

仮日本語訳

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

Version 2.0

Adopted on 29 January 2020

ビデオ装置を介した個人データの取扱いに関するガイドライン 3/2019

バージョン 2.0

2020年1月29日に採択

本書面は、The European Data Protection Board (欧州データ保護会議)により2020年1月29日に採択後、2020年2月26日に修正された、“Guidelines 3/2019 on processing of personal data through video devices”の英語版の一部を個人情報保護委員会が日本語に翻訳したものである。本書面は参考のための仮日本語訳であって、その利用について当委員会は責任を負わないものとし、正確な内容については原文を参照されたい。

Version history

バージョン履歴

Version 2.1	26 February 2020 2020年2月26日	Amending material mistake 形式上の間違いを修正
Version 2.0	29 January 2020 2020年1月29日	Adoption of the Guidelines after public consultation パブリック・コンサルテーション後におけるガイドラインの採択
Version 1.0	10 July 2019 2019年7月10日	Adoption of the Guidelines for public consultation パブリック・コンサルテーションのためのガイドラインの採択

目次

1	Introduction.....	5
2	SCOPE OF APPLICATION	9
2.1	Personal Data	9
2.2	Application of the Law Enforcement Directive, LED (EU 2016/680)	10
2.3	Household exemption	11
3	LAWFULNESS OF PROCESSING.....	14
3.1	Legitimate are interest, Article 6 (1) (f).....	15
3.1.1	Existence of legitimate interests	15
3.1.2	Necessity of processing	18
3.1.3	Balancing of interests	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).....	25
3.3	Consent, Article 6 (1) (a)	26
4	DISCLOSURE OF VIDEO FOOTAGE TO THIRD PARTIES	29
4.1	Disclosure of video footage to third parties in general.....	29
4.2	Disclosure of video footage to law enforcement agencies.....	30
5	PROCESSING OF SPECIAL CATEGORIES OF DATA.....	33
5.1	General considerations when processing biometric data.....	36
5.2	Suggested measures to minimize the risks when processing biometric data...44	
6	RIGHTS OF THE DATA SUBJECT	47
6.1	Right to access	47
6.2	Right to erasure and right to object	50
6.2.1	Right to erasure (Right to be forgotten)	50
6.2.2	Right to object.....	53

7	TRANSPARENCY AND INFORMATION OBLIGATION	56
7.1	First layer information (warning sign)	57
7.1.1	Positioning of the warning sign	57
7.1.2	Content of the first layer	58
7.2	Second layer information	59
8	STORAGE PERIODS AND OBLIGATION TO ERASURE	61
9	TECHNICAL AND ORGANISATIONAL MEASURES.....	63
9.1	Overview of video surveillance system	63
9.2	Data protection by design and by default	66
9.3	Concrete examples of relevant measures	67
9.3.1	Organisational measures.....	68
9.3.2	Technical measures.....	70
10	DATA PROTECTION IMPACT ASSESSMENT	73

The European Data Protection Board

欧州データ保護会議は

Having regard to Article 70 (1)(e) 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”),

個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679/EU (以下、「GDPR」という。)の第 70 条第 1 項(e)を考慮し、

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 154/2018¹ of 6 July 2018 ,

2018 年 7 月 6 日の EEA 共同委員会の決定 No 154/2018 により修正された EEA 協定 1、特にその付属書 XI 及びその議定書 37 を考慮し

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

その手続規則の第 12 条及び第 22 条を考慮して、

HAS ADOPTED THE FOLLOWING GUIDELINES

以下のガイドラインを採択した。

1 Introduction

はじめに

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.

¹ References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

ビデオ装置の集中的な使用は、市民の行動に影響を及ぼしている。このようなツールが個人の生活の多くの領域に大規模に導入されたことは、本来であれば異常だと思われるものが発見されることを防ぐために、個人への圧力を更に高めることになる。事実上、これらの技術は、匿名による移動及びサービスの匿名での利用の可能性を制限し得るものであり、一般的には気づかれずに済む可能性を制限する。そのデータ保護への影響は非常に大きい。

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.

例えば、セキュリティ目的で構築されたビデオ監視は、ある個人にとっては快適かもしれないが、データ主体が予期しない目的(マーケティング目的、従業員の業績の監視など)に不正利用されないように保証する必要がある。さらに、現在では、撮影した画像を利用するために多くのツールが導入されており、従来のカメラがスマート・カメラに切り替わりつつある。ビデオによって生成されるデータ量は、これらのツール及び技術との組み合わせることで、二次利用のリスク(システムに当初割り当てられた目的に関連するものであるかどうかにかかわらず)、あるいは、不正利用のリスクを増加させる。ビデオ監視を扱う際は常にGDPRの一般原則(第5条)が注意深く検討される必要がある。

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.

ビデオ監視システムは、民間及び公的部門の専門家がセキュリティを強化し、視聴者分析の結果を取得し、パーソナライズされた広告を配信するなどの目的で私的な又は公共の場所でやり取りする方法を多くの点から変化させる。ビデオ監視システムは、インテリジェントなビデオ分析の導入により性能が向上している。これらの技術は、よりプライバシーへの侵入性の高い性質を持つもの（例えば複雑な生体認証技術などの）と、侵入性の低いもの（例えば単純なカウント・アルゴリズムなど）がある。匿名性を維持し、個人のプライバシーを保護することは、一般的にはますます難しくなっている。それぞれの状況で発生するデータ保護の問題は、これらの技術のいずれか、又は、ほかの技術を使用する際の法的分析と同様に、異なる可能性がある。

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.

プライバシーの問題に加え、これらの装置の誤動作やそれにより引き起こされかねないバイアスの可能性に伴うリスクも存在する。研究者たちは、顔の識別、認識、又は分析に利用されるソフトウェアは、識別対象者の年齢、性別、民族によって性能が異なると報告している。アルゴリズムは、異なる人口統計学に基づいて実行されるため、顔認識におけるバイアスは社会の偏見を強化する恐れがある。そのため、データ管理者は、ビデオ監視から生成される生体データの取扱いについても、その妥当性と提供される保証の十分性を定期的に評価するようにしなければならない。

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.

ビデオ監視は、根本的な目的を達成するために、他の手段が存在する場合、デフォルトで行う必要はない。そうでなければ、文化的規範が変化して、プライバシーの欠如が一般的に受け入れられるようになる可能性がある。

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.

本ガイドラインは、ビデオ装置を介した個人データの取扱いに関連して、GDPRを適用する方法について指針を示すことを目的としている。以下の例は網羅的なものではなく、一般的な推論は、利用の可能性のあるすべての分野に適用することができる。

2 SCOPE OF APPLICATION²

適用範囲²

2.1 Personal Data

個人データ

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.

主に財産の保護のため、又は個人の生命や健康を守るために、光学的又は視聴覚的手段によって特定の空間を体系的に自動監視することは、現代の重要な現象となっている。こうした活動は、監視対象の空間に入る人物について、外観やその他の特定の要素に基づいて識別可能なすべての人物に関する画像情報又は視聴覚情報の収集と保持が行われる。これらの詳細な情報に基づいて、人物の身元を確認することができる。また、当該特定の空間に個人が存在した事実及びそこでの行動についての個人データの更なる処理が取扱可能になる。これらのデータが不正に利用されるリスクは、監視対象の空間の大きさ、また、空間を頻繁に利用する人々の数に関連して増大する。この事実は、一般データ保護規則第35条第3項(c)に反映されている。この条項では、公衆がアクセス可能な場所を大規模に体系的に監視する場合、データ保護影響評価を行うよう求められており、また、同規則第37条第1項(b)では、取扱業務がその性質上、データ主体を定期的かつ体系的に監視する必要がある場合、処理者がデータ保護オフィサーを指名するよう求めている。

² The EDPB notes that where the GDPR so allows, specific requirements in national legislation might apply. EDPB は、GDPR が認める場合、国内法の特定の要件が適用され得る点に留意する。

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.

しかし、同規則は、個人と関連性がない場合、例えば個人を直接又は間接的に識別できない場合のデータの取扱いには適用されない。

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.

例: GDPRは、ダミーカメラ(つまり、カメラとして機能せず、したがって個人データを取扱っていないカメラ)には適用されない。ただし、一部の加盟国では、ダミーカメラが他の法律に服する場合がある。

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.

例: 高所からの録画は、取扱われたデータが特定の人物に関連づけられ得る場合にのみ、GDPRの適用範囲に含まれる。

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.

例: 駐車操作を支援するためのビデオカメラが自動車に組み込まれている。カメラが自然人に関する情報(ナンバープレート又は通行人を識別できる情報など)を収集しないように設定又は調整されている場合にはGDPRが適用されない。

- 9.

2.2 Application of the Law Enforcement Directive, LED (EU 2016/680)

法執行指令, LED (EU 2016/680)の適用

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.

特に、公共の安全への脅威からの保護と予防を含む、犯罪行為の防止、捜査、検出、起訴又は刑事罰の執行を目的とする所轄官庁による個人データの取扱いは、指令 EU2016/680の対象となる

2.3 Household exemption

家庭の適用除外

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.³

第2条2項(c)に従い、自然人が純粹に私的又は家庭内の行為の過程(オンライン活動も含み得る)で行われる個人データの取扱いは、GDPRの適用範囲外である³。

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*”.⁴ 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*”⁵.

³ See also Recital 18.

前文第 18 項も参照されたい。

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

欧州司法裁判所、ケース C-101/01 の判決、*ボディ・リンドクヴィストのケース*、2003 年 11 月 6 日、パラグラフ 47。

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

欧州司法裁判所、ケース C-212/13 の判決、*フランティシェク・ライネシュ対チェコ共和国個人情報保護局*、2014 年 12 月 11 日、パラグラフ 33。

この規定(いわゆる家庭の適用除外)は、ビデオ監視の文脈では、狭義に解釈されなければならない。したがって、欧州司法裁判所で判示されたように、いわゆる「家庭の適用除外」は「個人の私的な生活又は家庭生活の過程で行われる活動にのみ関連すると解釈されなければならないが、インターネット上で公開され、不特定数の人々がデータにアクセスできるように構成された個人データの取扱いは、明らかにこれに該当しない」⁴。さらに、ビデオ監視システムが個人データの継続的な録画と保存を伴い、「部分的であっても公共空間を含み、したがってデータをその方法で取扱っている者の私的な空間から外に向けられている」場合、それは指令95/46第3条第2項の2つ目のインデントの目的上、純粋に『私的な又は家庭内の』の活動であるとはみなされない⁵。

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.

