reactivated without notification.
HDPA (Greece) - 12/2021	17 Fev 2021	The **Greek DPA** fined a controller € 2000 for violating **employees' rights** by using a surveillance camera at its premises without a legal basis, and in violation of the principle of data minimisation The DPA held that the use of the camera by the Company cannot be justified in the light of the principle of proportionality. The camera was not focused only on the entrance of the premises but instead it was watching as well the employee's offices, violating the principle of data minimization of the GDPR. Additionally, the fact that the director of the company was able to watch in real time at any time the images taken form the camera, could not justify the necessity and emergence of having a surveillance camera for security reasons. based on these facts the DPA imposed a fine of 2000€ to the company for violating articles 5(1)(c) and 6(1) GDPR.
LfD (Lower Saxony) - notebooksbilliger.de	08 Jan 2021	The **Landesbeauftragte für den Datenschutz (LfD) Niedersachsen (DPA of Lower Saxony, Germany**) fined notebooksbilliger.de € 10,4 million for **monitoring their employees over video without legal basis**. he LfD Niedersachsen reminded notebooksbilliger.de that a company must always **first consider milder means** than videos surveillance for purposes of crime prevention and solving. Moreover, a video surveillance to detect criminal acts would only have been lawful if there had been reasonable suspicion against specific persons, which was not given in this case. What would have been possible, was to monitor people for only a limited period of time. At notebooksbilliger.de, however, the video surveillance was neither limited to a specific period nor to specific employees. What's for the surveillance of customers, the LfD Niedersachsen considered the data subjects to have high interest worthy of protection, especially where they would spend longer periods of time to test the equipment. In that regard, the video surveillance was not proportionate.

		In consideration thereof, the LfD Niedersachsen fined notebooksbilliger.de €10,4 million, their highest fine issued so far under the applicability of the GDPR.
AEPD - PS/00253/2020	04 Jan 2021	The **Spanish DPA** imposed a fine of € 5,000 on the owner of a property that he rented out. The defendant had placed a video camera inside the rented property which went beyond filming the entrance as he claimed. This breached Article 5(1)(c) GDPR. The DPA held that the facts highlighted that there was a video surveillance camera installed in a rental property processing personal data without a reason or clear purpose. The DPA referred to Article 5(1)(c) GDPR on data minimisation. It also highlighted that it is for the individual in charge of camera to comply with the requirement of the law. The DPA held that when it comes to a property that is rented out (the object of a contract), the notion of personal of "purely personal or household activities" disappears. The owner of the property (that is rented to a third party), who is in charge of the video camera, must comply with the GDPR. The DPA went on to highlight a **Constitutional Court decision (nº 22/1984 (Rec.59/1983))** on the concept of a private home, which stated that this is a place where an individual can exercise their freedom more intimately, outside of social conventions. Therefore, the DPA concluded that the defendant processed personal data without just cause by filming the complainant inside their rented house. This was particularly because the video camera did not just record the entrance to scare burglars, but instead also filmed some other parts of the property. Therefore, the defendant breach Art 5(1)(c) GDPR.
Datatilsynet (Norway) - 20/01790	22 Dec 2020	The **Norwegian DPA** fined a company € 38,800 for **unlawfully disclosing** personal data from a surveillance footage, thus breaching Article 5(1)(a) GDPR and Article 6. The company appealed to the Norwegian Privacy Appeals Board, who first removed the fine in its entirety, then awarded the controller € 6,959 to cover their legal costs. The DPA notes that the company has legal grounds for using surveillance in their shop, in general, as per Art 6(1)(f). Filming and sharing a recording from the footage, however, is a new processing activity which also requires legal grounds as per the GDPR. The company has not determined legal grounds, as this processing activity shouldn't take place and is a breach of the company's internal routines. The DPA notes that the **purpose of the processing** was to identify the children in the footage. Sharing the footage with third parties, however, was not necessary to achive the purpose. The company should have reported the incident to the police and waited for them to initiate a criminal investigation, including asking for surveillance footage.

