

# Guidelines



## **Guidelines 3/2019 on processing of personal data through video devices**

**關於以影像裝置運用個人資料之指引3/2019**

**Version 2.0**

**版本2.0**

**Adopted on 10 July 2019**

**2019年7月10日通過**

## Version history

### 版本更新歷程

Version 2.1 版本 2.1	26 February 2020 2020年2月26日	Amending material mistake 修正文字錯誤
Version 2.0 版本 2.0	29 January 2020 2020年1月29日	Adoption of the Guidelines after public consultation 公眾諮詢後通過本指引
Version 1.0 版本 1.0	10 July 2019 2019年7月10日	Adoption of the Guidelines for public consultation 通過本指引供公眾諮詢

## Table of contents

### 目錄

1	Introduction 導言 .....	6
2	Scope of application 適用範圍 .....	9
2.1	Personal Data 個人資料 .....	9
2.2	Application of the Law Enforcement Directive, LED (EU2016/680) 執法指令 (LED) (EU2016/680) 之適用 .....	10
2.3	Household exemption 家庭活動例外 .....	11
3	Lawfulness of processing 運用之合法性 .....	14
3.1	Legitimate interest, Article 6 (1) (f) 正當利益，第6條第1項第f款.....	15
3.1.1	Existence of legitimate interests 存在正當利益 .....	15
3.1.2	Necessity of processing 運用之必要性 .....	17
3.1.3	Balancing of interests 利益衡平 .....	20
3.2	Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e) 為執行符合公共利益之職務或行使公權力所必要，第6條第1 項第e款 .....	25
3.3	Consent, Article 6 (1) (a) 同意，第6條第1項第a款.....	26
4	Disclosure of video footage to third parties 向第三方揭露影片 .....	28
4.1	Disclosure of video footage to third parties in general 向第三方揭露影片概述.....	28
4.2	Disclosure of video footage to law enforcement agencies 向執法機關揭露影片 .....	29
5	Processing of special categories of data 運用特種個資 .....	32
5.1	General considerations when processing biometric data 運用生物特徵資料之一般考量 .....	34

5.2	Suggested measures to minimize the risks when processing biometric data	
	運用生物特徵資料時將風險降到最小之建議措施.....	42
6	Rights of the data subject 當事人的權利.....	45
6.1	Right to access 近用權.....	45
6.2	Right to erasure and right to object 刪除權和拒絕權.....	48
6.2.1	Right to erasure (Right to be forgotten)	
	刪除權（被遺忘權）.....	48
6.2.2	Right to object 拒絕權.....	51
7	Transparency and information obligations	
	透明化和資訊提供義務.....	53
7.1	First layer information (warning sign)	
	第一層資訊（警示標誌）.....	54
7.1.1	Positioning of the warning sign 警示標誌之放置方式	54
7.1.2	Content of the first layer 第一層內容.....	55
7.2	Second layer information 第二層資訊.....	57
8	Storage periods and obligation to erasure	
	儲存期間和刪除義務.....	59
9	Technical and organisational measures	
	技術性和組織性措施.....	61
9.1	Overview of video surveillance system	
	影像監控系統概述.....	61
9.2	Data protection by design and by default	
	資料保護之設計和預設.....	64
9.3	Concrete examples of relevant measures	
	相關措施的具體示例.....	65
9.3.1	Organisational measures 組織性措施.....	67
9.3.2	Technical measures 技術性措施.....	68
10	Data protection impact assessment 個資保護影響評估.....	71

## The European Data Protection Board

Having regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

### HAS ADOPTED THE FOLLOWING GUIDELINES

#### 歐盟個人資料保護委員會

依據歐洲議會與歐盟理事會於2016年4月27日通過之「關於運用\*個人資料時對自然人之保護與確保此等資料之自由流通，以及廢除指令95/46/EC的歐盟規則2016/679/EU」（下稱GDPR）第70條第1項第e款；

依據歐洲經濟區聯合委員會於2018年7月6日第154/2018號決定修改之歐洲經濟區（EEA）協議，尤其是附件11及其議定書37<sup>1</sup>；

依據「歐盟個人資料保護委員會議事規則」第12條和第22條；

#### 通過以下指引：

---

\* 譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing譯為「運用」，processor譯為「受託運用者」。

<sup>1</sup> References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

本意見所稱之「會員國」應理解為「EEA會員國」。

## 1 INTRODUCTION

### 導言

1. The intensive use of video devices has an impact on citizen's behaviour. Significant implementation of such tools in many spheres of the individuals' life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed. Data protection implications are massive.

影像裝置的密集使用影響了公民之行為。此等工具在個人生活之諸多領域大量裝設，將使人需要防範別人探知其可能被視為異常之行為，從而給個人造成額外壓力。事實上，這些技術可能限制匿名行動和匿名使用服務之可能性，且會普遍限制保持不被注意狀態之可能性。這對於資料保護有深遠影響。

2. While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse. The general principles in GDPR (Article 5), should always be carefully considered when dealing with video surveillance.

雖然個人或許能夠接受錄影監控，例如為某些安全目的所裝設，仍必須採取保障措施，避免不當用於完全不同且（對於當事人而言）意料之外之目的（例如行銷目的、監控員工表現等）。此外，當前所裝設的諸多工具，係為利用所拍攝的畫面，並將傳統相機轉化為智慧相機。影像所生成之諸多資料，結合這些工具和技術，使得次級使用（secondary usage）（無論與系統設置之原始目的是否相關）、乃至不當使用之風險升高。處理影像監控議題時，應始終仔細考量GDPR之一般原則（第5條）。

3. Video surveillance systems in many ways change the way professionals

from the private and public sector interact in private or public places for the purpose of enhancing security, obtaining audience analysis, delivering personalized advertising, etc. Video surveillance has become high performing through the growing implementation of intelligent video analysis. These techniques can be more intrusive (e.g. complex biometric technologies) or less intrusive (e.g. simple counting algorithms). Remaining anonymous and preserving one's privacy is in general increasingly difficult. The data protection issues raised in each situation may differ, so will the legal analysis when using one or the other of these technologies.

影像監控系統在諸多方面改變了公私部門的專業人員為增進安全、獲取對象分析、投放個人化廣告等目的，在公私場所之互動。智慧影像分析逐漸普及，影像監控的性能也隨之提高。這些技術的干預性可能較高（例如複雜生物辨識技術），也可能較低（例如簡單計數演算法）。整體觀之，維持匿名和保護個人隱私越來越困難。各種情況下所涉及之資料保護議題可能不同，因此使用這些不同技術時的法律分析也存在差異。

4. In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it's identifying. Algorithms would perform based on different demographics, thus, bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided.

除隱私議題外，還可能存在裝置功能異常和引發偏見之風險。研究者發現，用於臉部識別、辨識或分析之軟體，其表現因被辨識者的年齡、性別和種族不同而有差異。演算法之表現依其分析之對象不同而有差異，因此，臉部辨識偏見可能加劇社會歧視。正是因此，對於影像監控衍生之生物特徵資料運用，資料控管者必須確保定期評估其相關性與保障措施充足性。

5. Video surveillance is not by default a necessity when there are other

means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset.

存在實現基本目的之其他方法時，影像監控未必是預設方案。否則，我們將面臨文化規範轉變，導致對缺乏隱私普遍接受之風險。

6. These guidelines aim at giving guidance on how to apply the GDPR in relation to processing personal data through video devices. The examples are not exhaustive, the general reasoning can be applied to all potential areas of use.

本指引目的係對GDPR如何適用於以影像裝置運用個人資料提供指導。相關示例並非完全列舉，其一般論理可適用於一切潛在之使用領域。



## 2 SCOPE OF APPLICATION<sup>2</sup>

### 適用範圍<sup>2</sup>

#### 2.1 Personal Data

##### 個人資料

7. Systematic automated monitoring of a specific space by optical or audio-visual means, mostly for property protection purposes, or to protect individual's life and health, has become a significant phenomenon of our days. This activity brings about collection and retention of pictorial or audio-visual information on all persons entering the monitored space that are identifiable on basis of their looks or other specific elements. Identity of these persons may be established on grounds of these details. It also enables further processing of personal data as to the persons' presence and behaviour in the given space. The potential risk of misuse of these data grows in relation to the dimension of the monitored space as well as to the number of persons frequenting the space. This fact is reflected by the General Data Protection Regulation in the Article 35 (3) (c) which requires the carrying out of a data protection impact assessment in case of a systematic monitoring of a publicly accessible area on a large scale, as well as in Article 37 (1) (b) which requires processors to designate a data protection officer, if the processing operation by its nature entails regular and systematic monitoring of data subjects.

主要為保護財產目的、或為保護個人生命和健康，以光學或影音手段系統性、自動化地監控特定空間，已成為日常生活中的重要現象。此一活動蒐集和保留進入該受監控空間的一切人員的圖像或影音資訊，且相關人員可基於其外表或其他特定要素而被識別。基於這些詳細資訊，可能確定這些人員之身分。這也使得相關人員在特定空間出現及其行為的個人資料可被進階運用。受監控空間的面積越大、經常出入該空間的人數越多，不當使用這些資料之風險也越高。GDPR第35條第3項第c款反映這一事實，要求對於公眾開放區域進行大規模、系統性之監控時，須辦理個資保護影響評估；第37條第1項

---

<sup>2</sup> The EDPB notes that where the GDPR so allows, specific requirements in national legislation might apply.

EDPB注意到，在GDPR許可的情況下，可能適用國家立法中的特定要求。

第b款也反應這一事實，要求受託運用者在運用作業本質需要經常性、系統性監控當事人時，指派個資保護長。

8. However, the Regulation does not apply to processing of data that has no reference to a person, e.g. if an individual cannot be identified, directly or indirectly.

然而，「規則」並不適用於與個人無關的資料運用活動，例如無法直接或間接識別個人之情況。

9.

Example: The GDPR is not applicable for fake cameras (i.e. any camera that is not functioning as a camera and thereby is not processing any personal data). However, in some Member States it might be subject to other legislation.

示例：GDPR並不適用於假的相機（亦即，無法發揮功能且因此不運用任何個人資料的相機）。然而，這在某些會員國可能受其他法律規範。

Example: Recordings from a high altitude only fall under the scope of the GDPR if under the circumstances the data processed can be related to a specific person.

示例：高空拍攝只有在其運用的資料關聯到特定個人時，方落入GDPR之適用範圍。

Example: A video camera is integrated in a car for providing parking assistance. If the camera is constructed or adjusted in such a way that it does not collect any information relating to a natural person (such as licence plates or information which could identify passers-by) the GDPR does not apply.

示例：汽車上裝設錄影鏡頭，以協助停車。若依該相機的裝設或調整方式，並不蒐集與自然人相關之任何資訊（例如車牌或可識別路人之資訊），則不適用GDPR。

## 2.2 Application of the Law Enforcement Directive, LED (EU2016/680) 執法指令（LED）（EU2016/680）之適用

10. Notably processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of

criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, falls under the directive EU2016/680.

值得注意的是，權責機關為預防、調查、偵查或起訴犯罪或執行刑罰（包括因應和防範公共安全威脅）而運用個人資料之行為，適用指令EU2016/680。

## 2.3 Household exemption

### 家庭活動例外

11. Pursuant to Article 2 (2) (c), the processing of personal data by a natural person in the course of a purely personal or household activity, which can also include online activity, is out of the scope of the GDPR.<sup>3</sup>

依第2條第2項第c款，自然人在單純個人或家庭活動過程中運用個人資料之行為(有可能包含線上活動)，在GDPR的適用範圍外<sup>3</sup>。

12. This provision – the so-called household exemption – in the context of video surveillance must be narrowly construed. Hence, as considered by the European Court of Justice, the so called “household exemption” must *“be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people”*.<sup>4</sup> Furthermore, if a video surveillance system, to the extent it involves the constant recording and storage of personal data and covers, *“even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely ‘personal or household’ activity for the purposes of the second indent of Article 3(2) of Directive 95/46”*<sup>5</sup>.

在影像監控方面，本條—即所謂的家庭活動例外—須作狹義解釋。因此，正如歐洲法院之見解，所謂的「家庭活動例外」必須「解釋為僅與個人之私人或家庭生活過程中實施之活動相關，若在網路上公開資料、使之可為不特定多數人存取，此等個人資料運用活動顯

---

<sup>3</sup> See also Recital 18.  
另見前言第18點。

然非屬此類」<sup>4</sup>。此外，若影像監控系統經常性地錄製與儲存個人資料，且「（即使僅部分地）包含公共空間，並因此脫離個人運用資料之私人背景，則其不得被視為指令95/46第3條第2項第二點所規定的之單純『個人或家庭』活動」<sup>5</sup>。

13. What regards video devices operated inside a private person's premises, it may fall under the household exemption. It will depend on several factors, which all have to be considered in order to reach a conclusion. Besides the above mentioned elements identified by ECJ rulings, the user of video surveillance at home needs to look at whether he has some kind of personal relationship with the data subject, whether the scale or frequency of the surveillance suggests some kind of professional activity on his side, and of the surveillance's potential adverse impact on the data subjects. The presence of any single one of the aforementioned elements does not necessarily suggest that the processing is outside the scope of the household exemption, an overall assessment is needed for that determination.

至於在個人之私人處所內部運作之影像裝置，則可能落入家庭活動例外範圍內。這取決於數項要素，須全部予以考慮後方可得出結論。除上述歐洲法院（ECJ）確定的要素外，家庭影像監控的使用者需檢視其與當事人間是否存在某種私人關係，監控的規模與頻率是否意味著其在從事某種職業活動，以及監控對當事人的潛在不利影響。存在前述任何要素之一，並不必然意味著運用不屬於家庭活動例外，得出此一結論需進行整體評估。

- 14.

**Example:** A tourist is recording videos both through his mobile phone and through a camcorder to document his holidays. He shows the footage to friends and family but does not make it accessible for an indefinite number of people. This would fall under the household

<sup>4</sup> European Court of Justice, Judgment in Case C-101/01, *Bodil Lindqvist case*, 6th November 2003, para 47.

歐洲法院，第C-101/01號案件（*Bodil Lindqvist*案）判決，2003年11月6日，第47段。

<sup>5</sup> European Court of Justice, Judgment in Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33.

歐洲法院，第C-212/13號案件（*František Ryneš v Úřad pro ochranu osobních údajů*）判決，2014年12月11日，第33段。

exemption.