私人の敷地内で動作するビデオ装置に関しては、家庭の適用除外に該当する可能性がある。これは、結論に至るため考慮しなければならないいくつかの要素に依存する。ECJが判決で特定された上記の要素に加え、家庭でのビデオ監視の使用者は、データ主体と何らかの個人的な関係を有しているかどうか、監視の規模や頻度が、監視対象者側のある種の専門的な活動を示唆しているかどうか、監視がデータ主体に悪影響を及ぼす可能性があるかどうかを検討する必要がある。前述の要素が一つでも該当すれば、必ずしもその取扱いが家庭の適用除外の範囲外であることを示唆するものではなく、その判断については総合的な評価が必要である。

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 exemption.

例: 旅行者が、自身の休暇を記録するために携帯電話とビデオカメラの両方で録画している。当該旅行者は、その映像を友人や家族には見せるものの、不特定数の人々がアクセスできる状態にはしない。これは家庭の適用除外に該当する。

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.

例: ダウンヒル・マウンテン・バイクの走者がアクションカメラで降下を録画しようとする。当該走者は人里離れた地域を走っており、自宅での個人鑑賞にその録画を利用する予定のみである。この場合、個人データがある程度処理されていても取扱家庭の適用除外に該当する。

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.

例: ある者が自身の庭を監視・している。敷地は柵で囲まれており、管理者自身とその家族のみが定期的に庭に出入りしている。これは、ビデオ監視が部分的にでも公共の場や近隣の土地が映っていないことを条件に、家庭の適用除外に該当する。

14.

3 LAWFULNESS OF PROCESSING

取扱いの適法性

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.⁶ 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)).

ビデオ監視を利用する前に、その取扱目的が詳細に特定される必要がある(第5条第1項(b))。ビデオ監視は、たとえば不動産やその他の資産の保護の支援、個人の生命及び身体的な完全性の保護の支援、民事訴訟のための証拠収集など、多くの目的に役立つ⁶。これらの監視目的は書面で文書化される必要があり(第5条第2項)、使用するすべてのビデオ監視ごとに特定される必要がある。複数のカメラが単一の管理者により同じ目的で利用される場合には、一緒に文書化することができる。さらに、第13条に従って取扱目的をデータ主体に通知しなければならない(第7章、透明性と情報に関する義務を参照されたい)。単に「安全性」又は「あなたの安全のため」という目的に基づくビデオ監視は、十分に特定されているとはいえない(第5条第1項(b))。さらに、これは、個人データが、データ主体との関係において、合法的、公正かつ透明性のある方法で取扱われなければならないという原則にも反する(第5条(1)(a)参照)。

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.⁷ However in practice, the provisions most likely to be used are

⁶ Rules on collecting evidence for civil claims varies in Member States.

民事訴訟のために証拠を収集するルールは加盟国で異なる。

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

本ガイドラインでは、加盟国間で異なりうる国内法の分析を行わず、又はその詳細に立ち入らない。

原則として、第6条第1項のすべての法的根拠は、ビデオ監視データを取扱う法的根拠となり得る。例えば、国内法がビデオ監視を行う義務を規定している場合には、第6条第1項(c)が適用される⁷。しかし、実際には、最も使用される可能性のある条項は、以下の規定である。

- Article 6 (1) (f) (legitimate interest),
第6条第1項(f)(正当な利益)
- Article 6 (1) (e) (necessity to perform a task carried out in the public interest or in the exercise of official authority).
第6条第1項(e)(公共の利益において、又は、公的機関の権限の行使において行われる職務を遂行する必要性)。

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

やや例外的なケースでは、第6条第1項(a)(同意)が管理者により法的根拠として利用されうる。

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

正当な利益、第6条第1項 (f)

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

第6条第1項(f)の法的評価は、前文第47項に従って以下の基準に基づいて行うべきである。

3.1.1 Existence of legitimate interests

正当な利益の存在

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 legal⁸, economic or non-material interests.⁹ 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

⁸ European Court of Justice, Judgment in Case C-13/16, *Rīgas satiksme case*, 4 may 2017
欧州司法裁判所、ケース C-13/15 の判決、*リガ交通*のケース、2017年5月4日

⁹ see WP217, Article 29 Working Party.
第29条作業部会 WP217 を参照されたい。

compelling legitimate interest which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

ビデオ監視は、管理者又は第三者が求める正当な利益の目的を達成するために必要な場合、当該利益よりも個人データの保護を求めるデータ主体の利益又は基本的な権利及び自由が優先される場合を除き、適法である(第6条第1項(f))。管理者又は第三者が追及する正当な利益は、法的利益⁸、経済的利益、又は非物質的な利益の可能性⁹がある。しかし、管理者は、データ主体が第21条に従って監視に異議を述べた場合、データ主体の利益、権利、及び自由よりも優先するやむを得ない正当な利益である場合、又は法的請求の確立、行使又は防御のためにのみ、データ主体のビデオ監視を進めることができる点を考慮する必要がある。

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.**

現実かつ危険な状況下では、強盗、窃盗、破壊行為から財産を保護するという目的は、ビデオ監視の正当な利益を構成することができる。

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)¹⁰. 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).**

正当な利益は、現実存在し、現在の問題である必要がある(すなわち、架空又は推測されるものであってはならない)¹⁰。監視を開始する前に、過去の損害や重大な事件など、現実に困難な状況が発生している必要がある。アカウントビリティの原則に照らして、管理者は関連する事件(日付、方法、経済的損失)及び関連する刑事責任を文書化することが望ましい。これらの文書化された事件は、正当な利益が存在する強力な証拠となり得る。正当な利

¹⁰ see WP217, Article 29 Working Party, p. 24 seq. See also ECJ Case C-708/18 p.44

第29条作業部会 WP217、24 ページ以下を参照されたい。欧州司法裁判所ケース C-708/18 の 44 ページも参照されたい。

益の存在と監視の必要性は、定期的に(例えば年に1回など、状況に応じて)再評価されるべきである。

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.

例：店主が、新しい店をオープンするにあたり、破壊行為を防ぐためにビデオ監視システムを設置したいと考えている。店主は、近隣で破壊行為が多発していることを、統計データを提示することで、証明することができる。また、近隣の店舗の経験も参考になる。当該店主が損害を被っている必要はない。近隣での被害が危険性などを示唆するものであれば、正当な利益を示すものとなる。しかし、問題となる区域や特定の店舗の危険性を分析せずに、全国的又は一般的な犯罪統計を提示するだけでは不十分である。

- 21.
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).

銀行や貴重品販売店(例えば、宝石店)、又は財産犯の典型的な犯罪現場として知られている場所(例えば、ガソリンスタンド)など、差し迫った危険状況は正当な利益を構成し得る。
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.

また、GDPR 第6条第1項第2文は、公的機関がその職務を遂行している限り、その取扱いを正当な利益に依拠することはできないと明確に述べている。

3.1.2 Necessity of processing

取扱いの必要性

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.

個人データは、取扱われる目的の必要性に照らして、適切で、関連性があり、必要なものに限定されるべきである(「データの最小化」)。第5条第1項(c)を参照されたい。管理者は、ビデオ監視システムを設置する前に、この手段が第一に目的を達成することに適当であるかどうか、第二に目的に対して適切かつ必要であるかどうかを常に批判的に検討する必要がある。ビデオ監視システムは、データ主体の基本的な権利及び自由への侵害が少ない他の手段によって、取扱いの目的が合理的に達成できない場合にのみ選択されるべきである。

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.

管理者が不動産関連の犯罪を防止したいと考えている場合、管理者は、ビデオ監視システムを設置する代わりに、不動産を柵で囲い、警備員による定期的なパトロールを導入し、門番を置き、照明の数を増やし、セキュリティロックやいたずら防止の窓や扉を設置し、又は落書き防止用コーティングの施工若しくは壁へのホイルの貼付をするなど、別のセキュリティ対策を講じることも可能である。これらの対策は、強盗、窃盗、破壊行為に対してビデオ監視システムと同等の効果が期待できる。管理者は、このような対策が合理的な解決策になるかどうかをケース・バイ・ケースで評価しなければならない。

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.

管理者は、カメラシステムを運用する前に、ビデオ監視措置が、必要な場所と時間を厳密に評価する義務を負っている。通常は、夜間及び通常勤務時間外に作動する監視システムは、不動産への危険を防止するためのニーズを満たすものである。

27. In general, the necessity to use video surveillance to protect the controllers' premises ends at the property boundaries.¹¹ 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.

一般に、管理者の不動産を保護するためにビデオ監視を使用する必要性は、敷地の境界内にとどまる¹¹。しかし、効果的な保護のためには、敷地内の監視だけでは不十分な場合がある。個々のケースでは、ビデオ監視の対象を敷地の周辺にまで広げる必要があるかもしれない。この場合、管理者は、例えば関係のない区域について遮断又はピクセル化などの物理的及び技術的な手段を考慮する必要がある。

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.

例: 書店が、その店舗を破壊行為から保護したいと考えている。当該目的に照らしてビデオ監視は、書店の敷地内のみを撮影すべきであり、敷地周辺の公共区域を監視する必要はありません。

- 28.

¹¹ This might also be subject to national legislation in some Member States.
また、一部の加盟国ではこれも国内法の義務に服する場合もある。

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 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.

取扱いの必要性に関する疑問は、証拠の保全方法についても生じる。いくつかのケースでは、一定の保存期間後に映像が自動的に削除され、また事件が発生した場合にのみ映像にアクセスできるようなブラックボックス方式を利用することが必要かもしれない。また、映像を記録する必要がない場合もあるが、ブラックボックス方式とリアルタイム監視のどちらを選択するかは、目的に基づいて決定する必要がある。例えば、ビデオ監視の目的が証拠保全であれば、リアルタイムの方法は通常適していない。また、リアルタイム監視は、映像を保存して、一定期間経過後に、自動的に削除するよりも侵入性が高い場合がある(例えば、誰かが常にモニター見ている場合、モニターがなく、映像が直接ブラックボックスに保存される場合よりも侵入性が高い場合がある)。データの最小化の原則は、この文脈において考慮されなければならない(第5条第1項(c))。また、管理者は、ビデオ監視の代わりに、即座に対応し介入できる警備員を利用することも可能であることを念頭に置くべきである。

3.1.3 Balancing of interests

正当な利益の均衡を図ること

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.