		Consequently, the DPA held that the company didn't have legal grounds for sharing the footage, as per Article 6. As the processing lacked legal basis, they were also in breach of Art 5(1)(a) GDPR.
Persónuvernd - 2020010548	17 Dec 2020	The **Icelandic DPA** ordered a resident of an apartment building to stop **monitoring other residents and public spaces** through CCTV cameras installed in the resident's apartment and car. The DPA concluded that the processing did not comply with the GDPR and ordered the resident to delete the footage. The DPA established that the processing of the personal data in question cannot be considered to concern only private interests of the responsible party or be intended for his personal use. According to the DPA, the responsible party had not demonstrated the imminent danger to him or his property or the need to monitor areas outside his own private property, ie. areas that belong to common property or are considered private property of other residents of the house. The DPA called the responsible party to refrain from all electronic monitoring which targets the common property and private property of other residents, delete all footage collected to this day and delete relevant content posted in social media.
Datainspektionen - DI-2020-4534	14 Dec 2020	The **Swedish DPA** held that it was not proportionate with regard to Art 6(1)(f) GDPR to conduct camera surveillance of all tenants in an apartment in order to investigate harassment and disturbances towards one tenant. The DPA held that Uppsalahem AB had processed personal data in breach of Article 6 (1) (f) GDPR by conducting camera surveillance of common areas in an apartment building.
NAIH - NAIH/2020/2729/15	14 Dec 2020	The **Hungarian DPA** imposed a fine of to € 2000 to a construction company close for excessive monitoring of property which allowed for the surveillance of employees without their knowledge. The DPA concluded that the video surveillance system installed by the company was unreasonable and that it failed to provide sufficient information about collection of personal data from its employees. The company was fined 700.000 HUF and instructed to change the angle of view of the camera so that it doesn't monitor workers' activities.
ANSPDCP - Warning issued to Bucharest Municipality (District 4)	11 Dec 2020	The **Romanian DPA** issued a warning against the Bucharest Municipality - District 4 as the General Directorate of 4th District Local Police breached Art 5(1)(a) and 6(1) GDPR. The warning was issued along with a corrective measure. The DPA found that the staff of the General Directorate of 4th District Local Police were hierarchically obliged to wear audio-video surveillance devices ("BADGE" type) during their working hours, without any legal provisions in force to

		govern the use of portable audio-video surveillance systems in the activity of local police officers. Therefore, the personal data (image and voice) were processed without a legal basis by using audio-video surveillance devices ("BADGE" type). The Romanian DPA issued the warning because the controller processed the personal data (image, voice) without fulfilling the legality conditions provided in Article 6(1) GDPR. In addition, the ANSPDCP applied a corrective measure through a remediation plan according to which the controller must ensure the compliance of the processing operations, performed by using the "BADGE" surveillance portable device, with the provisions of Art 5 and Art 6 GDPR.
Datainspektionen - DI-2019-7782	24 Nov 2020	The **Swedish DPA** held that the installation of CCTV cameras in an LSS home (housing with special services for adults) breached Art 5(1)(a) 6(1), 9(2), 13, 35 and 36 GDPR and Section 15 Camera Surveillance Act. The DPA imposed a fine of SEK 200,000 (approx. €19500).
APD/GBA - 74/2020	24 Nov 2020	The **Belgian DPA** imposed a fine of € 1500 on a private individual for the unlawful filming of public roads and private property of third parties with surveillance cameras, and for illegally sharing images taken from this system in breach of Article 6(1)(f) GDPR. There were legitimate interests for the defendants to install surveillance cameras to protect their own private property. But the way those surveillance cameras were positioned and the fact that they were constantly monitoring was not deemed necessary to safeguard those legitimate interests. The DPA such processing of personal data through the surveillance cameras to be overridden by the interests of the complainants and other data subjects while a one-off smartphone photograph, as a direct response to seeing an alleged offence, was seen as constituting a lawful processing within the meaning of Article 6(1)(f) of the GDPR.
APD/GBA - 73/2020	13 Nov 2020	The **Belgian DPA** imposed an administrative fine of € 1500 on a social housing company for breaching several fundamental principles and obligations of the GDPR. The DPA split the cases in several subtopics: - Privacy Policy & Right of Access - DPO - Cookie Policy - Processing of health data - Law on cameras - Processing through digital meters The DPA points out that, pursuant to Art 5(2) and Arti 24 GDPR, the person responsible for processing personal data must take appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the