示例：一名遊客同時使用其手機和錄影機記錄其假期。他讓朋友和家人觀看該影片，但並未將其提供給不特定多數人。這將適用家庭活動例外。

Example: A downhill mountain biker wants to record her descent with an actioncam. She is riding in a remote area and only plans to use the recordings for her personal entertainment at home. This would fall under the household exemption even if to some extent personal data is processed.

示例：一名下坡山地車手想要以運動攝影機攝錄其下坡過程。她在偏遠地區騎行，且計劃將所錄影片僅用於在家私人欣賞。即使在某種程度上運用個人資料，這也屬於家庭活動例外。

Example: Somebody is monitoring and recording his own garden. The property is fenced and only the controller himself and his family are entering the garden on a regular basis. This would fall under the household exemption, provided that the video surveillance does not extend even partially to a public space or neighbouring property.

示例：某人對其自己的花園進行監控錄影。該花園裝有圍欄，且僅有控管者及其家人會經常進出。若該影像監控並不（即使部分地）延伸至公共空間或鄰近地產，亦屬於家庭活動例外。

### 3 LAWFULNESS OF PROCESSING

#### 運用之合法性

15. Before use, the purposes of processing have to be specified in detail (Article 5 (1) (b)). Video surveillance can serve many purposes, e.g. supporting the protection of property and other assets, supporting the protection of life and physical integrity of individuals, collecting evidence for civil claims.<sup>6</sup> These monitoring purposes should be documented in writing (Article 5 (2)) and need to be specified for every surveillance camera in use. Cameras that are used for the same purpose by a single controller can be documented together. Furthermore, data subjects must be informed of the purpose(s) of the processing in accordance with Article 13 (see section 7, *Transparency and information obligations*). Video surveillance based on the mere purpose of “safety” or “for your safety” is not sufficiently specific (Article 5 (1) (b)). It is furthermore contrary to the principle that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (see Article 5 (1) (a)).

在使用前，須特定運用之目的（第5條第1項第b款）。影像監控可用於諸多目的，例如支援財產和其他資產之保全、支援個人生命和人身安全之保護、為民事主張蒐集證據等<sup>6</sup>。應書面記錄這些監控目的（第5條第2項），且對所使用的每個監控攝影機均應特定其目的。同一控管者為同樣目的使用之多個攝影機得合併紀錄。此外，須依第13條（見第7節，透明化和資訊提供義務）向當事人告知運用之目的。僅以「安全」或「為你的安全」作為影像監控之目的，並不夠具體特定（第5條第1項第b款）。這還違反資料運用應以合法、公平合理且對當事人以透明之方式為之的原則（見第5條第1項第a款）。

16. In principle, every legal ground under Article 6 (1) can provide a legal basis for processing video surveillance data. For example, Article 6 (1) (c) applies where national law stipulates an obligation to carry out video surveillance.<sup>7</sup> However in practice, the provisions most likely to be used are

原則上，第6條第1項規定的各款法律依據皆可作為運用影像監控資

---

<sup>6</sup> Rules on collecting evidence for civil claims varies in Member States. 會員國關於民事主張的蒐證規則存在差異。

料之依據。例如，國內法規定實施影像監控之義務時，適用第6條第1項第c款<sup>7</sup>。但實務中，最可能使用的條款為：

- Article 6 (1) (f) (legitimate interest),  
第6條第1項第f款（正當利益），
- Article 6 (1) (e) (necessity to perform a task carried out in the public interest or in the exercise of official authority).  
第6條第1項第e款（為執行符合公共利益之職務或行使公權力所必要）。

In rather exceptional cases Article 6 (1) (a) (consent) might be used as a legal basis by the controller.

在相當例外的情形下，控管者可能以第6條第1項第a款（同意）為法律依據。

### 3.1 Legitimate interest, Article 6 (1) (f)

正當利益，第6條第1項第f款

17. The legal assessment of Article 6 (1) (f) should be based on the following criteria in compliance with Recital 47.

第6條第1項第f款之法律評估應依據前言第47點，基於下列標準實施。

#### 3.1.1 Existence of legitimate interests

存在正當利益

18. Video surveillance is lawful if it is necessary in order to meet the purpose of a legitimate interest pursued by a controller or a third party, unless such interests are overridden by the data subject's interests or fundamental rights and freedoms (Article 6 (1) (f)). Legitimate interests pursued by a controller or a third party can be legal,<sup>8</sup> economic or non-material interests.<sup>9</sup> However, the controller should consider that if the data subject objects to the surveillance in accordance with Article 21 the controller can only proceed with the video surveillance of that data subject if it is a compelling legitimate interest which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

---

<sup>7</sup> These guidelines do not analyse or go into details of national law that might differ between Member States.

本指引並不分析或深入討論國內法，各會員國的國內法可能不同。

若影像監控係為了滿足控管者或第三方所追求之正當利益目的所必要，則監控為合法，除非其利益被當事人之利益或基本權利與自由所超越（第6條第1項第f款）。控管者或第三方所追求之正當利益可能為法律上<sup>8</sup>、經濟上或非財物利益<sup>9</sup>。然而，控管者應考慮，若當事人依第21條拒絕監控，則控管者僅得在下列情形實施影像監控：存在超越當事人利益、權利和自由之必要正當利益，或為建立、行使或防禦法律上之請求。

19. Given a real and hazardous situation, the purpose to protect property against burglary, theft or vandalism can constitute a legitimate interest for video surveillance.

於存在真實危險之情形下，保護財產免受非法入室、竊盜、故意破壞之目的，得構成影像監控之正當利益。

20. The legitimate interest needs to be of real existence and has to be a present issue (i.e. it must not be fictional or speculative)<sup>10</sup>. A real-life situation of distress needs to be at hand – such as damages or serious incidents in the past – before starting the surveillance. In light of the principle of accountability, controllers would be well advised to document relevant incidents (date, manner, financial loss) and related criminal charges. Those documented incidents can be a strong evidence for the existence of a legitimate interest. The existence of a legitimate interest as well as the necessity of the monitoring should be reassessed in periodic intervals (e. g. once a year, depending on the circumstances).

正當利益需真實存在，且須為現存之問題（即不得為假想或猜測）<sup>10</sup>。在開始監控前，需現實存在迫切危難—例如損害或過去發生的嚴重事故。依課責性原則，建議控管者宜記錄相關事故（日期、方式、經濟損失）和相關刑事控告。所記錄的事故可作為存在正當利益的有力證據。應定期重新評估是否存在正當利益和監控必要性（例如根據情形每年一次）。

---

<sup>8</sup> European Court of Justice, Judgment in Case C-13/16, *Rīgas satiksme case*, 4 may 2017.

歐洲法院，第C-13/16號案件（*Rīgas satiksme*案）判決，2017年5月4日。

<sup>9</sup> see wp 217, Article 29 Working Party.

見wp217，第29條工作小組。

<sup>10</sup> see wp 217, Article 29 Working Party, p. 24 seq. See also ECJ Case C-708/18 p.44

見wp217，第29條工作小組，第24頁以下。另見歐洲法院第C-708/18號案件，第44段（譯註：原文第44頁應為誤植）。



21.

Example: A shop owner wants to open a new shop and wants to install a video surveillance system to prevent vandalism. He can show, by presenting statistics, that there is a high expectation of vandalism in the near neighbourhood. Also, experience from neighbouring shops is useful. It is not necessary that a damage to the controller in question must have occurred. As long as damages in the neighbourhood suggest a danger or similar, and thus can be an indication of a legitimate interest. It is however not sufficient to present national or general crime statistic without analysing the area in question or the dangers for this specific shop.

示例：一名店主希望開設一間新店，且想要裝設影像監控系統以防範故意破壞行為。其可通過展示統計數據，論證其鄰近地區故意破壞行為的可能性很高。此外，附近商店的經驗也是有用的。該控管者並不一定已受損失。只要鄰近地區的損失已表明存在危險或類似事由，即可作為正當利益之表徵。然而，若僅提出全國性或一般性的犯罪統計數據，而未分析相關地區或該特定商店面臨的危險，則並不足夠。

22. Imminent danger situations may constitute a legitimate interest, such as banks or shops selling precious goods (e.g. jewellers), or areas that are known to be typical crime scenes for property offences (e. g. petrol stations).

迫切危險情形可構成正當利益，比如銀行或銷售貴重商品（例如珠寶）之商店，或公認的財產犯罪常見地點（例如加油站）。

23. The GDPR also clearly states that public authorities cannot rely their processing on the grounds of legitimate interest, as long as they are carrying out their tasks, Article 6 (1) sentence 2.

GDPR第6條第1項第2句還明確規定，公務機關在執行公務時，不得援用正當利益作為運用之依據。

### 3.1.2 Necessity of processing

#### 運用之必要性

24. Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data

minimisation'), see Article 5 (1) (c). Before installing a video-surveillance system the controller should always critically examine if this measure is firstly suitable to attain the desired goal, and secondly adequate and necessary for its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means which are less intrusive to the fundamental rights and freedoms of the data subject.

個人資料應適當、相關且限於其運用目的所必要（「資料最小化」），見第5條第1項第c款。在裝設影像監控系統前，控管者首先應總是審慎檢視此一措施是否適合實現所預期目的，其次對其目的是否適當且必要。唯有對當事人之基本權利與自由干預性較低之其他措施無法合理實現運用之目的時，方得選擇影像監控措施。

25. Given the situation that a controller wants to prevent property related crimes, instead of installing a video surveillance system the controller could also take alternative security measures such as fencing the property, installing regular patrols of security personnel, using gatekeepers, providing better lighting, installing security locks, tamper-proof windows and doors or applying anti-graffiti coating or foils to walls. Those measures can be as effective as video surveillance systems against burglary, theft and vandalism. The controller has to assess on a case-by-case basis whether such measures can be a reasonable solution.

在防範財產犯罪的情境中，控管者可能不裝設影像監控系統，而是採取替代性安全措施，例如對財產架設圍欄、由保全人員定期巡視、設置門衛、提供更佳照明、安裝安全鎖和防盜門窗，或對牆壁使用防塗鴉塗層或貼膜。在防範非法入室、竊盜、故意破壞財物方面，這些措施與影像監控系統同樣有效。控管者必須對個案評估這些措施是否為合理解決方案。

26. Before operating a camera system, the controller is obliged to assess where and when video surveillance measures are strictly necessary. Usually a surveillance system operating at night-time as well as outside the regular working hours will meet the needs of the controller to prevent any dangers to his property.

在運作錄影系統前，控管者有義務評估影像監控系統在何時及何地有絕對必要性。通常，在夜間和正常工作時間外運作之監控系統將

滿足控管者防範財產損害危險之需求。

27. In general, the necessity to use video surveillance to protect the controllers' premises ends at the property boundaries<sup>11</sup> However, there are cases where the surveillance of the property is not sufficient for an effective protection. In some individual cases it might be necessary to exceed the video surveillance to the immediate surroundings of the premises. In this context, the controller should consider physical and technical means, for example blocking out or pixelating not relevant areas.

一般而言，使用影像監控保護控管者處所的必要性止於其財產的邊界<sup>11</sup>。然而，某些情形下，對財產的監控並不足以提供有效保護。某些個別情形下，可能有必要將影像監控擴張到場所密切相鄰之範圍。此時，控管者應考慮實體（physical）與技術方法，例如遮蔽不相關區域或打馬賽克（pixelate）。

28.

Example: A bookshop wants to protect its premises against vandalism. In general, cameras should only be filming the premises itself because it is not necessary to watch neighbouring premises or public areas in the surrounding of the bookshop premises for that purpose.

示例：一家書店想要防範對其經營場所的故意破壞活動。一般而言，攝影機應僅攝錄該經營場所本身，因為此一目的不需要監控附近其他場所或該書店周邊的公共空間。

29. Questions concerning the processing's necessity also arise regarding the way evidence is preserved. In some cases it might be necessary to use black box solutions where the footage is automatically deleted after a certain storage period and only accessed in case of an incident. In other situations, it might not be necessary to record the video material at all but more appropriate to use real-time monitoring instead. The decision between black box solutions and real-time monitoring should also be based on the purpose pursued. If for example the purpose of video surveillance is the preservation of evidence, real-time methods are usually not suitable. Sometimes real-time monitoring may also be more

---

<sup>11</sup> This might also be subject to national legislation in some Member States.  
在某些會員國，這可能也受國內立法規範。

intrusive than storing and automatically deleting material after a limited timeframe (e. g. if someone is constantly viewing the monitor it might be more intrusive than if there is no monitor at all and material is directly stored in a black box). The data minimisation principle must be regarded in this context (Article 5 (1) (c)). It should also be kept in mind that it might be possible that the controller could use security personnel instead of video surveillance that are able to react and intervene immediately.

證據的保存方式也可能引發運用的必要性問題。某些情形下，可能有必要運用黑箱（black box）方案，即影片於保存一定期間後自動刪除，且僅於發生事故時才被存取。其他情形下，可能根本不必錄影，而是更適合進行即時監控。在黑箱方案與即時監控間選擇何者，亦應基於所追求的目的決定。例如，若影像監控的目的係保存證據，即時方案則通常不適合。有時，較之於儲存有限期間後自動刪除影片，即時監控可能干預性更高（例如，相較於完全沒有顯示器、影片直接儲存在黑箱中，有人不斷觀看顯示器的干預性可能更高）。此種情形下必須遵守資料最小化原則（第5條第1項第c款）。還應謹記，控管者可能不使用影像監控，而是使用能夠直接採取因應與干預措施的保全人員。

### 3.1.3 Balancing of interests

#### 利益衡平

30. Presuming that video surveillance is necessary to protect the legitimate interests of a controller, a video surveillance system may only be put in operation, if the legitimate interests of the controller or those of a third party (e.g. protection of property or physical integrity) are not overridden by the interests or fundamental rights and freedoms of the data subject. The controller needs to consider 1) to what extent the monitoring affects interests, fundamental rights and freedoms of individuals and 2) if this causes violations or negative consequences with regard to the data subject's rights. In fact, balancing the interests is mandatory. Fundamental rights and freedoms on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully.

假設影像監控是保護控管者正當利益的必要措施，則唯有控管者或

第三方的正當利益（例如保護財產或人身安全）未被當事人之利益或基本權利與自由超越時，方可啟用影像監控系統。控管者需要考慮：1) 監控在多大程度上影響個人之利益、基本權利與自由；以及2) 是否侵害當事人之權利或有不利影響。事實上，利益衡平是強制要求。必須審慎評估和衡平基本權利與自由，以及控管者的正當利益。

31.