仮に管理者の正当な利益を保護するためにビデオ監視が必要な場合、管理者又は第三者の正当な利益(例えば、財産又は身体的な完全性の保護)がデータ主体の利益又は基本的な権利及び自由に優先しない場合に限り、ビデオ監視システムを作動させることができる。管理者は、1)監視が個人の利益、基本的な権利及び自由にどの程度影響を及ぼすか、2)これがデータ主体の権利を侵害又はこれに悪い結果を生じさせるかどうか、について考慮する必要がある。実際、正当な利益の均衡を図ることは必須である。一方で基本的な権利及び自由、他方で管理者の正当な利益について、慎重に評価し、また均衡をとらなければならない。

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 customers' 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.

例: 民間の駐車場会社では、駐車場内の車が盗難の被害にあうことを繰り返し文書化している。駐車場は開放された空間であり、誰でも容易にアクセスできるものの、駐車場の周囲には標識やロードブロッカーが設置されている。駐車場会社は、駐車場利用者の車の盗難を防ぐという正当な利益があるため、盗難が発生している時間帯にこの区域を監視することにした。データ主体が監視されるのは限られた時間であり、データ主体は娯楽目的でその区域にいるわけではなく、また、盗難が防止されることはデータ主体自身の利益にもなる。この場合、データ主体の監視されたくないという利益は、管理者の正当な利益によって優先される。

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.

例：レストランが、衛生設備の清潔度を管理するためにトイレにビデオカメラを設置することにした。この場合、データ主体の権利は明らかに管理者の正当な利益を明らかに上回っているため、カメラをそこに設置することはできない。

31.

3.1.3.1 Making case-by-case decisions

ケース・バイ・ケースの決定

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.

規則によれば正当な利益の均衡を図ることは必須であるため、その決定はケース・バイ・ケースで行われなければならない(第6条第1項(f)参照)。抽象的な状況を参照する、類似のケースを相互に比較するのみでは不十分である。管理者は、データ主体の権利を侵害するリスクを評価しなければならない。この場合、個人の権利及び自由への介入の強さが決定的な基準となる。

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.

この強さは、特に、収集される情報の種類(情報内容)、範囲(情報密度、空間的及び地理的範囲)、(人数又は関連する人数の割合として)関係するデータ主体の数、問題となっている状況、データ主体の集団の実際の利益、代替手段、及びデータ評価の性質と範囲によって決められる。

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.

均衡を図る重要な要素は、監視対象区域の広さと、監視対象となるデータ主体の数である。遠隔地でのビデオ監視の利用目的(例えば野生動物の観察又は私有の無線アンテナなどの重要なインフラの保護)は、歩行者ゾーンやショッピングモールでのビデオ監視とは異なる評価をしなければならない。

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.¹¹

例: (例えば事故が起きた場合に証拠を収集する目的で)ドライブレコーダーを設置する場合には、そのカメラによって交通や道路付近にいる人々が常時録画されることのないことを確認することが重要である。そうでなければ、交通事故というかなり理論上の出来事の証拠としてビデオを録画する利益は、データ主体の権利に対する重大な干渉を正当化することはできない¹¹。

- 35.

3.1.3.2 Data subjects' reasonable expectations

データ主体の合理的な期待

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.

前文第47項によれば、正当な利益の存在は慎重に評価する必要がある。この場合、個人データを取扱う時点及び状況におけるデータ主体の合理的の期待を含められなければならない。体系的な監視については、データ主体と管理者との関係が場合により大きく異なることがあり、その点はデータ主体が持つ合理的な期待に影響を与える可能性がある。合理的な期待という概念の解釈は、問題となる主観的な期待のみに基づくべきではない。むしろ、その特定の状況において、客観的な第三者が、監視の対象とされることを合理的に予測し、それを受け入れる判断を下すことができるかどうかを決定的な基準としなければならない。

37. For instance, an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer.¹² 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.

例えば、職場にいる従業員は、ほとんどの場合、雇用者に監視されることを予測していないだろう¹²。また、自宅の庭やリビング、診察室や治療室で監視されることも予測していない。同様に、人々が衛生設備やサウナ施設で監視されることを予測していると考えerことは合理的ではない。そのような区域を監視することは、データ主体の権利を著しく侵害することになる。データ主体が合理的に期待することは、こうした区域においてビデオ監視が行われないことである。一方で、銀行の顧客は、銀行内やATMで監視されることを予測する可能性がある。

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

¹² See also: Article 29 Working Party, Opinion 2/2017 on data processing at work, WP249, adopted on 8 June 2017. また、以下も参照されたい。第 29 条作業部会、業務上のデータの取扱いについての意見 2/2017、WP249、2017 年 6 月 8 日採択。

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.

また、データ主体は、公衆が自由に利用可能な区域において、特にそれが一般に英気の回復、精神的なリフレッシュ、及びレジャー活動に利用されるような場所である場合、また、待合所、レストランの席、公園、映画館、フィットネス施設など個人が滞在したり、コミュニケーションをとったりする場所では、監視されないことも期待できる。ここでは、データ主体の利益又は権利と自由が、管理者の正当な利益に優先されることが多い。

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

例：データ主体は、トイレで監視されないことを期待している。例えば、事故を防ぐためのビデオ監視は比例しない。

39.

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

ビデオ監視についてデータ主体に知らせる標識は、データ主体が客観的に期待できることを判断する際には関係がない。これは、例えば店主が、入口にある標識で、監視していることを入店者に知らせていることだけで、顧客が監視されることについて客観的に合理的な期待を有しているとは言えないことを意味する。

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)

公共の利益において、又は、管理者に与えられた公的機関の権限の行使において行われる職務を遂行する必要性、第6条第1項 (e)

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 in the exercise

of official authority.¹³ 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.

公共の利益において、又は、管理者に与えられた公的機関の権限の行使において行われる職務の遂行のために必要な場合には、第6条第1項(e)に基づきビデオ監視を通じて個人データを取扱うことができる¹³。公的権限の行使では、そのような取扱いが許されていない場合であっても、訪問客や従業員の「健康と安全」を保護するなどの他の法的根拠により、GDPRの義務とデータ主体の権利を考慮しつつ、個人データの取扱いの範囲を限定することができる。

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).

加盟国は、GDPRが定める原則(例えば保存の制限、比例性)に従っている限り、取扱いに関する特定の要件をより正確に定めることにより、GDPRを適用するために、ビデオ監視に関する個別の国内法を維持又は導入することができる。

3.3 Consent, Article 6 (1) (a)

同意、第6条第1項 (a)

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

¹³ 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)).

言及されている取扱いの根拠は、EU法又は加盟国の国内法により定められていなくてはならず、公共の利益において、又は、管理者に与えられた公的機関の権限の行使において行われる職務の遂行のための取扱いに必要なものでなければならない(第6条第3項)。

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

第29条作業部会 (Art.29 WP) 『2016/679規則に基づく同意に関するガイドライン』(WP259 rev.01) - EDPBにより承認。

同意に関するガイドラインで説明されているように、同意は、自由に与えられ、特定され、事前に説明を受け、不明瞭でないものでなければならない¹⁴。

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)).

体系的な監視の場合、データ主体の同意は、例外的な場合にのみ、第7条に従った法的根拠として機能する(前文第43項参照)。こうした監視の性質上、この技術は不特定数の人々を同時に監視する。データ主体が自己の個人データの取扱いについて、事前に同意していることを管理者が証明することはほぼ不可能である(第7条第1項)。データ主体が自己の同意を撤回した場合に、管理者が個人データを以後取扱われていないことを証明することは困難である(第7条第3項)。

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.

例: スポーツ選手が、自己の技術やパフォーマンスを分析するために、各練習中にモニタリングするよう求める場合がある。他方で、スポーツクラブ主導でチーム全体のモニタリングを同じ目的で実施する場合には、個々のスポーツ選手が同意を拒否することでチームメイトに悪影響を及ぼさないよう同意を迫られていると感じるかもしれないため、そのような同意はしばしば有効でない。

- 45.
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.¹⁵

管理者が同意を根拠としたい場合、管理者には、ビデオ監視の対象区域に立ち入るすべてのデータ主体から同意を得られていることを確認すべき義務がある。この同意は、第7条の条件を満たすものでなければならない。標識のある監視区域への立入り(例えば、人々が特定の廊下又はゲートを通過して監視区域に入るよう求められている場合)は、同意に関するガイドラインに記載されている第4条及び第7条の基準を満たさない限り、同意に必要な陳述又は明確な積極的行為を構成しない¹⁵。

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.

雇用者が従業員個人データを取扱う場合、雇用者と従業員との力関係が対等ではない点を考えると、同意が自由に与えられたとは考えにくい。ほとんどの場合、同意に頼るべきではない。この文脈で、同意に関するガイドラインが考慮に入れられるべきである。

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).

加盟国の国内法、又は、『労働協約』を含む団体協約は、雇用関係における労働者の個人データの取扱いに関する特定の規定を定めることができる(第88条参照)。

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

第29条作業部会 (Art. 29 WP) 『2016/67規則に基づく同意に関するガイドライン』 (WP 259) - EDPBにより承認 - これを考慮する必要がある。

4 DISCLOSURE OF VIDEO FOOTAGE TO THIRD PARTIES

第三者へのビデオ映像の開示

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

原則として、GDPRの一般規則はビデオ映像の第三者への開示に適用される。

4.1 Disclosure of video footage to third parties in general

第三者へのビデオ映像の開示全般

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.

開示は、第4条(2)において、送信(例えば個人間の通信)、配布(例えばオンラインでの公開)、又は、その他の方法で利用可能な状態にすることとして定義されている。第三者は、第4条(10)で定義されている。第三国又は国際機関に開示される場合は、第44条などの特別な規定も適用される。

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.

個人データの開示は、管理者が第6条の法的根拠を有する必要がある個人データの別の種類の取扱いである。

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).

例: ビデオ映像をインターネットにアップロードしたい管理者は、例えば第6条第1項(a)に従い、データ主体から同意を得るなど、その取扱いに関する法的根拠に依拠する必要がある。

- 52.
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).

第6条第4項の規定下で行われる場合であれば、個人データが収集された目的以外の目的のためにビデオ映像を第三者に送信することも可能である。

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.

例: 損害賠償を解決する目的で、(駐車場の)壁にビデオ監視が設置されている。損害が発生し、その録画を弁護士に渡して、訴訟を提起する。この場合、録画する目的と移転する目的は同じである。

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).

例: 損害賠償を解決する目的で、(駐車場の)壁にビデオ監視が設置されている。純粋な娯楽目的から録画をオンラインで公開している。この場合、目的は変更されており、当初の目的とは一致しない。さらに、この取扱い(公開すること)についての法的根拠を特定することは困難である。

54.

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).