		processing of personal data is carried out in accordance with the GDPR. In doing so, the GDPR requires, among other things, that the nature and scope of the processing as well as the risks for the data subjects are taken into account. These elements will play an important role in assessing whether and to what extent sanctions should be imposed. 1) **Privacy Policy & Right of Access** The DPA upheld that a privacy policy should serve to fully inform the data subject about what is actually done with his or her personal data and in what context those data are processed. Any processing of personal data should be lawful, proper and transparent. Data subjects should be clearly informed of what data is being processed, how the processing is being carried out and why the personal data is being processed. It is not possible to deduce from the Privacy Sheet presented what exactly the personal data is used for. Clear and concrete language must be used when communicating to data subjects. As the data subjects are socially disadvantaged people, the **language must be adapted** to them to be clear and plain. The word "concise" in Art 12(1) GDPR, however, does not mean incomplete, all mandatory information from Art 13 GDPR must still be included. The contact details of the DPO must be filled in correctly as well. The controller does not fulfil their requirement of transparency by inadequately informing the data subjects. **2) DPO** Pursuant to Art 37(5) GDPR, the DPO should be designated, inter alia, on the basis of their in data protection law and practice. Art 37(7) GDPR provides that the **contact details of the DPO** shall be disclosed and communicated to the supervisory authority. These two requirements were not fulfilled. The choice for the DPO was not sufficiently motivated (in light of a tender) and the DPO wasn't communicated to the data subject as a single point of contact. Furthermore, the **contact to the DPO must be direct**, and not through several parts of an organisation as this can dissuade people from contacting the DPO. Lastly, the DPO was not properly involved in all data protection manners, which means the controller breached Article 38(1) GDPR. **3) Cookie policy** For a Google-DoubleClick.net cookie, no consent was asked. In the Planet49 judgment, the Court of Justice ruled that information must be provided by the person responsible for processing in order to place cookies. The information provided must show for how long the cookies will remain active and whether third parties can also have access to those cookies. This is necessary in order to guarantee proper and transparent information.

		The consent requirement does not apply to the technical storage of information. Even if the placement of cookies is necessary for the provision of a service expressly requested by the subscriber or end user, the consent requirement does not apply. The processing of personal data through cookies without consent is a breach of Article 6(1) GDPR as there is no legal basis for the processing. **4) Processing of health data** The e-mail exchanges between the parties show that the data subject voluntarily informed the controller of his health situation and indicated that he could provide the controller with another medical certificate if necessary. The processing of sensitive information was necessary for purposes of Article 9(2)(h) GDPR. **5) CCTV surveillance** The data subject argues that there is camera surveillance **in several residential units of the apartment**. According to the data subject, the privacy policy does not mention anything about camera surveillance. The data subject also wants to know the legal basis and purpose of this processing. In the renting agreement, cameras are mentioned but nothing more. The cameras were installed for safety, on request of some residents and are legally registered. The DPA determined that it wasn't clear why the cameras were installed exactly nor do the elements brought up suffice to determine if the cameras are compliant to the the law on cameras. No **register of camera processing** was kept (article 6 § 2 Camera law) nor was the retention period of 30 days respected (article 6 § 3 Camera law). The DPA found a violation of the requirement to keep a register of processing activities of Article 30 GDPR and storage limitation Article 5(1)(e) GDPR. **6) Digital meters** The data subject complains that the controller uses digital consumption meters and thus records the consumption of the tenants and unlawfully processes data about that consumption without a valid legal basis. The data subject indicates that they had not given their consent to the processing of data relating to their consumption of gas and electricity. During the hearing, the controller indicated that the digital meters are linked to the address. In this way, it is read how much has been consumed at a certain address. This data is also passed on to a third party (local company) with whom there is a processing agreement. That company reads out the consumption. The controller receives a list of this and links it to the tenant files, according to the controller. On the basis of Article 6 GDPR, the person responsible for processing personal data must have a legal basis in order for the processing to be lawful. On the basis of Article

		24 and Art 25 GDPR, the controller must therefore take appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the processing takes place in accordance with the GDPR. In doing so, the data controller must effectively implement the principles of data protection, protect the rights of the data subjects and only process personal data that is necessary for each specific purpose of the processing. Based on these facts and documents, the DPA finds that the controller has not been able to demonstrate that any privacy policy has been developed with respect to the digital remote reading of meter readings. Moreover, it is unclear on what legal basis the data are processed in accordance with Art 6 GDPR. This constitutes a breach of Art 6 GDPR. The data subject indicates that they had not given permission for the processing. The controller does not invoke any other legal grounds for the processing. In addition, the DPA inds in this case a violation of Art 5(1)(a) GDPR now that it appears from the above that the personal data are not processed in a lawful, proper and transparent manner. The controller indicates that a third party reads out the consumption data and forwards them to the controller. The DPA points out that according to Art 28(3) GDPR the processing by a processor should be regulated in a contract between the controller and the processor. Sanction The DPA considers it particularly necessary in this case to give a strict interpretation to the (optional) exemption from administrative fines provided for in Article 83(7) for "government bodies and agencies". Moreover, the article does not allow Member States to define the concept of "public authorities and public bodies". It is therefore a concept of Union law that must be given an autonomous and uniform meaning. It is therefore only up to the Union institutions, in particular the Court of Justice, to define the limits of that concept. In the opinion of the DPA, a private law organization such as the controller's housing company does not fall under this category, even though this organization carries out tasks in the public interest in the field of social housing. On these grounds, the DPA orders the controller to become complaint within 3 months, to inform the DPA about this as well and to pay an administrative fine of €1500.