Example: A private parking company has documented reoccurring problems with thefts in the cars parked. The parking area is an open space and can be easily accessed by anyone, but is clearly marked with signs and road blockers surrounding the space. The parking company have a legitimate interest (preventing thefts in the customer's cars) to monitor the area during the time of day that they are experiencing problems. Data subjects are monitored in a limited timeframe, they are not in the area for recreational purposes and it is also in their own interest that thefts are prevented. The interest of the data subjects not to be monitored is in this case overridden by the controller's legitimate interest.

示例：一家私有停車場公司已記錄反復發生的車內竊盜事故。該停車場為開放空間，任何人都可輕易進入，但該停車場有明確標誌，周圍設有路障。該停車場公司在發生問題的時段內，對監控該空間有正當利益（防範對客戶之車內竊盜行為）。當事人在有限時段內受監控，他們並非為娛樂目的進入該區域，防範竊盜亦符合他們自己的利益。此時，控管者的正當利益超越當事人不受監控的利益。

Example: A restaurant decides to install video cameras in the restrooms to control the tidiness of the sanitary facilities. In this case the rights of the data subjects clearly overrides the interest of the controller, therefore cameras cannot be installed there.

示例：一家餐館決定在洗手間裝設攝影機，以確保衛生設備的整潔。此時，當事人之權利顯然超越控管者的利益，因此不得在此裝設攝影機。

### 3.1.3.1 Making case-by-case decisions

#### 進行個案判斷

32. As the balancing of interests is mandatory according to the regulation, the decision has to be made on a case-by-case basis (see Article 6 (1) (f)). Referencing abstract situations or comparing similar cases to one another is insufficient. The controller has to evaluate the risks of the intrusion of the data subject's rights; here the decisive criterion is the intensity of intervention for the rights and freedoms of the individual.

由於「規則」強制要求利益衡平，必須進行個案判斷（見第6條第1項第f款）。援用抽象情形或類比相似案例並不足夠。控管者必須評估干預當事人權利之風險；此處的判斷標準是對該個人權利與自由之干預強度。

33. Intensity can *inter alia* be defined by the type of information that is gathered (information content), the scope (information density, spatial and geographical extent), the number of data subjects concerned, either as a specific number or as a proportion of the relevant population, the situation in question, the actual interests of the group of data subjects, alternative means, as well as by the nature and scope of the data assessment.

強度可尤其（*inter alia*）以如下要素界定：所蒐集資訊之類型（資訊內容），範圍（資訊密度、空間與地理範圍），所涉當事人之數量（具體數目或在相關人群中所佔比例），所涉具體情況，當事人群體之真實利益，替代方法，以及資料評估之性質與範圍。

34. Important balancing factors can be the size of the area, which is under surveillance and the amount of data subjects under surveillance. The use of video surveillance in a remote area (e.g. to watch wildlife or to protect critical infrastructure such as a privately owned radio antenna) has to be assessed differently than video surveillance in a pedestrian zone or a shopping mall.

重要的衡平要素可能是：受監控區域的面積，以及受監控當事人之數目。在偏遠地區使用影像監控（例如觀察野生動物，或保護私有無線電天線等關鍵基礎設施）之評估，必須有別於在行人徒步區或購物中心實施影像監控之評估。

35.

Example: If a dash cam is installed (e. g. for the purpose of collecting evidence in case of an accident), it is important to ensure that this camera is not constantly recording traffic, as well as persons who are near a road. Otherwise the interest in having video recordings as evidence in the more theoretical case of a road accident cannot justify this serious interference with data subjects' rights.<sup>11\*\*</sup>

示例：若已安裝行車記錄器（例如為事故蒐證目的），重要的是確保該記錄器不會持續攝錄交通以及路邊人員。否則，在道路事故之假想情況下以錄影為證據的利益，不得作為嚴重干預當事人權利之正當理由<sup>11\*\*</sup>。

### 3.1.3.2 *Data subjects' reasonable expectations*

#### *當事人之合理期待*

36. According to Recital 47, the existence of a legitimate interest needs careful assessment. Here the reasonable expectations of the data subject at the time and in the context of the processing of its personal data have to be included. Concerning systematic monitoring, the relationship between data subject and controller may vary significantly and may affect what reasonable expectations the data subject might have. The interpretation of the concept of reasonable expectations should not only be based on the subjective expectations in question. Rather, the decisive criterion has to be if an objective third party could reasonably expect and conclude to be subject to monitoring in this specific situation.

依前言第47點，正當利益是否存在需要審慎評估。此時，必須納入當事人在其個資運用當時之合理期待。關於系統性監控，當事人和控管者間的關係可能有重大區別，並可能影響當事人所抱持的合理期待。合理期待這一概念的解釋不應僅基於所涉當事人的主觀期待。相反，決定性標準應是客觀第三方在該特定情形下，可否合理期待並決定受監控。

37. For instance, an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer.<sup>12</sup> Furthermore, monitoring is not to be expected in one's private garden, in living areas,

or in examination and treatment rooms. In the same vein, it is not reasonable to expect monitoring in sanitary or sauna facilities – monitoring such areas is an intense intrusion into the rights of the data subject. The reasonable expectations of data subjects are that no video surveillance will take place in those areas. On the other hand, the customer of a bank might expect that he/she is monitored inside the bank or by the ATM.

例如，大部分情況下，員工不期待在其工作場所被僱主監控<sup>12</sup>。此外，在私人花園、起居場所，或診察或治療室，也不期待被監控。同樣地，衛生或桑拿設施中受監控之期待並不合理—監控這些區域係對當事人權利之重大干預。當事人合理期待這些區域不會進行影像監控。另一方面，銀行的客戶可能期待其在銀行內部或ATM中被監控。

38. Data subjects can also expect to be free of monitoring within publicly accessible areas especially if those areas are typically used for recovery, regeneration, and leisure activities as well as in places where individuals stay and/or communicate, such as sitting areas, tables in restaurants, parks, cinemas and fitness facilities. Here the interests or rights and freedoms of the data subject will often override the controller's legitimate interests.

當事人還可能期待在公眾開放區域不受監控，特別是當這些區域通常用於恢復、放鬆與休閒活動，以及個人逗留和（或）交流之場所，例如休息區、餐廳的餐桌、公園、電影院和健身設備。此時，當事人之利益或權利與自由通常超越控管者的正當利益。

39.

**Example:** In toilets data subjects expect not to be monitored. Video surveillance for example to prevent accidents is not proportional.

**示例：**當事人期待在廁所裡不受監控。為防範事故等目的實施影像監控不合比例。

40. Signs informing the data subject about the video surveillance have no

\*\*譯註：原文此處註11無內容，應為誤植。

<sup>12</sup> See also: Article 29 Working Party, Opinion 2/2017 on data processing at work, WP249, adopted on 8 June 2017.

另見：第29條工作小組，關於職業環境的資料運用之意見2/2017（WP249），2017年6月8日通過。



relevance when determining what a data subject objectively can expect. This means that e.g. a shop owner cannot rely on customers objectively having reasonable expectations to be monitored just because a sign informs the individual at the entrance about the surveillance.

在確定當事人的客觀期待時，設立告示牌告知當事人存在影像監控並非相關要素。這意味著，例如，店主不能僅基於入口處設有告示牌告知人們存在監控，即主張顧客客觀期待受監控。

### 3.2 Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e)

為執行符合公共利益之職務或控管者受託行使公權力所必要，  
第6條第1項第e款

41. Personal data could be processed through video surveillance under Article 6 (1) (e) if it is necessary to perform a task carried out in the public interest or in the exercise of official authority.<sup>13</sup> It may be that the exercise of official authority does not allow for such processing, but other legislative bases such as “health and safety” for the protection of visitors and employees may provide limited scope for processing, while still having regard for GDPR obligations and data subject rights.

為執行符合公共利益之職務或行使公權力所必要時，得依據第6條第1項第e款以影像監控運用個人資料<sup>13</sup>。可能的情形是，行使公權力並不允許此等運用，但其他法律依據，例如保護來訪者和員工的「健康和 safety」，可能允許有限範圍之運用，而仍遵守GDPR義務和當事人權利。

42. Member States may maintain or introduce specific national legislation for video surveillance to adapt the application of the rules of the GDPR by determining more precisely specific requirements for processing as long as it is in accordance with the principles laid down by the GDPR (e.g. storage limitation, proportionality).

會員國得為影像監控維持或提出特定國家立法，在符合GDPR所定原

---

<sup>13</sup> The basis for the processing referred shall be laid down by Union law or Member State law» and «shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (3)).

此一運用依據應由歐盟法律或會員國法律規定，「且」係為執行符合公共利益之職務或行使控管者已被賦予之公權力所必要（第6條第3項）。

則（例如儲存限制、比例原則）的前提下，更精確地確定運用之具體要求，調整GDPR規則之適用。

### 3.3 Consent, Article 6 (1) (a) 同意，第6條第1項第a款

43. Consent has to be freely given, specific, informed and unambiguous as described in the guidelines on consent.<sup>14</sup>

如同意指引所述，同意必須自主給予、特定、知情且非模糊<sup>14</sup>。

44. Regarding systematic monitoring, the data subject's consent can only serve as a legal basis in accordance with Article 7 (see Recital 43) in exceptional cases. It is in the surveillance's nature that this technology monitors an unknown number of people at once. The controller will hardly be able to prove that the data subject has given consent prior to processing of its personal data (Article 7 (1)). Assumed that the data subject withdraws its consent it will be difficult for the controller to prove that personal data is no longer processed (Article 7 (3)).

關於系統性監控，僅有在符合第7條的特殊情形下（見前言第43點），方可援用當事人的同意作為法律依據。依監控之本質，該技術同時監控不特定數目之人。控管者將幾乎無法證明當事人在其個資被運用前已給予同意（第7條第1項）。假設當事人撤回同意，控管者將很難證明不再運用該個資（第7條第3項）。

- 45.

**Example:** Athletes may request monitoring during individual exercises in order to analyse their techniques and performance. On the other hand, where a sports club takes the initiative to monitor a whole team for the same purpose, consent will often not be valid, as the individual athletes may feel pressured into giving consent so that their refusal of consent does not adversely affect teammates.

**示例：**運動員可能要求監控個人訓練，以便分析其技巧與表現。另一方面，若運動俱樂部為同樣目的對整支隊伍實施監控，則同意通常是無效的，因為運動員個人可能覺得不得不給予同意，以免拒絕

<sup>14</sup> In addition, the Article 29 Working Party (Art. 29 WP) adopted „Guidelines on consent under Regulation 2016/679“ (WP 259 rev. 01). - endorsed by the EDPB

此外，第29條工作小組（Art. 29 WP）通過了「關於第2016/679號規則（GDPR）中的同意之指引」（WP 259 rev. 01），EDPB採認。

同意對隊友造成不利影響。

46. If the controller wishes to rely on consent it is his duty to make sure that every data subject who enters the area which is under video surveillance has given her or his consent. This consent has to meet the conditions of Article 7. Entering a marked monitored area (e.g. people are invited to go through a specific hallway or gate to enter a monitored area), does not constitute a statement or a clear affirmative action needed for consent, unless it meets the criteria of Article 4 and 7 as described in the guidelines on consent.<sup>15</sup>

若控管者想要援引同意，則其有責任確保進入該區域的每個當事人皆給予同意<sup>15</sup>。此等同意必須符合第7條規定之條件。除非滿足同意指引所論述的第4條和第7條之標準，否則進入標示為受監控之區域（例如，人們受邀通過特定走廊或大門進入受監控區域），並不構成同意所必需之聲明或「清楚肯定行為」。

47. Given the imbalance of power between employers and employees, in most cases employers should not rely on consent when processing personal data, as it is unlikely to be freely given. The guidelines on consent should be taken into consideration in this context.

考量到僱主和員工間權利不對等，大部分情形下，僱主不應援引同意運用個人資料，因為同意不太可能係自主給予。此時，應考慮同意指引的內容。

48. Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context (see Article 88).

會員國法律或團體協約，包括「工會協約」，可能為僱傭關係中運用員工之個人資料規定具體規則（見第88條）。

---

<sup>15</sup> In addition, the Article 29 Working Party (Art. 29 WP) adopted „Guidelines on consent under Regulation 2016/679“ (WP 259) - endorsed by the EDPB - which should be taken in account.

此外，還應考慮第29條工作小組（Art. 29 WP）通過之「關於第2016/679號規則（GDPR）中的同意之指引」（WP 259 rev. 01），EDPB採認。

## 4 DISCLOSURE OF VIDEO FOOTAGE TO THIRD PARTIES

### 向第三方揭露影片

49. In principle, the general regulations of the GDPR apply to the disclosure of video recordings to third parties.

原則上，GDPR之一般規則適用於向第三方揭露影片。

#### 4.1 Disclosure of video footage to third parties in general

##### 向第三方揭露影片概述

50. Disclosure is defined in Article 4 (2) as transmission (e.g. individual communication), dissemination (e.g. publishing online) or otherwise making available. Third parties are defined in Article 4 (10). Where disclosure is made to third countries or international organisations, the special provisions of Article 44 et seq. also apply.

第4條第2款將揭露定義為傳輸（例如個人通訊）、散播（例如線上公開）或以其他方式提供。第4條第10款定義了第三方。向第三國或國際組織揭露時，還適用第44條以下的特殊規定。

51. Any disclosure of personal data is a separate kind of processing of personal data for which the controller needs to have a legal basis in Article 6.

任何揭露個資的行為都是對個資的獨立運用，控管者需要具備第6條規定的法律依據。

52.

Example: A controller who wishes to upload a recording to the Internet needs to rely on a legal basis for that processing, for instance by obtaining consent from the data subject according to Article 6 (1) (a).

示例：控管者想要將影片上傳至網路，需要對此運用援引法律依據，例如依第6條第1項第a款獲得當事人同意。

53. The transmission of video footage to third parties for the purpose other than that for which the data has been collected is possible under the rules of Article 6 (4).

依第6條第4項，得為不同於該資料蒐集之原始目的的其他目的，向第三方傳輸影片。

54.

Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. A damage occurs and the recording is transferred to a lawyer to pursue a case. In this case the purpose for recording is the same as the one for transferring.

示例：為處理故意破壞行為之目的，對（停車場）路障裝設影像監控。破壞行為發生後，影片被交予律師進行求償。此時錄影之目的與移轉影片之目的相同。

Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. The recording is published online for pure amusement reasons. In this case the purpose has changed and is not compatible with the initial purpose. It would furthermore be problematic to identify a legal basis for that processing (publishing).