第三者の取得者は、自らの法的分析を、特に、第6条に基づき自らが取扱う(例えば、資料を受け取る)法的根拠を特定する必要がある。

4.2 Disclosure of video footage to law enforcement agencies

法執行機関へのビデオ映像の開示

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

法執行機関へのビデオ録画の開示も独立したプロセスであり、管理者が取扱うには別の正当な理由が必要になる。

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).

第6条第1項(c)によれば、管理者が従うべき法的義務を遵守するために必要な場合、取扱いは適法である。適用される警察法は加盟国の専権事項であるものの、どの加盟国であれ、法執行機関への証拠開示の移転を規制する一般的な規則が存在する可能性が高い。データを引き渡す管理者の取扱いはGDPRにより規制される。国内法により、法執行機関(例えば捜査)に協力することが管理者に求められている場合、第6条第1項(c)の下での法的義務がデータを引き渡す法的根拠となる

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.

その場合、加盟国の国内法が開示を行う明白な根拠になるため、第6条第4項に規定される目的の限定は問題にならない。したがって、目的を変更するための特別な要件(a)から(e)までについて考慮する必要はない。

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.

例：店主が入り口の映像を録画している。この映像は、ある者が別の人の財布を盗んでいる様子を映している。警察は、その捜査を支援するために、その資料を引き渡すように管理者に求める。この場合、店主は、資料を引き渡す取扱いについて、関連する国内法と併せて読まれる第6条第1項(c)(法的義務)に基づく法的根拠に依拠できる。

- 59.

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.

例：セキュリティ上の理由から、店にカメラが設置されている。その映像に不審なものが移っていると考え、(何らかの捜査が行われている兆候は存在しなかったものの)店主はその資料を警察に送ることにした。このような場合の大半において、店主は、第6条第1項(f)が満たされているかどうかを評価しなければならない。これは通常、犯罪が行われたとの合理的な疑いを持っている場合に当てはまる。

60.

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).

法執行機関自身による個人データの取扱いについては、GDPRに従うのではなく(第2条第2項(d)参照)、代わりに、法執行指令(EU2016/680)に従う。

5 PROCESSING OF SPECIAL CATEGORIES OF DATA

特別な種類のデータの取扱い

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.

ビデオ監視システムは通常、大量の個人データを収集し、その中に極めて個人的な性質のデータや、特別な種類のデータさえも含まれている可能性がある。実際、もともとビデオによって収集された、一見重要でないデータが、別の目的(例えば個人の習慣をマッピングすること)を達成するため他の情報を推測するために使われることがある。しかし、ビデオ監視は、特別な種類の個人データを取扱っているとは必ずしも考えられていない。

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.

例: データ主体が眼鏡をかけている、車椅子を利用していることを映すビデオ映像は、それ自体が特別な種類の個人データであるとはみなされない。

- 63.
64. However, if the video footage is processed to deduce special categories of data Article 9 applies.

しかし、特別な種類のデータを推論するために、ビデオ映像が取扱われる場合には、第9条が適用される。

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.

例: 例えば、特定可能なデータ主体がイベントに参加したり、ストライキを行ったりする等の様子を映した画像からは政治的見解が推測されうる。これは第9条に該当する。

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).

例：病院が患者の健康状態を監視するためにビデオカメラを設置する行為は、特別な種類の個人データの取扱いであるとみなされる(第9条)。

65.

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.

一般的には、原則として、ビデオ監視システムを設置する際は、データ最小化の原則を慎重に考慮すべきである。したがって、第9条第1項が適用されない場合でも、データ管理者は、目的にかかわらず、(第9条を超えて)他のセンシティブデータを示す映像を撮影するリスクを常に最小限に抑えるよう努めるべきである。

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.

例：教会を撮影するビデオ監視は、それだけでは第9条に該当しない。しかし、管理者がデータ主体の利益を評価する際は、データの性質や(第9条を超えた)他のセンシティブデータを撮影するリスクを考慮して、第6条第1項(f)の下で慎重に評価しなければならない。

67.

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.

特別な種類のデータを取扱うためにビデオ監視システムを利用する場合、データ管理者は、第9条に基づく特別な種類のデータを取扱うための例外(つまり、特別な種類のデータを取扱ってはならないという一般的な規則からの除外)と第6条に基づく法的根拠の両方を特定しなければならない。

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.

例えば、第9条第2項(c)（「(略) データ主体又はその他の自然人の生命に関する利益を保護するために取扱いが必要となる時(略)」)は、理論上及び例外的に使用することができるものの、データ管理者は、人の生命に関する利益を保護するために絶対的に取扱いが必要であることを正当化しなければならず、また、その「(略) データ主体が物理的又は法的に同意を与えることができない」ことを証明しなければならない。さらに、それ以外の理由でデータ管理者がそのシステムを利用することは認められない。

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.

ここで重要なことは、第9条に記載されているすべての適用除外事項が、いずれもビデオ監視による特別な種類のデータの取扱いを正当化するためには使用できない可能性が高いということである。より具体的には、ビデオ監視の過程でこれらのデータを取扱うデータ管理者は、データ主体によって明らかに公開された個人データに関連する取扱いを認める第9条第2項(e)に依拠することはできない。データ主体がビデオ監視の対象区域に入ったという事実のみでは、データ主体が自己に関連する特別な種類のデータを公開する意図があることを示唆するものではない。

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.

さらに、特別な種類のデータを取扱うには、例えば、必要に応じて高度なセキュリティやデータ保護影響評価など、特定の義務に対する高度で継続的な警戒が必要となる。

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

例：雇用者は、ストライキの参加者を特定するために、デモの様子を撮影したビデオ監視の映像を使用してはならない。

72.

5.1 General considerations when processing biometric data

生体データの取扱いの際の一般的な考慮事項

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.

生体データ、特に顔認識の使用は、データ主体の権利に対するリスク高める。そのような技術に頼る場合は、GDPRに規定されている適法性、必要性、比例性、及びデータ最小化の原則を十分に尊重することが肝要である。これらの技術の利用は特に効果的であると考えられるものの、管理者はまず、基本的な権利及び自由への影響を評価し、取扱いの正当な目的を達成するために、より侵入性の低い手段を考慮するべきである。

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. ¹⁶

¹⁶ Recital 51 GDPR 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. [...]*”.

自然人の身体的、生理的又は行動的な特性などの生データの取扱いが、GDPRで定義されている生体データとしてみなされるには、その取扱いが、こうした特性の測定を示唆するものでなければならない。生体データはそのような測定の結果として得られるものであるため、GDPRの第4条(14)において、それが「(略) 自然人の身体的、生理的又は行動的特性に関連する特別な技術的取扱いから得られる、当該自然人を一意に識別できるようにするもの、又はその識別を確認するもの。(略)」と述べる。しかし、個人についてのビデオ映像が、その個人の識別に資するために特別な技術処理を行われた稲井場合は、それ自体を第9条に基づく生体データであるとみなすことはできない¹⁶。

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”.

それが特別な種類の個人データの取扱い(第9条)とみなされるためには、生体データの取扱いが「自然人を一意に識別することを目的」で取扱われることが必要である。

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

要するに、第4条(14)及び第9条に照らして、三つの基準が考慮されなければならない。

- **Nature of data** : data relating to physical, physiological or behavioural characteristics of a natural person,
データの性質: 自然人の身体的、生理的又は行動的な特性に関するデータであること。
- **Means and way of processing** : data “resulting from a specific technical processing”,
取扱いの手段及び方法: 「特別な技術的取扱いから得られる」データであること。
- **Purpose of processing**: data must be used for the purpose of uniquely identifying a natural person.
取扱いの目的: データ、自然人を一意に識別することを目的として利用されなければならない。

GDPR 前文第 51 項はこの分析を支持し、「(略) 写真の取扱いは、特別な種類の個人データの取扱いであると即断してはならない。なぜなら、自然人を一意に識別又は認証をすることができる特別な技術的手段を用いて取扱われる場合においてのみ生体データに含まれるからである。(略)」と記載されている。

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.

民間団体が独自の目的(例えば、マーケティング、統計、又は、セキュリティ目的さえも含む)のために設置した生体認証機能を含むビデオ監視の利用は、ほとんどの場合にはすべてのデータ主体からの明示的な同意が必要となり(第9条第2項(a))、もつとも、第9条の他の適切な例外も適用される可能性がある。

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.

例: 民間企業が、サービス向上のために、空港内の乗客識別チェックポイント(手荷物預かり、搭乗)をビデオ監視システムに置き換え、顔認識技術を用いて、そのような手続きに同意することを選択した乗客の身元を確認するその取扱いは第9条に該当するため、事前に明確にかつ説明を受けた上での同意を与えていた乗客は、それぞれの搭乗券と身元証明に関連付けられた顔のテンプレートを作成して登録するために、例えば自動端末に登録しなければならないことになる。顔認識機能を備えたチェックポイントは、明瞭に分離されている必要があり、例えば、同意していない者の生体認証用テンプレートが取り込まれないよう、システムはゲート内に設置されなければならない。事前に同意を与え、かつ登録した乗客のみが、生体認証システムを備えたゲートを利用する。

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.

例：管理者は、顔認識技術を用い、建物へのアクセスを管理している。(第9条2項(a)に従い)明確に説明を受けた上での同意を事前に与えている場合にのみ、このアクセス方法を利用できる。しかし、事前に同意を与えていない者のデータが取り込まれることのないことを確保するためには、例えばボタンを押すなどの方法によるなど、データ主体自身が顔認識機能を作動させるようにするべきである。取扱いの適法性を確保するために、管理者は、バッジや鍵など、生体認証の取扱いなく建物にアクセスするための代替手段を常に提供しなければならない。

78.

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.

生体認証用のテンプレートが作成されるケースでは、管理者は、一致又は不一致の結果が得られた場合、データ主体が登録時に作成したテンプレートと比較するために(データ主体の明確かつ説明を受けた上での同意のもとに)、その場で作成したすべての中間テンプレートを直ちに安全に削除することを保証しなければならない。登録のために作成されたテンプレートは、取扱いの目的を実現する目的でのみこれを保持されなければならない。また、保存又は保管をしてはならない。

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.

しかし、取扱いの目的が、例えば、あるカテゴリーの人々を他のカテゴリーの人々と区別することであり、誰かを一意に識別することではない場合、その取扱いは第9条に該当しない。

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).

例: 店主が、ビデオ監視システムで撮影した顧客の性別と年齢の特徴に基づいて、広告をカスタマイズしたいと考えている。そのシステムが、顧客を一意に識別するための生体テンプレートを作成するのではなく、むしろ人を分類するために身体的特徴を検出するだけであれば(他の特別な種類のデータが取扱われない限り)、その取扱いは第9条のケースに該当しない。

- 81.
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.