示例：為處理故意破壞行為之目的，對（停車場）路障裝設影像監控。該影片為單純娛樂目的被公開於網路。此時，目的已改變，與原始目的不符。識別此一運用（公開）之法律依據進而成為問題。

55. A third party recipient will have to make its own legal analysis, in particular identifying its legal basis under Article 6 for his processing (e.g. receiving the material).

第三方接收者本身必須進行法律分析，特別是依第6條識別其運用（例如接收該影片）之法律依據。

#### 4.2 Disclosure of video footage to law enforcement agencies

##### 向執法機關揭露影片

56. The disclosure of video recordings to law enforcement agencies is also an independent process, which requires a separate justification for the controller.

向執法機關揭露影片也是一項獨立運用，控管者對此另行需要正當理由。

57. According to Article 6 (1) (c), processing is legal if it is necessary for compliance with a legal obligation to which the controller is subject. Although the applicable police law is an affair under the sole control of the Member States, there are most likely general rules that regulate the transfer of evidence to law enforcement agencies in every Member State. The processing of the controller handing over the data is regulated by

the GDPR. If national legislation requires the controller to cooperate with law enforcement (e. g. investigation), the legal basis for handing over the data is legal obligation under Article 6 (1) (c).

依據第6條第1項第c款，運用若係履行控管者負有的法定義務所必要，則為合法。雖然可適用的警察法為會員國自主管轄之事務，每個會員國很可能設有規範向執法機關移交證據之一般規則。控管者交出資料之運用行為受GDPR規範。若國家立法要求控管者配合執法（例如調查），則交出資料之法律依據為第6條第1項第c款之法定義務。

58. The purpose limitation in Article 6 (4) is then often unproblematic, since the disclosure explicitly goes back to Member State law. A consideration of the special requirements for a change of purpose in the sense of lit. a - e is therefore not necessary.

此時，由於揭露明確回歸到會員國法律，第6條第4項規定的目的限制通常不會有問題。因此無需考慮第a款至第e款關於變更目的之特殊要求。

59.

Example: A shop owner records footage at its entrance. The footage shows a person stealing another person's wallet. The police asks the controller to hand over the material in order to assist in their investigation. In that case the shop owner would use the legal basis under Article 6 (1) (c) (legal obligation) read in conjunction with the relevant national law for the transfer processing.

示例：一名店主在入口處錄影。影片顯示一個人在偷竊他人錢包。警方要求控管者交出影片，以協助其調查。此時，控管者對此移交運用行為，得使用第6條第1項第c款（法定義務）連結相關國內法為法律依據。

60.

Example: A camera is installed in a shop for security reasons. The shop owner believes he has recorded something suspicious in his footage and decides to send the material to the police (without any indication that there is an ongoing investigation of some kind). In this case the shop owner has to assess whether the conditions under, in most cases, Article 6 (1) (f) are met. This is usually the case if the shop owner has a

reasonable suspicion of that a crime has been committed.

示例：一家商店為安全原因裝設攝影機。店主認為其錄到了可疑行為，並將影片發送給警方（而無跡象表明正在進行某種調查）。此時，大部分情形下，店主須評估是否符合第6條第1項第f款規定之條件。若店主合理懷疑已實施犯罪，則通常屬於此情形。

61. The processing of the personal data by the law enforcement agencies themselves does not follow the GDPR (see Article 2 (2) (d)), but follows instead the Law Enforcement Directive (EU2016/680).

執法機關本身對個人資料之運用不適用GDPR（見第2條第2項第d款），而是適用執法指令（EU2016/680）。

## 5 PROCESSING OF SPECIAL CATEGORIES OF DATA

### 運用特種個資

62. Video surveillance systems usually collect massive amounts of personal data which may reveal data of a highly personal nature and even special categories of data. Indeed, apparently non-significant data originally collected through video can be used to infer other information to achieve a different purpose (e.g. to map an individual's habits). However, video surveillance is not always considered to be processing of special categories of personal data.

影像監控系統通常蒐集巨量的個人資料，且可能揭示高度私人性質之資料，甚至特種個資。事實上，影片初始蒐集看似不重要的資料可能用以推斷實現不同目的的其他資訊（例如剖繪個人習慣）。然而，影像監控並非總是構成對特種個資的運用。

63.

Example: Video footage showing a data subject wearing glasses or using a wheel chair are not per se considered to be special categories of personal data.

示例：影片顯示當事人戴眼鏡或使用輪椅並不當然屬於特種個資。

64. However, if the video footage is processed to deduce special categories of data Article 9 applies.

然而，若影片被用於推斷特種個資，則適用第9條。

65.

Example: Political opinions could for example be deduced from images showing identifiable data subjects taking part in an event, engaging in a strike, etc. This would fall under Article 9.

示例：從可得識別之當事人出席活動、參加罷工等畫面，可推知其政治立場。這將適用第9條。

Example: A hospital installing a video camera in order to monitor a patient's health condition would be considered as processing of special categories of personal data (Article 9).

示例：醫院裝設攝影機，以監控病患的健康狀況，這構成運用特種個資（第9條）。

66. In general, as a principle, whenever installing a video surveillance system



careful consideration should be given to the data minimization principle. Hence, even in cases where Article 9 (1) does not apply, the data controller should always try to minimize the risk of capturing footage revealing other sensitive data (beyond Article 9), regardless of the aim.

一般而言，作為一項原則，在裝設影像監控系統時，均應審慎考慮資料最小化原則。因此，即使在不適用第9條第1項的情況下，無論其目的如何，資料控管者應總是盡力降低影片揭示（第9條之外的）其他敏感資料之風險。

67.

Example: Video surveillance capturing a church does not per se fall under Article 9. However, the controller has to conduct an especially careful assessment under Article 6 (1) (f) taken into account the nature of the data as well as the risk of capturing other sensitive data (beyond Article 9) when assessing the interests of the data subject.

示例：對教堂的影像監控並不當然適用第9條。然而，控管者在評估當事人的利益時，必須考量資料之性質與拍攝到（第9條之外的）其他敏感資料之風險，依第6條第1項第f款進行審慎評估。

68. If a video surveillance system is used in order to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 (i.e. an exemption from the general rule that one should not process special categories of data) and a legal basis under Article 6.

若影像監控系統係用於運用特種個資，資料控管者必須同時識別第9條規定的運用特種個資之例外（亦即，不得運用特種個資之一般原則的例外），以及第6條規定之法律依據。

69. For instance, Article 9 (2) (c) (“[...] *processing is necessary to protect the vital interests of the data subject or of another natural person [...]*”) could – in theory and exceptionally – be used, but the data controller would have to justify it as an absolute necessity to safeguard the vital interests of a person and prove that this “[...] data subject *is physically or legally incapable of giving his consent.*”. In addition, the data controller won’t be allowed to use the system for any other reason.

例如，第9條第2項第c款（「……運用係為保護當事人或其他自然人之重大利益所必要……」）能夠—理論上且例外地—用於此處，但

資料控管者必須論證此為保護相關人員重大利益之絕對必要，且證明「……當事人身體上或法律上無法給予同意……」。此外，資料控管者不得為其他理由使用此系統。

70. It is important to note here that every exemption listed in Article 9 is not likely to be usable to justify processing of special categories of data through video surveillance. More specifically, data controllers processing those data in the context of video surveillance cannot rely on Article 9 (2) (e), which allows processing that relates to personal data that are manifestly made public by the data subject. The mere fact of entering into the range of the camera does not imply that the data subject intends to make public special categories of data relating to him or her.

重要的是，此處應注意，第9條所列各項例外不太可能被用作以影像監控運用特種個資的正當理由。具體而言，資料控管者以錄影監控運用此類資料，不得援用第9條第2項第e款，該款允許運用當事人明顯已自行公開之資料。進入攝影機攝錄範圍的單純事實並不意味著當事人有意公開其特種個資。

71. Furthermore, processing of special categories of data requires a heightened and continued vigilance to certain obligations; for example high level of security and data protection impact assessment where necessary.

此外，運用特種個資需要對特定義務有更高程度及持續的警覺；例如高度安全保護、必要時辦理個資保護影響評估。

72.

**Example:** An employer must not use video surveillance recordings showing a demonstration in order to identify strikers.

**示例：**僱主不得使用罷工遊行之監控錄影識別罷工者。

### 5.1 General considerations when processing biometric data

#### 運用生物特徵資料之一般考量

73. The use of biometric data and in particular facial recognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as

particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.

使用生物特徵資料，特別是臉部辨識，將提高當事人權利之風險。關鍵是在援用此類技術時，充分尊重GDPR所規定的合法性、必要性、合乎比例和資料最小化等原則。儘管使用此等技術可能被認為特別有效，控管者應首先評估對基本權利與自由之影響，並考慮以干預性較低的手段實現其運用之正當目的。

74. To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of this characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is “[...] *resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person [...]*”. The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual.<sup>16</sup>

構成GDPR所定義的生物特徵資料的條件為，對於原始資料（例如自然人的身體、生理或行為特徵）的運用，必須隱含對此等特徵之評量。由於生物特徵資料係這種評量之結果，GDPR在第4條第14款規定，其係「……對自然人身體、生理或行為特徵之特定技術運用，以實現或確認對該自然人的獨特性識別……」。然而，若未將某一個人之影片作特定技術運用，以協助識別該個人，則該影片本身不構成第9條規定的生物特徵資料<sup>16</sup>。

75. In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed “for the purpose of uniquely identifying a natural person”.

---

<sup>16</sup> Recital 51 supports this analysis, stating that “[...] *The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. [...]*”.

前言第51點支持這一分析，認為「……運用照片不應一概被視為運用特種個資，因為只有在運用係以特定技術方法為之，且能夠獨特性識別或認證某一自然人時，其才落入生物特徵資料的定義範圍……」。

構成運用特種個資（第9條）之條件為，係「為獨特性識別自然人目的」而運用生物特徵資料。

76. To sum up, in light of Article 4.14 and 9, three criteria must be considered:

概言之，依第4條第14款和第9條，必須考量三項標準：

- **Nature of data** : data relating to physical, physiological or behavioural characteristics of a natural person,  
資料性質：資料係關於自然人的身體、生理或行為特徵，
- **Means and way of processing** : data “resulting from a specific technical processing”,  
運用方法和方式：資料係「特定技術運用之結果」，
- **Purpose of processing**: data must be used for the purpose of uniquely identifying a natural person.  
運用目的：資料必須以用於獨特性識別自然人為目的。

77. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require explicit consent from all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable.

私人實體為其本身目的（例如行銷、統計，甚至保全），運用其所裝設的包含生物特徵辨識功能的影像監控裝置，將在大部分情況下需要全部當事人之明確同意（第9條第2項第a款），而第9條規定的其他適當例外也可能適用。

78.

Example: To improve its service a private company replaces passenger identification check points within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure. Since the processing falls under Article 9, the passengers, who will have previously given their explicit and informed consent, will have to enlist themselves at for example an automatic terminal in order to create and register their facial template associated with their boarding pass and identity. The check points with facial recognition need

to be clearly separated, e. g. the system must be installed within a gantry so that the biometric templates of non-consenting person will not be captured. Only the passengers, who will have previously given their consent and proceeded with their enrolment, will use the gantry equipped with the biometric system.

示例：為提升服務，一家私人公司以影像監控系統代替了機場內旅客身分查驗點（托運行李、登機），對於同意這一作業的旅客，運用臉部辨識技術查驗其身分。由於此等運用適用第9條，旅客須事先給予明確知情同意後，必須主動前往自動終端等設施，創設並登錄與其登機證和身分相關之臉部模板。臉部識別查驗點應作明確區分，例如，該系統應裝設門架（gantry），以免拍攝未給予同意人員的生物辨識模板。唯有已給予同意並進行登錄的旅客將使用裝設生物辨識系統的門架。

Example: A controller manages access to his building using a facial recognition method. People can only use this way of access if they have given their explicitly informed consent (according to Article 9 (2) (a)) beforehand. However, in order to ensure that no one who has not previously given his or her consent is captured, the facial recognition method should be triggered by the data subject himself, for instance by pushing a button. To ensure the lawfulness of the processing, the controller must always offer an alternative way to access the building, without biometric processing, such as badges or keys.

示例：一名控管者使用臉部辨識方法進行門禁管理。唯有事前給予明確知情同意（依第9條第2項第a款）的人員方可使用此通行方式。然而，為確保避免拍攝未事先同意之人，該臉部辨識方法應由當事人自己啟動，例如通過按鈕等方式。為確保運用之合法性，控管者必須隨時提供不涉及生物特種運用的替代通行方式，例如門卡或鑰匙。

79. In this type of cases, where biometric templates are generated, controllers shall ensure that once a match or no-match result has been obtained, all the intermediate templates made on the fly (with the explicit and informed consent of the data subject) in order to be compared to the ones created by the data subjects at the time of the enlistment, are immediately and securely deleted. The templates

created for the enlistment should only be retained for the realisation of the purpose of the processing and should not be stored or archived.

此類案例中，若生成生物特徵模板，在獲得匹配或不匹配之結果後，對於為了與當事人加入系統時創設的模版相比對而製作的臨時模版（經當事人明確知情同意），控管者應確保立即以安全方式將其刪除。加入系統時創設之模版，其保存期間應以實現運用目的為限，而不得被儲存或建檔。

80. However, when the purpose of the processing is for example to distinguish one category of people from another but not to uniquely identify anyone the processing does not fall under Article 9.

然而，若運用是為了區分某一類人等目的，而非獨特性識別某個人，則其不適用第9條。

81.

Example: A shop owner would like to customize its advertisement based on gender and age characteristics of the customer captured by a video surveillance system. If that system does not generate biometric templates in order to uniquely identify persons but instead just detects those physical characteristics in order to classify the person then the processing would not fall under Article 9 (as long as no other types of special categories of data are being processed).

示例：一名店主想要根據影像監控系統攝錄到的顧客性別和年齡特徵客製其廣告。若該系統並不生成用以獨特性識別個人的生物特徵模板，而是為客群分類目的偵測此等生理特徵，則其運用不適用第9條（在不運用其他特種個資的前提下）。

82. However, Article 9 applies if the controller stores biometric data (most commonly through templates that are created by the extraction of key features from the raw form of biometric data (e.g. facial measurements from an image)) in order to uniquely identify a person. If a controller wishes to detect a data subject re-entering the area or entering another area (for example in order to project continued customized advertisement), the purpose would then be to uniquely identify a natural person, meaning that the operation would from the start fall under Article 9. This could be the case if a controller stores generated templates to provide further tailored advertisement on several

billboards throughout different locations inside the shop. Since the system is using physical characteristics to detect specific individuals coming back in the range of the camera (like the visitors of a shopping mall) and tracking them, it would constitute a biometric identification method because it is aimed at recognition through the use of specific technical processing.

然而，若控管者為獨特性識別個人而儲存生物特徵資料（通常是從原始形式的生物特徵資料（例如圖像中的臉部測量值）中提取出關鍵特徵並創設模板），則適用第9條。若控管者想要偵測一名當事人重新進入該區域或進入其他區域（例如，為了持續投放客製化廣告目的），則其目的係獨特性識別自然人，意味著此等作業自始即適用第9條。若控管者儲存所生成的模板，以便在店內不同位置的數個廣告牌上投放客製化程度更高的廣告，即屬於此情形。由於該系統係運用生理特徵偵測特定個人返回攝像機的攝錄範圍內（比如進入賣場之人）並追蹤該個人，則將構成生物特徵辨識方法，因為其目的在於透過特定技術運用進行識別。

83.

Example: A shop owner has installed a facial recognition system inside his shop in order to customize its advertisement towards individuals. The data controller has to obtain the explicit and informed consent of all data subjects before using this biometric system and delivering tailored advertisement. The system would be unlawful if it captures visitors or passers-by who have not consented to the creation of their biometric template, even if their template is deleted within the shortest possible period. Indeed, these temporary templates constitute biometric data processed in order to uniquely identify a person who may not want to receive targeted advertisement.

示例：一名店主在其店內安裝臉部辨識系統，以便向特定個人投放客製化廣告。資料控管者必須在使用這一生物特徵系統並投放客製化廣告前，獲得全部當事人之明確知情同意。若該系統拍攝到尚未給予同意的訪客或路人，並製作其生物特徵模板，則即使在極短時間內刪除該模板，亦不合法。實際上，這些臨時模板構成為獨特性識別個人而運用之生物特徵資料，而被識別之個人可能不願意接收定向廣告。

84. The EDPB observes that some biometric systems are installed in uncontrolled environments<sup>17</sup>, which means that the system involves capturing on the fly the faces of any individual passing in the range of the camera, including persons who have not consented to the biometric device, and thereby creating biometric templates. These templates are compared to the ones created of data subjects having given their prior consent during an enlistment process (i.e. a biometric device user) in order for the data controller to recognise whether the person is a biometric device user or not. In this case, the system is often designed to discriminate the individuals it wants to recognize from a database from those who are not enlisted. Since the purpose is to uniquely identify natural persons, an exception under Article 9 (2) GDPR is still needed for anyone captured by the camera.

EDPB觀察到，某些生物特徵系統裝設於不受控之環境<sup>17</sup>，這意味著該系統涉及一併拍攝進入攝影機範圍內的任何個人（包括尚未同意生物特徵裝置之人）之臉部，並創設其生物特徵模板。這些模板與已事先同意之當事人加入系統時（亦即生物特徵裝置使用者）所創設的模板相比對，從而使資料控管者識別其是否為生物特徵裝置使用者。此時，系統通常設計為區分想從資料庫被識別之人與尚未加入系統之人。由於其目的是獨特性識別自然人，對於攝影機拍攝到的任何人，都仍需要援用GDPR第9條第2項規定的例外。

85.

Example: A hotel uses video surveillance to automatically alert the hotel manager that a VIP has arrived when the face of the guest is recognized. These VIPs have priory given their explicit consent to the use of facial recognition before being recorded in a database established for that purpose. These processing systems of biometric data would be unlawful unless all other guests monitored (in order to identify the VIPs) have consented to the processing according to Article 9 (2) (a) GDPR.

<sup>17</sup> It means that the biometric device is located in a space open to the public and is able to work on anyone passing by, as opposed to the biometric systems in controlled environments that can be used only by consenting person's participation.

意指生物特徵裝置放置於公眾開放空間內，且能夠對任何路過之人使用，而不是位於受控環境中，僅對同意參與之人使用。



示例：一家旅館使用影像監控系統，在臉部辨識出VIP客人後，自動提示旅館經理一位VIP客人已抵達。這些VIP客人在其錄入相關資料庫前，已對臉部辨識給予事先明確同意。除非（為識別VIP客人而）受監控的其他客人全都依GDPR第9條第2項第a款同意此運用，否則該生物特徵資料運用系統並不合法。

Example: A controller installs a video surveillance system with facial recognition at the entrance of the concert hall he manages. The controller must set up clearly separated entrances; one with a biometric system and one without (where you instead for example scan a ticket). The entrances equipped with biometric devices, must be installed and made accessible in a way that prevents the system from capturing biometric templates of non-consenting spectators.

示例：一名控管者在其管理的音樂廳入口處裝設附有臉部辨識功能的影像監控系統。該控管者必須設置彼此明確區隔的不同入口，一個設有生物特徵系統，另一個則沒有（通過掃描票券等方式入場）。設有生物特徵系統的入口的裝設與提供方式，必須避免該系統拍攝未同意觀眾之生物特徵模板。

86. Finally, when the consent is required by Article 9 GDPR, the data controller shall not condition the access to its services to the acceptance of the biometric processing. In other words and notably when the biometric processing is used for authentication purpose, the data controller must offer an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject. This alternative solution is also needed for persons who do not meet the constraints of the biometric device (enrolment or reading of the biometric data impossible, disability situation making it difficult to use, etc.) and in anticipation of unavailability of the biometric device (such as a malfunction of the device), a "back-up solution" must be implemented to ensure continuity of the proposed service, limited however to exceptional use. In exceptional cases, there might be a situation where processing biometric data is the core activity of a service provided by contract, e.g. a museum that sets up an exhibition to demonstrate the use of a facial recognition device, in which case the data subject will not be able to reject the processing of biometric data should they wish to participate in the exhibition. In such case the

consent required under Article 9 is still valid if the requirements in Article 7 are met.

最後，當依GDPR第9條要求獲得同意，資料控管者不得將接受生物特徵運用作為獲取其服務之前提條件。換言之，特別是當為認證目的運用生物特徵時，資料控管者必須提供不涉及生物特徵運用之替代方案—而不得限制當事人或增加其成本。對於未符合生物特徵裝置限制條件之人（無法登錄或讀取生物特徵資料，因身心障礙而難以使用等），以及預料生物特徵裝置不可用的情形（如裝置故障），亦應提供替代方案。必須設置「備選方案」，以確保所涉服務之持續性，雖然其僅限於例外使用。在例外情形下，運用生物特徵資料可能係依契約提供之服務的核心活動，例如，博物館籌備一項展覽，展示臉部辨識裝置之使用，此時，若當事人想要參與該展覽，則不得拒絕運用生物特徵資料。此時，若符合第7條的要求，則第9條規定的同意仍為有效。

## 5.2 Suggested measures to minimize the risks when processing biometric data

### 運用生物特徵資料時將風險降到最小之建議措施

87. In compliance with the data minimization principle, data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing. Measures should be put in place to guarantee that templates cannot be transferred across biometric systems.

依資料最小化原則，資料控管者必須確保，為構建模板而從數位圖像中提取之資料不得過度，且僅包含為該特定目的所必需之資訊，從而避免任何潛在的進階運用。應採取措施確保模板無法在生物特徵系統間移轉。

88. Identification and authentication/verification are likely to require the storage of the template for use in a later comparison. The data controller must consider the most appropriate location for storage of the data. In an environment under control (delimited hallways or checkpoints), templates shall be stored on an individual device kept by the user and under his or her sole control (in a smartphone or the id card) or – when needed for specific purposes and in presence of objective

needs – stored in a centralized database in an encrypted form with a key/secret solely in the hands of the person to prevent unauthorised access to the template or storage location. If the data controller cannot avoid having access to the templates, he must take appropriate steps to ensure the security of the data stored. This may include encrypting the template using a cryptographic algorithm.

識別和認證/驗證可能要求儲存模板，以便用於後續比對。資料控管者必須考量儲存資料最適當的位置。在可控環境下（限定走道或查驗點），模板應儲存於由使用者保管且單獨控制的獨立裝置（智慧型手機或身分識別證）上，或者—當特定目的需要如此，且存在客觀需求時—以加密形式儲存在集中式資料庫中，且密鑰/加密僅由該人保管，以免未經授權存取模板或儲存位置。若資料控管者不得不存取模板，其必須採取適當步驟確保所儲存資料之安全。這可能包括使用加密演算法為模板加密。

89. In any case, the controller shall take all necessary precautions to preserve the availability, integrity and confidentiality of the data processed. To this end, the controller shall notably take the following measures: compartmentalize data during transmission and storage, store biometric templates and raw data or identity data on distinct databases, encrypt biometric data, notably biometric templates, and define a policy for encryption and key management, integrate an organisational and technical measure for fraud detection, associate an integrity code with the data (for example signature or hash) and prohibit any external access to the biometric data. Such measures will need to evolve with the advancement of technologies.

無論如何，控管者應採取一切必要預防措施，保護所運用資料的可用性、完整性與機密性。為此目的，控管者尤其應採取下列措施：在傳輸與儲存過程中劃分（compartmentalize）資料，將生物特徵模板與原始資料或身分資料儲存於不同資料庫中，加密生物特徵資料（特別是生物特徵模板），定義加密與密鑰管理政策，整合詐欺偵測之組織性和技術性措施，結合資料完整性編碼（例如簽名或雜湊值（hash）），以及禁止外部存取生物特徵資料。這些措施需要隨技術進步而演進。

90. Besides, data controllers should proceed to the deletion of raw data

(face images, speech signals, the gait, etc.) and ensure the effectiveness of this deletion. If there is no longer a lawful basis for the processing, the raw data has to be deleted. Indeed, insofar as biometric templates derives from such data, one can consider that the constitution of databases could represent an equal if not even bigger threat (because it may not always be easy to read a biometric template without the knowledge of how it was programmed, whereas raw data will be the building blocks of any template). In case the data controller would need to keep such data, noise-additive methods (such as watermarking) must be explored, which would render the creation of the template ineffective. The controller must also delete biometric data and templates in the event of unauthorized access to the read-comparison terminal or storage server and delete any data not useful for further processing at the end of the biometric device's life.

此外，資料控管者應刪除原始資料（臉部圖像、語音訊號、步態等），並確保有效刪除。若運用不再有合法依據，必須刪除原始資料。實際上，由於生物特徵模板係由這些資料衍生得出，可以認為構建資料庫係同等（若非更大）威脅（因為若不知生物特徵模板的編程方法，則不易讀取模板，而原始資料則是構建任何模板的基石）。若控管者需要保存這些資料，則必須探究添加雜訊（noise-additive）方法（例如加浮水印），使之無法有效創設模板。若讀取一比對終端或儲存伺服器未經授權而被存取，控管者也必須刪除生物特徵資料和模板，生物特徵裝置使用期限屆滿後，無法再作其他使用的資料，也應一併刪除。

## 6 RIGHTS OF THE DATA SUBJECT

### 當事人的權利

91. Due to the character of data processing when using video surveillance some data subject's rights under GDPR serves further clarification. This chapter is however not exhaustive, all rights under the GDPR applies to processing of personal data through video surveillance.

由於使用影像監控運用資料之特性，當事人依GDPR享有的某些權利需要進一步釐清。但本章並非完全列舉，GDPR所規定的一切權利均適用於透過影像監控運用個人資料之行為。

#### 6.1 Right to access

##### 近用權

92. A data subject has the right to obtain confirmation from the controller as to whether or not their personal data are being processed. For video surveillance this means that if no data is stored or transferred in any way then once the real-time monitoring moment has passed the controller could only give the information that no personal data is any longer being processed (besides the general information obligations under Article 13, see *section 7 – Transparency and information obligations*). If however data is still being processed at the time of the request (i.e. if the data is stored or continuously processed in any other way), the data subject should receive access and information in accordance with Article 15.

當事人有權向控管者確認其個人資料是否正被運用。對於影像監控而言，這意味著若不以任何方式儲存或移轉資料，則即時監控之瞬間一旦結束，控管者所提供的資訊只能是不再運用任何個人資料（應同時履行第13條的一般資訊提供義務，見第7節，*透明化和資訊提供義務*）。然而，若該資料在請求之時仍被運用（亦即，若該資料被儲存或連續地以其他方式運用），則當事人應依第15條獲得存取權限並獲知資訊。

93. There are however, a number of limitations that may in some cases apply in relation to the right to access.

然而，某些情形下，近用權可能適用諸多限制。

- Article 15 (4) GDPR, adversely affect the rights of others  
GDPR第15條第4項，對他人權利的不利影響

94. Given that any number of data subjects may be recorded in the same sequence of video surveillance a screening would then cause additional processing of personal data of other data subjects. If the data subject wishes to receive a copy of the material (article 15 (3)), this could adversely affect the rights and freedoms of other data subject in the material. To prevent that effect the controller should therefore take into consideration that due to the intrusive nature of the video footage the controller should not in some cases hand out video footage where other data subjects can be identified. The protection of the rights of third parties should however not be used as an excuse to prevent legitimate claims of access by individuals, the controller should in those cases implement technical measures to fulfil the access request (for example, image-editing such as masking or scrambling). However, controllers are not obliged to implement such technical measures if they can otherwise ensure that they are able to react upon a request under Article 15 within the timeframe stipulated by Article 12 (3).

鑒於同一影像監控影片序列中可能攝錄到數目不確定的當事人，過濾影片將導致對其他當事人個資的額外運用。若當事人想要獲得影片副本（第15條第3項），將對影片中其他當事人之權利與自由造成不利影響。為避免此影響，控管者因此應考慮，由於影片的干預性，在某些情況下，若可識別其他當事人，則不得交出影片。然而，不得以保護第三方權利為藉口，阻止個人的正當近用主張，此時，控管者應採取技術措施滿足近用請求（例如，遮蔽（mask）或加擾（scramble）等圖像編輯技術）。然而，若控管者能夠確保以其他方式在第12條第3項規定的時限內，回應依第15條提出之請求，則其並無義務採取這些技術措施。

- Article 11 (2) GDPR, controller is unable to identify the data subject  
GDPR第11條第2項，控管者無法識別當事人

95. If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject.

若無法在該影片中搜尋個人資料（亦即，控管者為了找到相關當事人，可能不得不查找所儲存的大量資料），則控管者可能無法識別該當事人。

96. For these reasons the data subject should (besides identifying themselves including with identification document or in person) in its request to the controller, specify when – within a reasonable timeframe in proportion to the amount of data subjects recorded – he or she entered the monitored area. The controller should notify the data subject beforehand on what information is needed in order for the controller to comply with the request. If the controller is able to demonstrate that it is not in a position to identify the data subject, the controller must inform the data subject accordingly, if possible. In such a situation, in its response to the data subject the controller should inform about the exact area for the monitoring, verification of cameras that were in use etc. so that the data subject will have the full understanding of what personal data of him/her may have been processed.