ただし、管理者が個人を一意に識別するために生体データ(最も一般的には、生体データの生データから主要な特徴(例えば、画像から顔の測定)を抽出して作成するテンプレートを通じて)を保存する場合には、第9条が適用される。管理者がその区域にデータ主体の再入場又は別の区域への入場を検出したい場合(例えばカスタマイズされた広告を継続的に表示するため)、その目的は自然人を一意に識別することであり、その運用は最初から第9条のケースに該当することとなる。また、管理者が、カスタマイズされた広告を店内のさまざまな場所にある複数の看板で提供するために、作成されたテンプレートを保存する場合にも該当し得る。このシステムは、個人の身体的特徴を利用して、カメラの監視範囲内に戻ってきた特定の人(ショッピングモールの来訪者など)を検出・追跡し、特定の技術的処理を利用して認識することを目的としているため、生体認証に該当する。

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.

例: 店主が、個人向けの広告をカスタマイズするため、顔認識システムを店内に設置した。データ管理者は、この生体認証システムを利用してカスタマイズされた広告を届ける前に、すべてのデータ主体から明確かつ十分な情報を提供したうえで、同意を得なければならない。このシステムは、生体テンプレートの作成に同意していない訪問客や通行人を撮影した場合、たとえテンプレートが可及的速やかに削除されたとしても、そのシステムは違法である。実際、これらの一時的なテンプレートは、ターゲティング広告の受け取りを希望しない者を一意に識別するために生体データの取扱いを構成する。

83.

84. The EDPB observes that some biometric systems are installed in uncontrolled environments¹⁷, 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.

欧州データ保護会議 (EDPB) は、一部の生体認証システムが管理されていない環境に設置されていること¹⁷を指摘している。すなわち、そのシステムが、生体認証装置の作動に同意していない人々を含め、カメラの視野を横切るいかなる個人の顔をその場で撮影し、それにより生体テンプレートを作成していると考ええる。こうしたシステムでは、その後、取り込んだテンプレートを、その個人が登録時に事前に同意したデータ主体 (つまり、生体認証システムのユーザー) のテンプレートと比較し、データ管理者がその人が生体認証システムのユーザーであるかどうかを認識することができる。この場合、データベースから認識したい個人と、登録していない個人を識別するように設計されていることが多い。自然人を一意に識別することが目的のため、やはりカメラで撮影されるいかなる人についてGDPR第9条第2項に定める例外に該当する必要がある。

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

¹⁷ 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.

これは、この生体認証装置が、管理された環境にあって同意している者の参加によってのみ利用される生体認証システムとは対照的に、公開された空間に配置され、通行人なら誰でも対象にされうることを意味する。

guests monitored (in order to identify the VIPs) have consented to the processing according to Article 9 (2) (a) GDPR.

例: ホテルが、ビデオ監視システムを利用して、VIPの顔を認識すると、そのVIPが到着したことをホテルのマネージャーに自動的に通知することができる。これらのVIPは、その目的で構築されたデータベースに登録される前に、顔認識の使用に明確に同意している。(VIPを識別する目的で)監視される他のすべての利用客が、GDPR第9条第2項(a)に従ってその取扱いに同意しない限り、生体データのこうした取扱いシステムは違法である。

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.

例: 管理者が、自らが管理するコンサートホールの入り口に顔認識機能を備えたビデオ監視システムを設置する。管理者は、生体認証システムを備えた入り口と、これを備えない(代わりに、例えばチケットをスキャンする)入り口の両方を設け、両者を明瞭に分けなければならない。生体認証システムを備えた入り口であっても、それに同意していない観客の生体テンプレートをシステムが取得できないように設置し、自由に利用できるものでなければならない。

85.

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.

最後に、GDPR第9条に基づき、同意を得ることが求められる場合、データ管理者は、生体データの取扱いを受け入れることをサービスへのアクセスを認める条件としてはならない。言い換えれば、特に生体データの取扱いが認証目的で利用される場合、データ管理者は、データ主体に対する制約や追加費用なしに、生体データの取扱いを伴わない代替方法を提供しなければならない。また、この代替方法は、生体認証システムの制約条件を満たさない人(生体データの登録又は読み取りが不可能な場合、障害を抱えているために使用が困難であるなど)に対しても必要であり、また、生体認証システムが利用できない場合(例えば装置の故障など)を想定して、その利用が例外的な場合に限定されるとしても、提案されたサービスの継続性を確保するための「バックアップ手法」も導入しなければならない。例外的なケースではあるものの、例えば博物館が顔認識システムの利用方法を実演するための展示会を開催する場合、など、生体データの取扱いが契約により提供されるサービスの中核的な活動となっている場合もある。その場合、データ主体が展示会への参加を希望した場合、生体データの取扱いを拒否することはできない。そのような場合でも、第7条の要件が満たされていれば、なお、第9条に基づいて要求される同意は依然として有効である。

5.2 Suggested measures to minimize the risks when processing biometric data

生体データの取扱いの際のリスクを最小限に抑えるために提案される措置

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.

データ最小化の原則の遵守において、データ管理者は、テンプレートを構築するためにデジタル画像から抽出されるデータが過剰でなく、特定された目的に必要な情報のみが含まれ、それによりそのデータの、起こりうる追加的取扱いを回避することを確保しなければならない。生体認証システム間でテンプレートを移転できないよう保証するための措置が講じられるべきである。

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.

識別及び認証／検証は、後で比較する際に利用するためにテンプレートを保存する必要がある可能性が高い。データ管理者は、データの保存に最適な場所を考慮しなければならない。管理された環境(区切られた廊下又はチェックポイント)において、テンプレートはユーザーが保管し、ユーザーのみが操作できる個々のデバイス(スマートフォン又はIDカード内など)に保存するか、または、特定の目的のために必要で、客観的なニーズがある場合には、テンプレート又は保存場所への不正アクセスを防止するために、本人のみが所持する鍵／秘密を用いて、暗号化された状態で集中化されたデータベースに保存されるべきである。データ管理者がテンプレートへのアクセスを回避できない場合、データ管理者は、保存されているデータのセキュリティを確保するための適切な手段をとらなければならない。これには、暗号化アルゴリズムを利用してテンプレートを暗号化することを含むだろう。

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.

いかなる場合においても、管理者は、取扱われるデータの可用性、完全性、及び機密性を維持するために必要なあらゆる予防措置を講じなければならない。この目的のため、管理者は特に以下の措置を講じなければならない:送信時及び保存時のデータの区分化、生体

テンプレートと生データ又はアイデンティティデータの区別されたデータベースへの保存、生体データ(特に生体テンプレート)の暗号化、暗号化及び鍵の管理についてのポリシーの策定、不正検知のための組織的・技術的な対策の統合、データへの整合性コード(例えば、署名やハッシュなど)の関連付け、並びに、生体データへの外部からのアクセスの禁止などが挙げられます。このような対策は、技術の進歩に合わせて発展していく必要がある。

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.

また、データ管理者は、生データ(顔画像、音声信号、歩行など)の削除を進め、この削除の有効性を確保するべきである。取扱いの法的根拠が失われた場合には、生データを削除しなければならない。実際に、(生体テンプレートの場合にはどのようにプログラムされたかについて理解していない限り解読することが必ずしも容易ではない一方、生データはあらゆるテンプレートの構成要素になるため)生体テンプレートを生データから作成する限り、データベースの構成は、より大きな脅威ではないにしても、同等の脅威があると考えることができる。データ管理者がそのようなデータを保管しなければならない場合、ノイズを付加する方法(電子透かしなど)を検討し、テンプレートの作成を無効にする必要がある。管理者は、読取比較端末又はストレージサーバーに不正アクセスが発生した場合には、生体データとテンプレートを削除し、また、生体認証装置の耐用期間終了後には、今後の取扱いに不要なデータを削除しなければならない。

6 RIGHTS OF THE DATA SUBJECT

データ主体の権利

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.

ビデオ監視を利用する場合におけるデータの取扱いの特性により、GDPRに基づく一部のデータ主体の権利は、さらに明確化が必要となる。しかし、本章は、GDPRに基づくすべての権利がビデオ監視による個人データの取扱いに適用されるため、網羅的ではないことにご留意いただきたい。

6.1 Right to access

アクセスする権利

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.

データ主体は、自己に関係する個人データが取扱われているか否かを管理者へ確認できる権利を有する。ビデオ監視の場合、これは、データがいかなる方法でも保存又は移転されていない場合、リアルタイムの監視の瞬間が過ぎた後は、管理者にとって、(第13条に基づく一般的な情報義務については、第7章 – 透明性及び情報に関する義務を参照。)いかなる個人データもはや取扱われていないとデータ主体に回答するしかないことを意味する。しかし、データ主体の要求時にデータがまだ取扱われている(つまり、データが保存されている、他の方法で継続的に取扱われている)場合、データ主体は、第15条に従ってアクセスと情報を受領するようにすべきである。

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

ただし、いくつかの場合ではアクセスの権利に関して一定の制限が適用され得る。

- Article 15 (4) GDPR, adversely affect the rights of others

GDPR第15条第4項、他の者の権利に不利な影響を及ぼす場合

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).

一連のビデオ監視において、何人ものデータ主体が録画されている可能性があることを考えると、スクリーニングによって、他のデータ主体の個人データが追加で取扱われることになる。データ主体が資料の複製物を受け取りたいと考える場合(第15条第3項)、それが資料内の他のデータ主体の権利及び自由に悪影響を及ぼす可能性がある。したがって、管理者は、こうした影響を防ぐため、ビデオ映像には侵害的な性質があることから、他のデータ主体を識別できる場合にはビデオ映像を引き渡してはならない場合があることを考慮すべきである。ただし、第三者の権利の保護が、個人による正当なアクセス要求を拒絶する口実にご利用されるべきではなく、この場合、管理者はアクセス要求を充足するための(例えば、マスキングやスクランブル処理などによる画像の編集の)技術上の措置を実施すべきである。しかし、管理者が、他の方法により、第12条第3項で規定されている期間内に第15条に基づく要求に応じることを他の方法で保証できる場合には、そのような技術的措置を実施する義務を負わない。

- Article 11 (2) GDPR, controller is unable to identify the data subject

GDPR第11条第2項、管理者がデータ主体を識別できない場合

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.