因此，當事人應（在表明其身分的同時，包括提供身分文件或親自到場）在其對控管者的請求中，說明其何時進入受監控區域，該時段精確度應與所攝錄當事人的數目成比例。控管者應將其為遵循該請求所需之資訊預先告知當事人。若控管者能夠證明其無法識別當事人，在可行的前提下，其必須向當事人為之告知。這種情況下，控管者在對當事人的回應中，應告知受監控的具體區域、確認所使用的攝影機等，以便當事人充分瞭解其哪些個人資料可能已被運用。

97.

Example: If a data subject is requesting a copy of his or her personal data processed through video surveillance at the entrance of a shopping mall with 30 000 visitors per day, the data subject should specify when he or she passed the monitored area within approximately a one-hour-timeframe. If the controller still processes the material a copy of the video footage should be provided. If other data subjects can be identified in the same material then that part of the material should be anonymised (for example by blurring the copy or parts thereof) before giving the copy to the data subject that filed the request.

示例：若當事人請求提供影像監控所運用的其個人資料之副本，而該監控係裝設在每日30,000人經過的賣場門口，則當事人應說明其經過受監控區域的時間，精確到大約1小時內。若控管者仍保留有

該影片，則應提供其副本。若同一影片中可識別其他當事人，則在把該副本提供予提出請求的當事人之前，應將影片的有關部分匿名化（例如，將該副本或其中一部分模糊化）。

Example: If the controller is automatically erasing all footage for example within 2 days, the controller is not able to supply footage to the data subject after those 2 days. If the controller receives a request after those 2 days the data subject should be informed accordingly.

示例：若控管者在一定期間（例如2天）內，自動刪除全部影片，則其無法在2天後向當事人提供影片。若控管者在2天期間經過後收到請求，則應對當事人為告知。

- Article 12 GDPR, excessive requests  
GDPR第12條，過度請求

98. In case of excessive or manifestly unfounded requests from a data subject, the controller may either charge a reasonable fee in accordance with Article 12 (5) (a) GDPR, or refuse to act on the request (Article 12 (5) (b) GDPR). The controller needs to be able to demonstrate the manifestly unfounded or excessive character of the request.

若當事人提出過度或顯無理由之請求，控管者得依GDPR第12條第5項第a款收取合理費用，或拒絕對該請求採取行動（GDPR第12條第5項第b款）。控管者需要能夠證明該請求顯無理由或過度之性質。

## 6.2 Right to erasure and right to object

### 刪除權和拒絕權

#### 6.2.1 Right to erasure (Right to be forgotten)

##### 刪除權（被遺忘權）

99. If the controller continues to process personal data beyond real-time monitoring (e.g. storing) the data subject may request for the personal data to be erased under Article 17 GDPR.

若控管者在即時監控之外繼續運用（例如儲存）個人資料，當事人得依GDPR第17條請求刪除個人資料。

100. Upon a request, the controller is obliged to erase the personal data without undue delay if one of the circumstances listed under Article 17 (1) GDPR applies (and none of the exceptions listed under Article 17 (3)



GDPR does). That includes the obligation to erase personal data when they are no longer needed for the purpose for which they were initially stored, or when the processing is unlawful (see also *Section 8 – Storage periods and obligation to erasure*). Furthermore, depending on the legal basis of processing, personal data should be erased:

經此請求後，若適用GDPR第17條第1項規定之數款情形之一（且沒有適用GDPR第17條第3項所列的例外情形），控管者有義務刪除該個人資料，不得無故遲延。這包括當資料對其最初儲存之目的不再需要，或運用不合法時，刪除個人資料之義務（另見第8節，儲存期間和刪除義務）。此外，根據運用的法律依據，下列情形應刪除個人資料：

- *for consent* whenever the consent is withdrawn (and there is no other legal basis for the processing)  
對於同意，撤回同意時（且運用無其他法律依據）。
- *for legitimate interest*:  
對於正當利益：
  - whenever the data subject exercises the right to object (see *Section 6.2.2*) and there are no overriding compelling legitimate grounds for the processing, or  
當事人行使拒絕權時（見第6.2.2節），且並無超越性的必要正當理由可進行運用；或
  - in case of direct marketing (including profiling) whenever the data subject objects to the processing.  
行銷（包括剖析）時，當事人拒絕運用。

101. If the controller has made the video footage public (e.g. broadcasting or streaming online), reasonable steps need to be taken in order to inform other controllers (that are now processing the personal data in question) of the request pursuant to Article 17 (2) GDPR. The reasonable steps should include technical measures, taking into account available technology and the cost of implementation. To the extent possible, the controller should notify – upon erasure of personal data – anyone to which the personal data previously have been disclosed, in accordance with Article 19 GDPR.

若控管者已公開影片（例如廣播或線上串流），需要依GDPR第17條

第2項採取合理步驟，將該請求告知其他（正在運用該個人資料之）控管者。該合理步驟應包括技術措施，並考量可用之技術與實施成本。在可行範圍內，控管者應—在刪除個人資料後—依GDPR第19條通知已向其揭露該個人資料之任何人。

102. Besides the controller's obligation to erase personal data upon the data subject's request, the controller is obliged under the general principles of the GDPR to limit the personal data stored (see *Section 8*).

除控管者依當事人請求刪除個人資料之義務外，依GDPR的一般原則，控管者有義務限制所儲存之個人資料（見第8節）。

103. For video surveillance it is worth noticing that by for instance blurring the picture with no retroactive ability to recover the personal data that the picture previously contained, the personal data are considered erased in accordance with GDPR.

對於影像監控，值得注意的是，若以模糊化等方式處理圖像，且無法回復該圖像曾經含有的個人資料，則所含有的個人資料視為已經依GDPR刪除。

104.

Example: A convenience store is having trouble with vandalism in particular on its exterior and is therefore using video surveillance outside of their entrance in direct connection to the walls. A passer-by requests to have his personal data erased from that very moment. The controller is obliged to respond to the request without undue delay and at the latest within one month. Since the footage in question does no longer meet the purpose for which it was initially stored (no vandalism occurred during the time the data subject passed by), there is at the time of the request, no legitimate interest to store the data that would override the interests of the data subjects. The controller needs to erase the personal data.

示例：一家便利商店經常遭受故意破壞行為困擾，特別是對其外觀的破壞，並因此在其入口處與外牆連結處使用影像監控。一名路人請求刪除其經過時的個人資料。控管者有義務回應此請求，不得無故遲延，且至遲於一個月內回應。由於該影片已不再符合其最初儲存之目的（當事人經過時，並未發生破壞行為），在請求之時，儲

存該資料並無超越當事人權利的正當利益。控管者需要刪除該個人資料。

## 6.2.2 Right to object

### 拒絕權

105. For video surveillance based on *legitimate interest* (Article 6 (1) (f) GDPR) or for the necessity when carrying out a task in the *public interest* (Article 6 (1) (e) GDPR) the data subject has the right – at any time – to object, on grounds relating to his or her particular situation, to the processing in accordance with Article 21 GDPR. Unless the controller demonstrates compelling legitimate grounds that overrides the rights and interests of the data subject, the processing of data of the individual who objected must then stop. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month.

對於基於正當利益（GDPR第6條第1項第f款），或為執行符合公共利益之職務所必要（GDPR第6條第1項第e款）實施之影像監控，當事人依GDPR第21條，根據其個別狀況，有權利—隨時—拒絕該運用。除非控管者證明存在超越當事人權利和利益之必要正當理由，否則必須停止運用該拒絕者的資料。控管者有義務回應當事人之請求，不得無故遲延，且至遲於一個月內回應。

106. In the context of video surveillance this objection could be made either when entering, during the time in, or after leaving, the monitored area. In practice this means that unless the controller has compelling legitimate grounds, monitoring an area where natural persons could be identified is only lawful if either

影像監控的情況下，在進入該受監控區域、位於該區域內或離開該區域後，均可拒絕。實務中，這意味著除非控管者有必要正當理由，對自然人可被識別的特定區域實施監控，僅有在下列情況下合法：

(1) the controller is able to immediately stop the camera from processing personal data when requested, or

控管者能夠一經請求立即停止攝影機運用個人資料，或

(2) the monitored area is in such detail restricted so that the controller can assure the approval from the data subject prior to

entering the area and it is not an area that the data subject as a citizen is entitled to access.

受監控區域受嚴格限制，控管者能夠確保在各當事人進入該區域前獲得其同意，且該區域並非當事人作為公民有權進入之場所。

107. These guidelines do not aim to identify what is considered a compelling legitimate interest (Article 21 GDPR).

本指引無意釐清何者構成必要正當利益（GDPR第21條）。

108. When using video surveillance for direct marketing purposes, the data subject has the right to object to the processing on a discretionary basis as the right to object is absolute in that context (Article 21 (2) and (3) GDPR).

為行銷目的使用影像監控時，由於此時拒絕權係一絕對權利，當事人有權自主決定拒絕其運用（GDPR第21條第2項和第3項）。

109.

Example: A company is experiencing difficulties with security breaches in their public entrance and is using video surveillance on the grounds of legitimate interest, with the purpose to catch those unlawfully entering. A visitor objects to the processing of his or her data through the video surveillance system on grounds relating to his or her particular situation. The company however in this case rejects the request with the explanation that the footage stored is needed due to an ongoing internal investigation, thereby having compelling legitimate grounds to continue processing the personal data.

示例：一家公司正遭受其公共入口處保全問題困擾，並基於正當利益，為偵測非法進入者目的，運用影像監控。一名來訪者基於其個別狀況，拒絕以影像監控系統運用其資料。然而，該公司拒絕其請求，並解釋其進行中的內部調查需要儲存該影片，因此其有必要正當理由繼續運用該個人資料。

## 7 TRANSPARENCY AND INFORMATION OBLIGATIONS<sup>18</sup>

### 透明化和資訊提供義務<sup>18</sup>

110. It has long been inherent in European data protection law that data subjects should be aware of the fact that video surveillance is in operation. They should be informed in a detailed manner as to the places monitored.<sup>19</sup> Under the GDPR the general transparency and information obligations are set out in Article 12 GDPR and following. Article 29 Working Party's "Guidelines on transparency under Regulation 2016/679 (WP260)" which were endorsed by the EDPB on May 25<sup>th</sup> 2018 provide further details. In line with WP260 par. 26, it is Article 13 GDPR, which is applicable if personal data are collected "[...] from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras [...])."

歐洲資料保護法向來要求應使當事人知曉影像監控正在運作，還應向其詳細告知受監控的地點<sup>19</sup>。依GDPR規定，一般透明化和資訊提供義務規定於GDPR第12條以下。EDPB於2018年5月25日採認之第29條工作小組（WP29）「關於第2016/679號規則（GDPR）中的透明化之指引（WP260）」包含更多的細節。依WP260第26段，若個人資料係「……以觀察方式（例如使用攝影機等自動化資料拍攝裝置或資料拍攝軟體）從當事人……」蒐集而得，則適用GDPR第13條。

111. In light of the volume of information, which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency (WP260, par. 35; WP89, par. 22). Regarding video surveillance the most important information should be displayed on the warning sign itself (first layer) while the further mandatory details may be provided by other means (second layer).

根據應向當事人提供之資訊的量，資料控管者得採用層級化方式，選擇使用不同方法之組合，以確保透明化（WP260，第35段；WP89，第22段）。關於影像監控，最重要的資訊應在警示標誌上顯示（第

---

<sup>18</sup> Specific requirements in national legislation might apply.

可能適用國家立法中的特定要求。

<sup>19</sup> See WP89, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance by Article 29 Working Party).

見WP89，第29條工作小組「關於以影像監控方式運用個人資料的意見4/2004」。

一層)，而其他強制告知之資訊得以其他方式提供（第二層）。

## 7.1 First layer information (warning sign)

### 第一層資訊（警示標誌）

112. The first layer concerns the primary way in which the controller first engages with the data subject. At this stage, controllers may use a warning sign showing the relevant information. The displayed information may be provided in combination with an icon in order to give, in an easily visible, intelligible and clearly readable manner, a meaningful overview of the intended processing (Article 12 (7) GDPR). The format of the information should be adjusted to the individual location (WP89 par. 22).

第一層係關於控管者與當事人初始互動之主要方式。此一階段，控管者得使用警示標誌展示相關資訊。所展示的資訊得附有圖標，以便以易見、易懂且清晰易讀之方式，就預計之運用提出有意義之概述（GDPR第12條第7項）。應根據具體位置調整資訊之格式（WP89，第22段）。

#### 7.1.1 Positioning of the warning sign

##### 警示標誌之放置方式

113. The information should be positioned in such a way that the data subject can easily recognize the circumstances of the surveillance before entering the monitored area (approximately at eye level). It is not necessary to reveal the position of the camera as long as there is no doubt as to which areas are subject to monitoring and the context of surveillance is clarified unambiguously (WP 89, par. 22). The data subject must be able to estimate which area is captured by a camera so that he or she is able to avoid surveillance or adapt his or her behaviour if necessary.

資訊的放置方式應使得當事人能夠在進入受監控區域前，很容易地瞭解監控狀況（大約平視位置）。在清楚標示受監控之區域且確實說明監控狀況的前提下，不必指明攝影機的位置（WP89，第22段）。當事人必須能夠估測攝影機所拍攝的範圍，以便在必要時避開監控或調整其行為。

## 7.1.2 Content of the first layer

### 第一層內容

114. The first layer information (warning sign) should generally convey the most important information, e.g. the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impacts of the processing.<sup>20</sup> This can include for example the legitimate interests pursued by the controller (or by a third party) and contact details of the data protection officer (if applicable). It also has to refer to the more detailed second layer of information and where and how to find it.

第一層資訊（警示標誌）一般應傳達最重要的資訊，例如運用之目的、控管者身分和當事人權利等方面的細節，以及運用最為重要的影響<sup>20</sup>。這可能包括，例如，控管者（或第三方）所追求的正當利益和個資保護長的聯絡資訊（若適用）。還應提及第二層更詳細的資訊，並說明在何處以何種方式獲得該資訊。

115. In addition the sign should also contain any information that could surprise the data subject (WP260, par. 38). That could for example be transmissions to third parties, particularly if they are located outside the EU, and the storage period. If this information is not indicated, the data subject should be able to trust that there is solely a live monitoring (without any data recording or transmission to third parties).