ビデオ映像が個人データを検索できるようなものではない場合(つまり、問題となるデータ主体を見つけるために管理者が保存された大量の資料を閲覧しなければならない可能性が高い場合)、管理者はデータ主体を識別できない可能性がある。

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.

これらの理由により、データ主体は、管理者への要求において(身元証明書で又は直接会うなどの方法で自らを識別する他に)、録画されているデータ主体の数に比例した妥当な時間の枠内で、いつ監視区域に立ち入ったかを特定するべきである。管理者は、要求に応じるためにどのような情報が必要かを、データ主体に事前に通知するべきである。管理者がデータ主体を特定できないことを証明できる場合、管理者は、可能であれば、そのことをデータ主体に知らせなければならない。このような状況のもと、管理者は、データ主体への回答において、正確な監視区域、使われたカメラの検証などを伝え、データ主体がどのような個人データが取扱われたかを完全に理解できるようにする必要がある。

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.

例: データ主体が、1日あたり3万人の訪問客がいるショッピングモールの入り口で、ビデオ監視により取扱われた個人データのコピーを要求する場合、そのデータ主体は、自分が監視対象区域を通過した時間帯を1時間程度の時間枠で特定すべきである。管理者がまだビデオ映像を取扱っている場合には、そのコピーを提供すべきである。同じ映像から他のデータ主体が識別できる場合は、要求を行ったデータ主体にコピーを提供する前に資料のその部分を匿名化(例えば、コピー又はその一部をぼかすこと)すべきである。

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.

例: 管理者が、あらゆる映像を例えば2日以内に自動的に消去している場合、管理者は、その2日後にデータ主体へ映像を提供することはできない。管理者が2日後に要求を受けた場合には、その旨をデータ主体へ知らせるべきである。

97.

- Article 12 GDPR, excessive requests
GDPR第12条、過剰な要求

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.

データ主体からの要求が過剰であるか又は明らかに根拠がない場合、管理者は、GDPR第12条第5項(a)に従って合理的な料金を課金するか、又は、要求された行為を拒むことができる(GDPR第12条第5項(b))。管理者は、その要求の明白な根拠がないか又は過剰な性質を証明できる必要がある。

6.2 Right to erasure and right to object

消去の権利と異議を述べる権利

6.2.1 Right to erasure (Right to be forgotten)

消去の権利(忘れられる権利)

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.

管理者がリアルタイムの監視を超えて(例えば保存など)個人データの取扱いを継続する場合、データ主体は、GDPR第17条の下で個人データの消去を要求できる。

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:

GDPR第17条第1項に掲げる状況のいずれかに該当する場合(かつ、GDPR第17条第3項に掲げる例外のいずれにも該当しない場合)、管理者はデータ主体からの要求に応じ、個人データを不当に遅滞なく消去する義務を負う。これには、その個人データが、それが当初保存され目的との関係で、もはや必要のないものとなっている場合、又はその取扱いが違法である場合に個人データを消去すべき義務が含まれる(第8章 – 保存期間と消去義務も参照)。さらに、取扱いのための法的根拠に応じて、以下の場合に個人データが消去されるべきである。

- *for consent* whenever the consent is withdrawn (and there is no other legal basis for the processing)

同意については、その同意が取り下げられた(また、取扱いのための他の法的根拠が存在しない)場合

- *for legitimate interest*:

正当な利益については:

- 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

データ主体が異議を述べる権利を行使し(6.2.2参照)、取扱いについての優先される、やむをえない正当な根拠がない場合、又は

- in case of direct marketing (including profiling) whenever the data subject objects to the processing.

(プロファイリングを含む)ダイレクト・マーケティングの場合には、データ主体が取扱いに異議を述べたとき。

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.

管理者がビデオ映像を公開している場合(例えば放送又はオンラインのストリーミングなど)、GDPR第17条第2項に従って、要求を(問題となる個人データを現在も取扱っている)他の管理者に通知するために、合理的な措置を講じる必要がある。この合理的な措置には、利用可能な技術及び実施のためのコストを考慮した技術的措置が含まれるべきである。管理者は、可能な範囲で、GDPR第19条に従い、個人データの消去時に、以前にそのデータの開示を受けた者に通知するべきである。

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*).

データ主体の要求に応じて個人データを消去すべき管理者の義務に加え、管理者は、GDPRの一般原則に基づき、保存されている個人データを制限する義務を負う(第8章を参照)。

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.

ビデオ監視の場合、例えば、画像をぼかすことで、その画像に以前含まれていた個人データを遡及的に復元できない場合、GDPRに従って個人データが消去されたとみなされる点は注意する必要がある。

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.

例: コンビニエンス・ストアが、特に何者かによる外壁に対する破壊行為に困っており、壁に直接面している入り口の外でビデオ監視を利用している。通行人が自身の個人データを瞬時に消去することを要求してきた。管理者は、要求に対して不当に遅滞することなく、遅くとも1か月以内に対応すべき義務を負う。問題の映像は、当初保存されていた目的を満たしていない(データ主体が通過する間に破壊行為が発生していなかった)以上、要求を受けた時点で、データ主体の利益より優先するデータを保存する正当な利益は存在しない。そのため、管理者は、個人データを消去する必要がある。

104.

6.2.2 Right to object

異議を述べる権利

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.

ビデオ監視が正当な利益に基づく(GDPR第6条第1項(f))又は公共の利益において職務を遂行する際の必要性(GDPR第6条第1項(e))のために必要である場合、データ主体は、自身の特定の状況に関連する根拠に基づき、GDPR第21条に基づく取扱いにいつでも異議を唱える権利を有する。管理者が、データ主体の権利と利益に優先されるやむを得ない正当な根拠を証明しない限り、異議を述べた個人のデータの取扱いを停止しなければならない。管理者は、データ主体からの要求に遅滞なく、遅くとも1か月以内に回答する義務を負う。

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

ビデオ監視の場合、この異議は、監視区域に入ったとき、そこにいる間、又はその区域を出た後に述べることができる。実際には、管理者にやむを得ない正当な根拠がない限り、自然人を識別できる区域を監視することは、以下のいずれかの場合にのみ適法であることを意味する。

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

管理者が、要求された時に、カメラによる個人データの取扱いを直ちに停止できる場合、または

(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.

監視区域が、管理者がデータ主体から当該区域に立ち入る前に承諾を得ることを保証できるように詳細に制限されており、また、市民としてのデータ主体がアクセスできる区域ではない場合。

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

本ガイドラインは、何がやむを得ない正当な利益(GDPR第21条)とみなされるものを特定することを目的としない。

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).

ダイレクト・マーケティングを目的としてビデオ監視を利用する場合、その文脈における異議を述べる権利は絶対的なものであるため、データ主体は自らの裁量により取扱いに異議を述べる権利を有する。(GDPR第21条第2項及び第3項)。

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.

例：企業が、一般の出入り口において、セキュリティ違反をめぐる問題を抱え、不法侵入者を捕まえる目的で、正当な利益を理由にビデオ監視システムを利用している。訪問者が、自身の特定の状況に関連する理由で、ビデオ監視システムを介して自分のデータを取扱うことに異議を述べる。しかし、このケースにおいて、その企業は、内部調査を継続しているために保存された映像が必要でありしたがって個人データの取扱いを続行するやむをえない正当な根拠を有すること、を説明し、その要求を拒否する。

109.

7 TRANSPARENCY AND INFORMATION OBLIGATION¹⁸

透明性と情報に関する義務¹⁸

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.¹⁹ 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 25th 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 [...])."

欧州のデータ保護法では、データ主体は、ビデオ監視が行われていることを認識すべきであるとされてきた。データ主体は、監視されている場所について詳細に知らされるべきである¹⁹。GDPRでは、透明性と情報に関する一般的な義務を第12条以下で定めている。2018年5月25日にEDPBにより承認された第29条作業部会の「規則に基づく透明性に関するガイドライン2016/679 (WP260)」では、さらなる詳細が記載されている。WP260第26項に沿って、個人データが「(略) (例えば、カメラなどの自動化されたデータ取込装置又はデータ取込ソフトウェアを利用して) 観察によりデータ主体から(略)」収集されている場合に適用されるのはGDPR第13条である。

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).

データ主体に提供する必要のある情報量を考慮して、データ管理者は透明性を確保するために、複数の方法を組み合わせて階層的に行うことができる (WP260第35項、WP89第

¹⁸ Specific requirements in national legislation might apply.

国内法の特定の要件が適用されるかもしれない

¹⁹ See WP859, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance by Article 29 Working Party.

第29条作業部会による、ビデオ監視の方法による個人データの取扱いに関する意見4/2004、WP859を参照されたい。

22項)。ビデオ監視については、最も重要な情報は警告標識自体(第1層)に表示し、それ以上の必須情報はほかの手段(第2層)により提供することができる。

7.1 First layer information (warning sign)

第1層の情報(警告標識)

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1層は、管理者がデータ主体と最初に関わりをもつ主要な方法である。管理者は、この段階において、関連する情報を示した警告標識を使用することができる。表示される情報は、容易に視認でき、分かりやすく、明確に理解できる態様で、予定されている取扱いの意味のある概要を提供するためのアイコンと組み合わせて提供することができる(GDPR第12条第7項)。情報の形式は、個々の場所に合わせて調整されるべきである(WP89第22項)。

7.1.1 Positioning of the warning sign

警告標識の設置位置

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.

情報は、データ主体が監視区域に立ち入る前に、監視の状況を容易に認識できるように(およそ目の高さ)配置するべきである。どの区域が監視されているかについて疑問の余地がなく、監視の状況が明確になっていれば、カメラの位置を明らかにする必要はない(WP89第22項)。データ主体は、監視を回避し、又は必要に応じて自らの行動を調整できるように、カメラに取り込まれる区域を推定できなければならない。

7.1.2 Content of the first layer

第1層の内容

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.²⁰ 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1層の情報(警告標識)では、一般的に最も重要な情報、例えば取扱い目的の詳細、管理者の身元、データ主体の権利の存在、及び取扱いの最も大きな影響についての情報など、を伝えるべきである²⁰。これには、例えば、管理者(又は第三者)が追求する正当な利益や(該当する場合)データ保護オフィサーの連絡先などの詳細な情報を含めることができる。また、第1層では、更に詳細な第2層の情報と、それをどこでどのように確認できるかについて言及しなければならない。

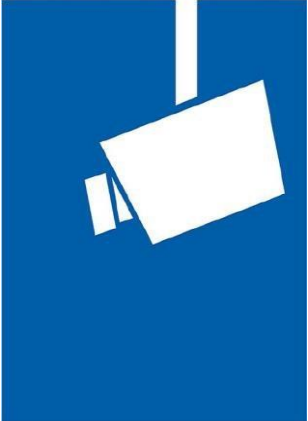

115. In addition the sign should also contain any information that could surprise the data subject (WP260, par. 38). That could for example be transmissions to third parties, particularly if they are located outside the EU, and the storage period. If this information is not indicated, the data subject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

さらに、この標識には、データ主体が想定していない可能性のある事実に関する情報も含めるべきである(WP260第38項)。これには、例えば、第三者への送信(特にその第三者がEU域外に存在する場合)、及び保存期間が考えられる。この情報が表示されていない場合、データ主体は、(データが録画又は第三者に送信されることなく)ライブ監視のみが行われていると信頼してしまうだろう。

²⁰ See WP260, par. 38.