此外，該標誌還應包括可能使當事人感到意外的其他任何資訊（WP260，第38段）。這可能包括，例如，向第三方傳輸，特別是當該第三方位於歐盟境外時，以及儲存期間。若未說明這些資訊，當事人應能夠信任僅有單純的即時監控（不攝錄或向第三方傳輸任何資料）。

---

<sup>20</sup> See WP260, par. 38.  
見WP260，第38段。

116.

**Example:**



**Video surveillance!**

Identity of the controller and, where applicable, of the controller's representative:

---

Contact details of the data protection officer (where applicable):


---

Purposes of the processing for which the personal data are intended as well as the legal basis for the processing:

---

**Data subjects rights:** As a data subject you have several rights against the controller, in particular the right to request from the controller access to or erasure of your personal data.

For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.



Further information is available:

- via notice
- at our reception/ customer information/ register
- via internet (URL)...

**示例：**



**錄影監控中！**

控管者身分以及可適用的控管者代表：

---

個資保護長之聯絡資訊（如適用）：

---

個人資料預計運用之目的及其法律依據：

---

**當事人權利：** 作為當事人，您可對控管者行使數項權利，特別是向控管者請求存取資料或刪除您的個人資料。

關於本影像監控之詳細資訊，包括您的權利，請見控管者透過左側所列選項提供之完整資訊。



更多資訊請見：

- 通知
- 我們的接待櫃檯/服務台/收銀櫃檯
- 網路（連結）……



## 7.2 Second layer information

### 第二層資訊

117. The second layer information must also be made available at a place easily accessible to the data subject, for example as a complete 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 warning sign has to refer clearly to the second layer information. In addition, it is best if the first layer information refers to a digital source (e.g. QR-code or a website address) of the second layer. However, the information should also be easily available non-digitally. It should be possible to access the second layer information without entering the surveyed area, especially if the information is provided digitally (this can be achieved for example by a link). Other appropriate means could be a phone number that can be called. However the information is provided, it must contain all that is mandatory under Article 13 GDPR.

第二層資訊也必須在當事人易於獲取的位置提供，例如，可在某一核心位置（例如服務台、接待櫃檯或收銀櫃檯）提供完整資訊頁，或在易於參閱的海報上顯示。如前所述，第一層警示標誌必須明確提及第二層資訊。此外，最佳情況是，第一層資訊說明第二層資訊的數位資源（例如QR-code或網站網址）。然而，該資訊還應易於以非數位化方式獲取。第二層資訊應能在不進入受監控區域的情況下獲取，尤其是在該資訊以數位方式提供（例如，可透過連結而達成）。其他適當方式可以是能夠撥打的電話號碼。無論該資訊以何種方式提供，其必須包含GDPR第13條強制要求提供的全部資訊。

118. In addition to these options, and also to make them more effective, the EDPB promotes the use of technological means to provide information to data subjects. This may include for instance; geolocating cameras and including information in mapping apps or websites so that individuals can easily, on the one hand, identify and specify the video sources related to the exercise of their rights, and on the other hand, obtain more detailed information on the processing operation.

這些選項之外，同時也是為了增強這些選項的有效性，EDPB鼓勵使用技術方式向當事人提供資訊。這可能包括，例如，地理攝影機，在地圖繪製應用程式或網站中納入該資訊，以便個人能夠一方面輕

易地識別和明確行使其權利的相關影片來源，另一方面獲知關於運用作業的更詳細的資訊。

119.

Example: A shop owner is monitoring his shop. To comply with Article 13 it is sufficient to place a warning sign at an easy visible point at the entrance of his shop, which contains the first layer information. In addition, he has to provide an information sheet containing the second layer information at the cashier or any other central and easy accessible location in his shop.

示例：一名店主對其商店進行監控。為符合第13條，得在商店入口處顯著位置放置包含第一層資訊的警示標誌。此外，其還必須在收銀櫃檯或店內其他核心且易接近之位置提供包含第二層資訊的資訊頁。

## 8 STORAGE PERIODS AND OBLIGATION TO ERASURE

### 儲存期間和刪除義務

120. Personal data may not be stored longer than what is necessary for the purposes for which the personal data is processed (Article 5 (1) (c) and (e) GDPR). In some Member States, there may be specific provisions for storage periods with regards to video surveillance in accordance with Article 6 (2) GDPR.

個人資料的儲存期限不得超過其運用目的所必要的期間（GDPR第5條第1項第c款和第e款）。某些會員國可能依GDPR第6條第2項，對於影像監控的儲存期間有具體規定。

121. Whether the personal data is necessary to store or not should be controlled within a narrow timeline. In general, legitimate purposes for video surveillance are often property protection or preservation of evidence. Usually damages that occurred can be recognized within one or two days. To facilitate the demonstration of compliance with the data protection framework it is in the controller's interest to make organisational arrangements in advance (e. g. nominate, if necessary, a representative for screening and securing video material). Taking into consideration the principles of Article 5 (1) (c) and (e) GDPR, namely data minimization and storage limitation, the personal data should in most cases (e.g. for the purpose of detecting vandalism) be erased, ideally automatically, after a few days. The longer the storage period set (especially when beyond 72 hours), the more argumentation for the legitimacy of the purpose and the necessity of storage has to be provided. If the controller uses video surveillance not only for monitoring its premises but also intends to store the data, the controller must assure that the storage is actually necessary in order to achieve the purpose. If so, the storage period needs to be clearly defined and individually set for each particular purpose. It is the controller's responsibility to define the retention period in accordance with the principles of necessity and proportionality and to demonstrate compliance with the provisions of the GDPR.

個人資料的儲存必要性應控制於嚴格時限內。一般而言，影像監控的正當目的通常係保護財產或保存證據。所發生的損害通常能於一或兩天內發現。為協助證明符合資料保護體系，控管者宜事先進行

組織性安排（例如，在必要時指派代表過濾影片並對影片採取安全措施）。考量GDPR第5條第1項第c款和第e款規定之原則，亦即資料最小化和儲存限制，個人資料在大部分情況下（例如，為發現故意破壞行為）都應在數天後予以刪除（自動刪除更佳）。所設定的儲存期間越長（特別是若超過72小時），越需要論證目的正當性和儲存必要性。若控管者不僅使用影像監控其處所，還想要儲存該資料，則其必須確保儲存行為確實為實現其目的所必要。若是如此，則需為各項目的，分別明確定義其儲存期間。控管者有責任依必要性原則和比例原則定義保存期間，並證明遵守GDPR之規定。

122.

Example: An owner of a small shop would normally take notice of any vandalism the same day. In consequence, a regular storage period of 24 hours is sufficient. Closed weekends or longer holidays might however be reasons for a longer storage period. If a damage is detected he may also need to store the video footage a longer period in order to take legal action against the offender.

示例：一家小店的店主通常在破壞事故發生的當天即會注意到故意破壞行為。因此，一般儲存期間為24小時已經足夠。然而，週末或長假期間的店休可能是較長儲存期間的理由。若發現損害，其可能還需要將影片儲存較長期間，以便對行為人採取法律行動。

## 9 TECHNICAL AND ORGANISATIONAL MEASURES

### 技術性和組織性措施

123. As stated in Article 32 (1) GDPR, processing of personal data during video surveillance must not only be legally permissible but controllers and processors must also adequately secure it. Implemented **organizational and technical measures** must be **proportional to the risks to rights and freedoms of natural persons**, resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to video surveillance data. According to Article 24 and 25 GDPR, controllers need to implement technical and organisational measures also in order to safeguard all data-protection principles during processing, and to establish means for data subjects to exercise their rights as defined in Articles 15-22 GDPR. Data controllers should adopt internal framework and policies that ensure this implementation both at the time of the determination of the means for processing and at the time of the processing itself, including the performance of data protection impact assessments when needed.

如GDPR第32條第1項所述，在影像監控期間運用個人資料不僅須為法律所允許，控管者和受託運用者還必須適當且充分地保護其安全。所實施的**組織性和技術性措施**，必須與所造成的**自然人的權利與自由之風險符合比例**，該風險可能係意外或違法破壞、丟失、竄改、未經授權揭露或存取影像監控資料而造成。依GDPR第24條和第25條，控管者還需執行技術性和組織性措施，以便在運用期間確保遵守一切資料保護原則，以及為了確立當事人行使GDPR第15條至第22條規定的各項權利的方法。資料控管者須採用內部體系和政策，以便在決定運用方法以及實際運用時可執行該等措施，包括必要時辦理個人資料保護影響評估。

### 9.1 Overview of video surveillance system

#### 影像監控系統概述

124. A video surveillance system (VSS)<sup>21</sup> consists of analogue and digital devices as well as software for the purpose of capturing images of a scene, handling the images and displaying them to an operator. Its components are grouped into the following categories:

影像監控系統（VSS）<sup>21</sup>包括類比和數位裝置及軟體，用以拍攝場景畫面、處理畫面並顯示予作業人員。其要素可分為如下兩類：

- Video environment: image capture, interconnections and image handling:

影像環境：畫面拍攝、互聯（interconnection）和畫面處理：

- the purpose of image capture is the generation of an image of the real world in such format that it can be used by the rest of the system,

拍攝畫面的目的係以系統其他部分可使用之格式，生成真實世界的影像；

- interconnections describe all transmission of data within the video environment, i.e. connections and communications. Examples of connections are cables, digital networks, and wireless transmissions. Communications describe all video and control data signals, which could be digital or analogue,

互聯描述影像環境內部的一切資料傳輸，亦即串聯（connection）和通訊（communication）。串聯的示例如線纜、數位網路和無線網路傳輸。通訊描述一切影片和控制資料訊號，可能係數位或類比性質。

- image handling includes analysis, storage and presentation of an image or a sequence of images.

畫面處理包括分析、儲存和呈現一幀畫面或一序列畫面。

- From the system management perspective, a VSS has the following logical functions:

系統管理方面，影像監控系統有下列邏輯功能：

- data management and activity management, which includes handling operator commands and system generated activities (alarm procedures, alerting operators), 資料管理和活動管理，包括處理作業人員命令和系統生成活動（警報程序、提醒作業人員）；

---

<sup>21</sup> GDPR does not provide a definition for it, a technical description can for example be found in EN 62676-1- 1:2014 Video surveillance systems for use in security applications – Part 1-1: Video system requirements.

GDPR並未對此作定義，相關技術描述之示例為EN 62676-1- 1:2014，安全應用中使用之影像監控系統，第1-1部分，影像系統要求。

- interfaces to other systems might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition).

對其他系統的介面可能包括連接至其他安全系統（權限控制、火災警報）和非安全系統（建築管理系統、自動車牌辨識）。

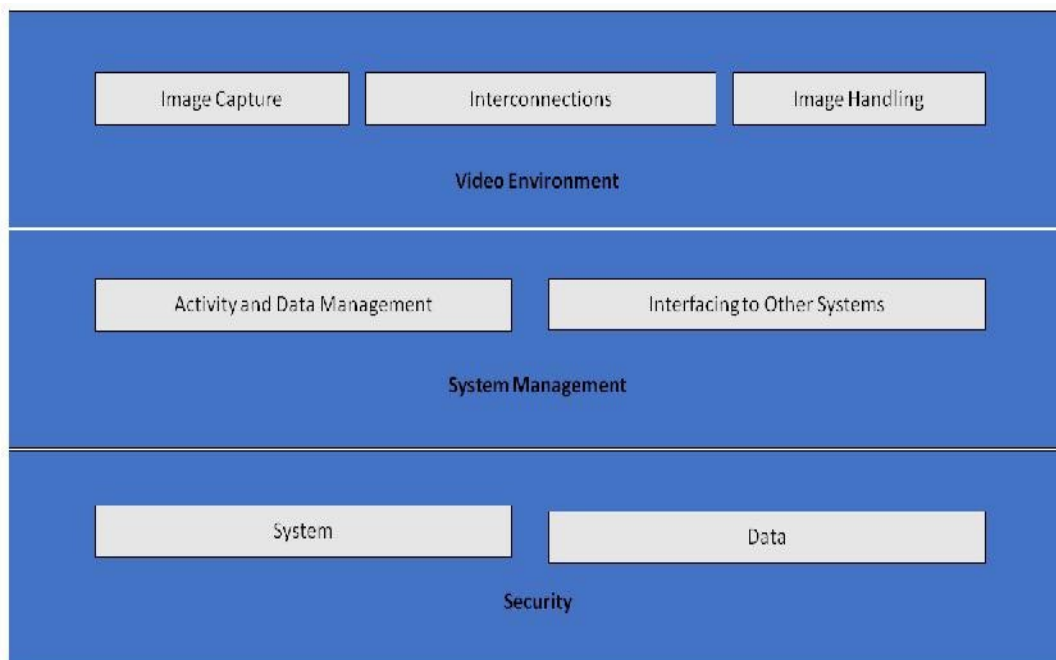
- VSS security consists of system and data confidentiality, integrity and availability:

影像監控系統安全包括系統和資料機密性、完整性和可用性：

- system security includes physical security of all system components and control of access to the VSS,  
系統安全包括一切系統要素的實體安全（physical security）和該影像監控系統的權限控制；
- data security includes prevention of loss or manipulation of data.

資料安全包括防範資料丟失和竄改。

125.



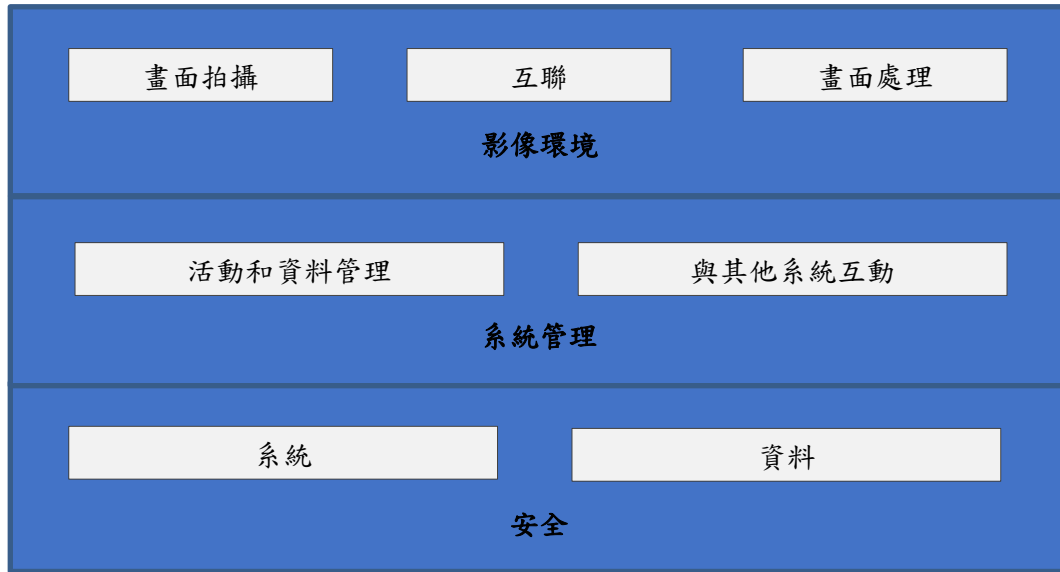


Figure 1- video surveillance system

圖1—影像監控系統

## 9.2 Data protection by design and by default

### 資料保護之設計和預設

126. As stated in Article 25 GDPR, controllers need to implement appropriate data protection technical and organisational measures as soon as they plan for video surveillance – before they start the collection and processing of video footage. These principles emphasize the need for built-in privacy enhancing technologies, default settings that minimise the data processing, and the provision of the necessary tools that enable the highest possible protection of personal data<sup>22</sup>.

如GDPR第25條所規定，控管者從開始計劃影像監控之時—在其開始蒐集和運用影片之前，就需要執行適當的技術性和組織性的資料保護措施。這些原則強調，需要內建式的隱私強化技術，最小化資料運用的預設設定以及提供必要工具，以實現最高程度的個資保護<sup>22</sup>。

<sup>22</sup> WP 168, Opinion on the "The Future of Privacy", joint contribution by the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (adopted on 01 December 2009).

WP168，關於「隱私的未來」之意見，第29條個資保護工作小組和警察和司法工作小組對與歐盟執委會「關於個資保護基本權利的法律框架的諮商」之聯合提案（2009年12月1日通過）。



127. Controllers should build data protection and privacy safeguards not only into the design specifications of the technology but also into organisational practices. When it comes to organisational practices, the controller should adopt an appropriate management framework, establish and enforce policies and procedures related to video surveillance. From the technical point of view, system specification and design should include requirements for processing personal data in accordance with principles stated in Article 5 GDPR (lawfulness of processing, purpose and data limitation, data minimisation by default in the sense of Article 25 (2) GDPR, integrity and confidentiality, accountability etc.). In case a controller plans to acquire a commercial video surveillance system, the controller needs to include these requirements in the purchase specification. The controller needs to ensure compliance with these requirements applying them to all components of the system and to all data processed by it, during their entire lifecycle.

控管者在技術的設計規格方面，以及組織性實務方面，皆應建立資料保護和隱私安全維護措施。在組織性實務方面，控管者應採行適當的管理體系，確立並實施影像監控相關之政策和程序。從技術的角度，系統規格和設計應包括依GDPR第5條規定的原則運用個人資料之要求（運用之合法性、目的和資料限制、GDPR第25條第2項意義上的預設資料最小化、完整性和機密性、課責性等）。若控管者計劃購買商業影像監控系統，則需要在訂單規格中納入這些要求。控管者需要確保遵守這些要求，並在其運作之完整期間內，將其適用於系統的全部要素及其所運用的全部資料。

### 9.3 Concrete examples of relevant measures

#### 相關措施的具體示例

128. Most of the measures that can be used to secure video surveillance, especially when digital equipment and software are used, will not differ from those used in other IT systems. However, regardless of the solution selected, the controller must adequately protect all components of a video surveillance system and data under all stages, i.e. during storage (data at rest), transmission (data in transit) and processing (data in use). For this, it is necessary that controllers and processors combine organisational and technical measures.

大部分可用於確保影像監控安全的措施，特別是所使用的數位設備和軟體，與其他IT技術系統所使用的並無不同。然而，無論選擇何種方案，控管者都必須充分保護影像監控系統的全部要素和各階段資料，亦即，儲存階段（靜止資料）、傳輸階段（傳輸中的資料）和運用階段（使用中的資料）。為此，控管者和受託運用者有必要結合組織性和技術性的措施。

129. When selecting technical solutions, the controller should consider privacy-friendly technologies also because they enhance security. Examples of such technologies are systems that allow masking or scrambling areas that are not relevant for the surveillance, or the editing out of images of third persons, when providing video footage to data subjects.<sup>23</sup> On the other hand, the selected solutions should not provide functions that are not necessary (e.g., unlimited movement of cameras, zoom capability, radio transmission, analysis and audio recordings). Functions provided, but not necessary, must be deactivated.

選擇技術方案時，控管者還應考慮隱私友好的技術，因為其能增強安全性。這種技術的示例係，在向當事人提供影片時，能夠遮蔽或加擾與監控無關之區域、或將第三人的影像編輯移除的系統<sup>23</sup>。另一方面，所選擇的方案不應提供非必要功能（例如，攝影機不受限制的移動、變焦能力、無線電傳輸、分析和錄音）。所提供的非必要功能必須予以關閉。

130. There is a lot of literature available on this subject, including international standards and technical specifications on the physical security of multimedia systems<sup>24</sup>, and the security of general IT systems<sup>25</sup>. Therefore, this section provides only a high-level overview of this topic.

此一主題有許多文獻，包括多媒體系統實體安全<sup>24</sup>與一般IT技術系統安全<sup>25</sup>相關的國際標準和技術規格。因此，本節僅對此一主題進行簡

---

<sup>23</sup> The use of such technologies may even be mandatory in some cases in order to comply with Article 5 (1) (c). In any case they can serve as best practice examples.

某些情況下，為符合第5條第1項第c款，甚至強制使用這些技術。無論如何，其可作為最佳實務之示例。

<sup>24</sup> IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use.

IEC TS 62045—多媒體安全—關於使用中和已停用的設備和系統之隱私保護指引。

<sup>25</sup> ISO/IEC 27000 — Information security management systems series

要回顧。

### 9.3.1 Organisational measures

#### 組織性措施

131. Apart from a potential DPIA needed (see *Section 10*), controllers should consider the following topics when they create their own video surveillance policies and procedures:

除可能需要個資保護影響評估（DPIA）外（見第10節），控管者在構建其影像監控政策和程序時，還應考慮下列問題：

- Who is responsible for management and operation of the video surveillance system.  
何人負責管理和運作該影像監控系統。
- Purpose and scope of the video surveillance project.  
該影像監控計畫的目的和範圍。
- Appropriate and prohibited use (where and when video surveillance is allowed and where and when it is not; e.g. use of hidden cameras and audio in addition to video recording)<sup>26</sup>.  
適當的和被禁止的使用（何時何地允許使用影像監控，何時何地不得使用；例如，使用隱藏式攝影機、錄影同時錄音）<sup>26</sup>。
- Transparency measures as referred to in *Section 7 (Transparency and information obligations)*.  
第7節（透明化和資訊提供義務）所述之透明化措施。
- How video is recorded and for what duration, including archival storage of video recordings related to security incidents.  
錄影的方法及其時限，包括將安全事故相關的錄影建檔儲存。
- Who must undergo relevant training and when.  
何人必須於何時接受相關培訓。
- Who has access to video recordings and for what purposes.  
何人得為哪些目的存取影片。
- Operational procedures (e.g. by whom and from where video surveillance is monitored, what to do in case of a data breach

---

ISO/IEC 27000—資訊安全管理系統系列。

<sup>26</sup> This may depend on national laws and sector regulations.  
可能依國內法和行業規則而不同

incident).

作業程序（例如，何人於何地觀看監控畫面，發生資料侵害事故時如何因應）。

- What procedures external parties need to follow in order to request video recordings, and procedures for denying or granting such requests.

外部人員如請求提供影片，應遵守哪些程序，拒絕或同意此等請求之程序。

- Procedures for VSS procurement, installation and maintenance.

影像監控系統採購、安裝和維護程序。

- Incident management and recovery procedures.

事故管理和恢復程序。

### 9.3.2 Technical measures

#### 技術性措施

132. **System security** means **physical security** of all system components, and system integrity i.e. **protection against and resilience under intentional and unintentional interference with its normal operations and access control**. Data security means **confidentiality** (data is accessible only to those who are granted access), **integrity** (prevention against data loss or manipulation) and **availability** (data can be accessed when it is required). 系統安全係指一切系統要素的**實體安全**與系統完整性，亦即，**防範和因應對其正常作業與存取權限控制的有意或無意干擾**。資料安全係指**機密性**（只有經授權者可存取資料），**完整性**（防止資料丟失或竄改）和**可用性**（在需要時可存取資料）。

133. **Physical security** is a vital part of data protection and the first line of defence, because it protect VSS equipment from theft, vandalism, natural disaster, manmade catastrophes and accidental damage (e.g. from electrical surges, extreme temperatures and spilled coffee). In case of an analogue based systems, physical security plays the main role in their protection.

**實體安全**是資料保護的重要部分且為第一道防線，其保護影像監控系統設備免受竊盜、故意破壞、自然災害、人為災禍和意外損害（例如，突波、極端溫度和打翻的咖啡）。在類比系統中，實體安全是主要保護措施。

134. **System and data security**, i.e. protection against intentional and unintentional interference with its normal operations may include:

系統和資料安全（亦即，防範對其正常作業的有意或無意干擾）可能包括：

- Protection of the entire VSS infrastructure (including remote cameras, cabling and power supply) against physical tampering and theft.  
保護影像監控系統基礎設施之整體（包括遠端攝影機、線纜和電源）免受實體破壞和竊取。
- Protection of footage transmission with communication channels secure against interception  
以安全通訊通道傳輸影片，防範攔截。
- Data encryption.  
資料加密。
- Use of hardware and software based solutions such as firewalls, antivirus or intrusion detection systems against cyber attacks.  
使用防火牆、防毒和入侵偵測系統等軟硬體解決方案，防範網路攻擊。
- Detection of failures of components, software and interconnections.  
偵測元件、軟體和互聯故障。
- Means to restore availability and access to the system in the event of a physical or technical incident.  
發生實體或技術事故時，恢復可用性和系統可存取性的方法。

135. **Access control** ensures that only authorized people can access the system and data, while others are prevented from doing it. Measures that support physical and logical access control include:

存取權限控制確保只有經授權者才能存取系統和資料，防止他人存取。支援實體和邏輯存取控制的措施包括：

- Ensuring that all premises where monitoring by video surveillance is done and where video footage is stored are secured against unsupervised access by third parties.  
確保受影像監控和儲存影片的一切場所皆採取安全措施，防範第三方在未經監督的情況下闖入。

- Positioning monitors in such a way (especially when they are in open areas, like a reception) so that only authorized operators can view them.  
調整顯示器位置（特別是當其位於接待櫃檯等開放區域時），使其僅能由授權作業人員觀看。
- Procedures for granting, changing and revoking physical and logical access are defined and enforced.  
定義並實施授予、變更和撤銷實體和邏輯存取權限的程序。
- Methods and means of user authentication and authorization including e.g. passwords length and change frequency are implemented.  
使用者認證和授權的方式與方法，包括實施密碼長度和修改頻率要求等。
- User performed actions (both to the system and data) are recorded and regularly reviewed.  
記錄並定期審查使用者（對系統和對資料）實施之行動。
- Monitoring and detection of access failures is done continuously and identified weaknesses are addressed as soon as possible.  
持續監控和偵測存取失敗，識別並儘快修正弱點。

## 10 DATA PROTECTION IMPACT ASSESSMENT

### 個資保護影響評估

136. According to Article 35 (1) GDPR controllers are required to conduct data protection impact assessments (DPIA) when a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons. Article 35 (3) (c) GDPR stipulates that controllers are required to carry out data protection impact assessments if the processing constitutes a systematic monitoring of a publicly accessible area on a large scale. Moreover, according to Article 35 (3) (b) GDPR a data protection impact assessment is also required when the controller intends to process special categories of data on a large scale.

根據GDPR第35條第1項，若某種資料運用可能導致對自然人權利與自由的高風險，控管者須辦理個資保護影響評估。GDPR第35條第3項第c款規定，若運用構成對公眾開放區域之大規模系統性監控，須辦理個資保護影響評估。此外，GDPR第35條第3項第b款規定，若控管者有意大規模運用特種個資，亦須辦理個資保護影響評估。

137. The Guidelines on Data Protection Impact Assessment<sup>27</sup> provide further advice, and more detailed examples relevant to video surveillance (e.g. concerning the “use of a camera system to monitor driving behaviour on highways”). Article 35 (4) GDPR requires that each supervisory authority publish a list of the kind of processing operations that are subject to mandatory DPIA within their country. These lists can usually be found on the authorities’ websites. Given the typical purposes of video surveillance (protection of people and property, detection, prevention and control of offences, collection of evidence and biometric identification of suspects), it is reasonable to assume that many cases of video surveillance will require a DPIA. Therefore, data controllers should carefully consult these documents in order to determine whether such an assessment is required and conduct it if necessary. The outcome of the performed DPIA should determine the controller’s choice of implemented data protection measures.

「關於個資保護影響評估之指引」<sup>27</sup>對影像監控提供進一步建議與更

---

<sup>27</sup> WP248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. - endorsed by the EDPB

詳細的示例（例如「使用攝影系統監控高速公路上的駕駛行為」）。GDPR第35條第4項要求各監管機關公布該國境內強制辦理DPIA之運用作業清單。這些清單通常刊載於機關網站上。考量到影像監控的典型目的（保護人員與財產，偵測、防範和控制違法行為，蒐集證據和嫌犯生物特徵），可合理假設很多影像監控將需要辦理個資保護影響評估。因此，資料控管者應仔細參閱這些文件，以確定是否應辦理評估，並在必要時辦理評估。所辦理的個資保護影響評估之結果應決定控管者選擇執行之資料保護措施。

138. It is also important to note that if the results of the DPIA indicate that processing would result in a high risk despite security measures planned by the controller, then it will be necessary to consult the relevant supervisory authority prior to the processing. Details on prior consultations can be found in Article 36.

還應注意，若個資保護影響評估結果顯示，雖有控管者計劃採取的安全措施，運用仍可能造成高風險，則有必要在運用前諮詢相關監管機關。此等事前諮詢的詳細資訊見於第36條。

For the European Data Protection Board

The Chair

(Andrea Jelinek)

歐盟個人資料保護委員會  
主席

(Andrea Jelinek)

---

WP248 rev.01，關於第 2016/679號規則（GDPR）中的個資保護影響評估（DPIA）以及確認運用是否「可能造成高風險」之指引，EDPB採認。