WP260、パラグラフ 38 を参照されたい。

Example (nonbinding suggestion): 例（拘束力のない提案）：

 <p>Video surveillance! ビデオ監視を行っています！</p>	<p><u>Identity of the controller and, where applicable, of the controller's representative:</u> 管理者の身元、及び該当する場合は管理者の代理人の身元：</p>
	<p><u>Contact details, including of the data protection officer (where applicable):</u> データ保護オフィサー（該当する場合）のものを含む、連絡先の詳細：</p>
	<p><u>Information on the processing that has the most impact on the data subject (e.g. retention period or live monitoring, publication or transmission of video footage to third parties):</u> データ主体に最も影響を及ぼす取扱いに関する情報（例えば、ビデオ映像の保存期間、又はライブ監視、公開若しくは第三者への送信）：</p>
	<p><u>Purpose(s) of the video surveillance:</u> ビデオ監視の目的：</p>
 <p>Further information is available: 追加情報は以下で確認できます： ・ via notice 通知 ・ at our reception/ customer information/ register 当社受付/情報案内係/登録 ・ via internet (URL)... インターネット (URL) ...</p>	<p><u>Data subjects rights:</u> As a data subject you have several rights to exercise, 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.</p> <p><u>データ主体の権利：</u>あなたは、データ主体として、いくつかの権利、特にあなたの個人データへのアクセス又はその消去を管理者に要求する権利を行使できます。あなたの権利を含むこのビデオ監視の詳細については、左側に表示された選択肢を通じて管理者によって提供される完全な情報をご参照ください。</p>

116.

7.2 Second layer information

第2層の情報

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.

また、第2層の情報は、データ主体が容易にアクセスできる場所、例えば重要な場所(インフォメーション・デスク、受付、レジなど)に置かれた情報案内用チラシ、で提供されなければならない。前述のように、第1層の警告標識は第2層の情報を明確に参照する必要がある。さらに、第1層の情報が第2層のデジタルデータソース(QRコードやウェブサイトのアドレスなど)を参照していればベストです。しかし、その情報はデジタル形式でなくとも、容易に確認できるものでなければなりません。特に情報をデジタル形式で提供する場合には、監視の対象区域に立ち入ることなく第2層の情報にアクセスできるようにするべきである(これは、例えばリンクを貼ることで実現できる)。その他の適切な手段としては、問い合わせ先電話番号を記載する方法がある。情報をどのような方法で提供するにしても、GDPR第13条で義務付けられているすべての内容を含めなければならない。

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; geo-locating 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.

これらの選択肢に加え、また、これらをより効果的にするため、EDPBでは、データ主体に情報を提供するために技術的手段を利用することを推奨している。これには、例えば位置情報機能を備えたカメラを設置し、地図アプリやウェブサイトに情報を掲載することで、個人が自分たちの権利行使に関連するビデオデータソースを特定できるようにし、他方では取扱業務に関するより詳細情報を取得できるようにすることが含まれる。

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.

例: 店主が自分の店を監視している。第13条を遵守するためには、自店の入り口の容易に視認できる場所に第1層の情報が含まれる警告表示を置けば十分である。さらに、店主は店のレジその他の重要かつ容易にアクセスしやすい場所に第2層の情報を含む情報案内用チラシを置かなければならない。

- 119.

8 STORAGE PERIODS AND OBLIGATION TO ERASURE

保存期間と消去義務

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.

個人データは、個人データが取扱われる目的に必要な期間を超えて保存することはできない(GDPR第5条第1項(c)及び(e))。一部の加盟国では、GDPR第6条第2項に基づき、ビデオ監視に関する保存期間について特別規定を定めている場合がある。

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.

個人データを保存する必要があるか否かは短い期間内に管理されるべきである。一般に、ビデオ監視が行われる正当な目的とは、財産の保護や証拠の保全であることが多い。通常、発生した損害は、1～2日以内に認識される。データ保護の枠組みを遵守していることを容易に証明するために、事前に組織的な取決め(例えば、必要に応じて、ビデオ映像のス

クリーニングを行い、保全する代理人を指名するなど)を行うことは管理者の利益になる。GDPR第5条第1項(c)及び(e)の原則、つまりデータの最小化及び保存の制限を考慮すると、ほとんどの場合(例えば、破壊行為を検知する目的など)、個人データを理想的には数日後に自動的に消去するべきである。保存期間が長く設定されるほど(特に72時間を超えて)、目的の正当性と保存の必要性について、より多くの論拠を示す必要がある。管理者が、ビデオ監視を敷地内の監視のためだけではなく、データを保存することも意図する場合、管理者は、目的を達成するために実際に保存する必要があることを保証しなければならない。その場合、保存期間を明確に定義し、それぞれの目的ごとに個別に設定する必要がある。管理者には、必要性及び比例性の原則に従って保管期間を定め、また、GDPRの規定への遵守を証明する責任がある。

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.

例: 小さな店であれば、破壊行為が行われたその日に店主が気付くであろう。そのため、通常の保存期間は24時間で十分である。しかし、閉店している週末やより長い休日は、保存期間を長くする必要がある。また、被害を発見した場合には、犯罪者に対して法的措置を講じるため、店主が、ビデオ映像を通常の場合よりも長期間保存する必要性もあるかもしれない。

122.

9 TECHNICAL AND ORGANISATIONAL MEASURES

技術的及び組織的な措置

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.

GDPR第32条第1項に規定されるように、ビデオ監視における個人データの取扱いは、法的に許容されているだけではなく、管理者及び処理者がそれを十分に保護しなければならない。実施された**組織的及び技術的な措置**は、ビデオ監視映像の偶発的又は違法な破壊、紛失、改ざん、不正な開示またはアクセスによって生じる**自然人の権利及び自由へのリスクに比例的なもの**でなければならない。GDPR第24条及び第25条によれば、管理者は、取扱いにおいてすべてのデータ保護原則を保護し、またデータ主体がGDPR第15条から第22条までに定める自らの権利を行使する手段を確立するためにも、技術的及び組織的な措置を実装する必要がある。データ管理者は、必要に応じて、データ保護影響評価の実施を含め、取扱い手段の決定時及び取扱い時の両方において、この実施を確実にする内部フレームワーク及びポリシーを採用する必要がある。

9.1 Overview of video surveillance system

ビデオ監視システムの概要

124. A video surveillance system (VSS)²¹ consists of analogue and digital devices as well as software for the purpose of capturing images of a scene, handling the images and

²¹ 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.

displaying them to an operator. Its components are grouped into the following categories:

ビデオ監視システム(VSS)²¹は、ある光景の画像を取り込むためのものであって、画像を処理し、オペレータに表示するアナログ及びデジタル装置及びソフトウェアで構成される。その構成要素は以下の各類型に分類される。

- **Video environment: image capture, interconnections and image handling:**
ビデオ環境: 画像の取り込み、相互接続、画像処理。
 - 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,
画像を取り込む目的は、実世界の画像をシステムの他の機能で利用できる形式で生成することにある。
 - 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,
相互接続とは、ビデオ映像内のすべてのデータ伝送、すなわち接続と通信を指す。接続手段の例は、ケーブル、デジタルネットワーク、及び無線伝送である。通信とは、デジタルまたはアナログのすべてのビデオおよび制御データ信号を表す。
 - image handling includes analysis, storage and presentation of an image or a sequence of images.
画像処理には、画像又は一連の画像の分析、保存、表示が含まれる。
- From the system management perspective, a VSS has the following logical functions:
システム管理の観点から、VSSには以下の論理的機能がある。
 - data management and activity management, which includes handling operator commands and system generated activities (alarm procedures, alerting operators),

GDPR ではこの定義を定めていないが、例えば、技術的説明は『EN 62676-1-1: 2014 セキュリティ・アプリケーションで利用されるビデオ監視システム – パート 1-1: ビデオ・システムの要件』で見つけることができる。

データ管理とアクティビティ管理。これには、オペレータのコマンドやシステムが生成するアクティビティ(警告手順、オペレータへの警告)の処理が含まれる。

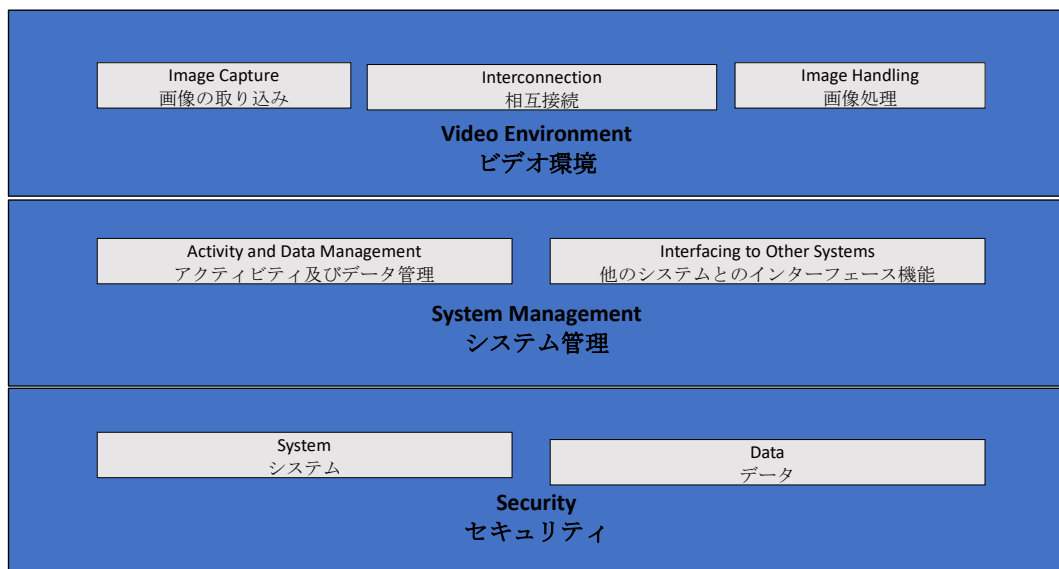
- o interfaces to other systems might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition).

他のシステムとのインターフェースには、他のセキュリティシステム(入退室管理、火災警報)や非セキュリティシステム(ビル管理システム、自動化されたナンバープレート認識)との接続が含まれる場合がある。

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

VSSのセキュリティは、システムとデータの機密性、完全性、可用性で構成される。

- o system security includes physical security of all system components and control of access to the VSS,
システム・セキュリティには、すべてのシステム構成要素の物理的セキュリティとVSSへのアクセス制御が含まれる。
- o data security includes prevention of loss or manipulation of data.
データセキュリティには、データの損失や改ざんの防止が含まれる。



125.

Figure 1- video surveillance system

図1 - ビデオ監視システム

9.2 Data protection by design and by default

データ保護バイデザイン及びバイデフォルト

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 data²².

GDPR第25条に規定されているように、管理者は、ビデオ監視を計画した時点で、つまりビデオ映像の収集と取扱いを開始する前に、適切なデータ保護の技術的及び組織的措置を実施する必要がある。これらの原則は、組み込まれたプライバシー強化技術、データの取扱いを最小限に抑える初期設定、及び個人データを最大限に保護するために必要なツールが提供される必要性を強調する²²。

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.

管理者は、データ保護とプライバシー保護措置を技術の設計仕様だけでなく、組織の慣行にも組み込む必要がある。組織の慣行に関して、管理者は、適切な管理フレームワークを

²² 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、『プライバシーの未来』に関する意見、第29条データ保護作業部会および警察と正義に関する作業部会による、個人データ保護の基本的権利に関する法的枠組みに関する欧州委員会の諮問への共同貢献（2009年12月1日採択）。

採用し、ビデオ監視に関連するポリシーと手続を確立し、実施する必要がある。技術的な観点からは、システムの仕様や設計には、GDPR第5条に規定された原則(取扱いの適法性、目的及びデータの限定、GDPR第25条第2項の意味でのデータ最小化バイデフォルト、完全性と機密性、アカウントビリティなど)に従って個人データを取扱うための要件を含めるべきである。管理者が商業用ビデオ監視システムの購入を計画している場合、その管理者は、購入する際の仕様書にこれらの要件を含める必要がある。管理者は、そのシステムのあらゆる構成要素とそれにより取扱われるあらゆるデータにこれらの要件を適用し、システムのライフサイクル全体を通して要件への遵守を確保する必要がある。

9.3 Concrete examples of relevant measures

関連する措置の具体例

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.

ビデオ監視のセキュリティを確保するために利用できる措置の大半は、特にデジタル機器やソフトウェアを使用する場合、他のITシステムで使用する手段と変わらない。しかし、選択した解決策にかかわらず、管理者は、ビデオ監視システムのあらゆる構成要素及びデータを、あらゆる段階、つまり保存(待機中データ)、送信(送信データ)及び取扱い(使用データ)などで適切に保護しなければならない。そのためには、管理者と処理者が組織的及び技術的な措置を組み合わせる必要がある。

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.²³ On the other hand, the selected solutions should not

²³ 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.

第5条第1項(c)に適合するため、そのような技術の利用が必須でさえあるような場合もある。いずれにせよ、それらが最良の実施事例となりうる。

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.

また、技術的ソリューションを選択する際、管理者は、セキュリティを強化するという理由で、プライバシーに配慮した技術を考慮する必要がある。そのような技術の例は、データ主体にビデオ映像を提供する際に、監視目的に関係のない区域をマスキング又はスクランブル処理すること、又は第三者の画像を編集することが可能なシステムである。²³。他方で、選択した解決策が、不要な機能（カメラの無制限な旋回、ズーム機能、無線送信、分析、音声記録など）を提供してはならない。実装されているものの、必要のない機能は無効にしなければならない。

130. There is a lot of literature available on this subject, including international standards and technical specifications on the physical security of multimedia systems²⁴, and the security of general IT systems²⁵. Therefore, this section provides only a high-level overview of this topic.

このテーマについては、マルチメディアシステムの物理的なセキュリティ²⁴やITシステム全般のセキュリティ²⁵に関する国際規格や技術仕様など、多くの文献が存在する。したがって、本章では、このテーマについての概要のみ説明する。

9.3.1 Organisational measures

組織的な措置

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:

管理者は、ビデオ監視に関する自己の方針及び手続を策定する際に、データ保護影響評価 (DPIA) (第10章を参照) が必要となる可能性以外にも、以下のポイントを考慮するべきである。

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

IEC TS 62045 – マルチメディア・セキュリティ - 使用中及び使用していない機器とシステムのプライバシー保護に関するガイドライン。

²⁵ ISO/IEC 27000 — Information security management systems series.

ISO/IEC 2700 - 情報セキュリティ管理システムのシリーズ。

- Who is responsible for management and operation of the video surveillance system.
ビデオ監視システムの管理及び運用の責任者。
- Purpose and scope of the video surveillance project.
ビデオ監視プロジェクトの目的と範囲。
- 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)²⁶.
適切な使用方法と禁止されている使用方法(ビデオ監視が許される場所と時間、許されない場所と時間; 例えばビデオ録画に加えて隠しカメラ及び音声の使用)²⁶。
- Transparency measures as referred to in *Section 7 (Transparency and information obligations)*.
第7章(透明性と情報に関する義務)で言及されている透明性に関する措置。
- How video is recorded and for what duration, including archival storage of video recordings related to security incidents.
セキュリティ・インシデントに関連したビデオ録画のストレージへの保管を含め、ビデオを録画する方法及び時間。
- Who must undergo relevant training and when.
関連する訓練を受けなければならない者とその時期。
- Who has access to video recordings and for what purposes.
ビデオ録画にアクセスできる者とその目的。
- Operational procedures (e.g. by whom and from where video surveillance is monitored, what to do in case of a data breach incident).
運用手続(例えば、ビデオ監視で監視する者及び監視している場所、データ侵害インシデントが発生した場合の対応)。
- What procedures external parties need to follow in order to request video recordings, and procedures for denying or granting such requests.
外部の当事者がビデオ録画を要求するために従う必要のある手続、及びそのような要求を拒絶又はこれに応諾するための手続。
- Procedures for VSS procurement, installation and maintenance.
VSSを調達、設置し、メンテナンスを行うための手続。

²⁶ This may depend on national laws and sector regulations.
これは、国内法及び産業部門に対する規制に左右される場合がある。

- Incident management and recovery procedures.

インシデント管理及び復旧手続。

9.3.2 Technical measures

技術的な措置

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).

システム・セキュリティとは、あらゆるシステム構成要素の物理的なセキュリティ、及びシステムの完全性、つまり、意図的及び非意図的な正常な動作への感情に対する保護と回復力、およびアクセス制御をいう。データセキュリティとは、機密性(アクセスを許されたユーザーのみがデータにアクセスできること)、完全性(データの損失又は改ざんを防ぐこと)、及び可用性(必要なときにデータにアクセスできること)をいう。

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.

物理的なセキュリティは、データ保護に極めて重要な部分であり、VSS機器を盗難、破壊行為、自然災害、人為的な大災害、及び偶発的な損害(例えば、電気サージ、極端な温度、こぼれたコーヒーなど)から保護するための最初の防衛手段である。アナログベースのシステムの場合、物理的なセキュリティが保護の主な役割を果たす。

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

システム及びデータのセキュリティ、つまり、通常の業務に対する意図的及び意図的でない干渉に対する保護には、以下を含むことができる。

- Protection of the entire VSS infrastructure (including remote cameras, cabling and power supply) against physical tampering and theft.

物理的な改ざんや盗難に対するVSSインフラ全体(リモートカメラ、ケーブル、電源を含む)の保護。

- **Protection of footage transmission with communication channels secure against interception**
傍受されない通信手段による映像伝送の保護
- **Data encryption.**
データ暗号化。
- **Use of hardware and software based solutions such as firewalls, antivirus or intrusion detection systems against cyber attacks.**
ファイアウォール、ウイルス対策、又はサイバー攻撃に対する侵入検知システムなどのハードウェア及びソフトウェア・ベースの解決策の利用。
- **Detection of failures of components, software and interconnections.**
部品、ソフトウェア、及び相互接続をめぐる障害の検知。
- **Means to restore availability and access to the system in the event of a physical or technical incident.**
物理的又は技術的な問題が発生した際に、可用性とシステムへのアクセスを復元する手段。

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:

アクセス制御は、許可された人だけがシステムやデータへアクセスでき、他の人によるアクセスの防止を確保する。物理的及び論理的なアクセス制御を支援する措置には以下にものがある。

- **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.**
ビデオ監視による監視対象及びビデオ映像が保存されるあらゆる施設が第三者による監督を受けないアクセスから保護されるよう確保すること。
- **Positioning monitors in such a way (especially when they are in open areas, like a reception) so that only authorized operators can view them.**
(特に、受付などの開放的な区域に設置されている場合に)許可されたオペレーターのみがモニターを見ることができるよう位置にモニターを配置すること。

- **Procedures for granting, changing and revoking physical and logical access are defined and enforced.**

物理的及び論理的アクセスを許可し、変更し、取り消すための手続が定められ、実施されていること。

- **Methods and means of user authentication and authorization including e.g. passwords length and change frequency are implemented.**

パスワードの長さや変更頻度など、ユーザー認証及び承認のための方法と手段が実施されていること。

- **User performed actions (both to the system and data) are recorded and regularly reviewed.**

ユーザーによる操作(システムとデータの両方)が記録され、定期的にチェックされていること。

- **Monitoring and detection of access failures is done continuously and identified weaknesses are addressed as soon as possible.**

アクセス障害の監視と検知が継続的に行われ、特定された脆弱性が可及的速やかに対処されていること。

10 DATA PROTECTION IMPACT ASSESSMENT

データ保護影響評価

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.

GDPR第35条第1項によれば、ある種類のデータ取扱いが自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者はデータ保護影響評価(DPIA)を実施することが求められる。GDPR第35条第3項(c)では、取扱いが一般にアクセス可能な場所を大規模に体系的に監視するものである場合、DPIAを実施する必要があると規定している。さらに、GDPR第35条第3項(b)によれば、管理者が特別な種類のデータを大規模に取扱う場合にも、DPIAが求められる。

137. The Guidelines on Data Protection Impact Assessment²⁷ 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.

²⁷ 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
WP248 rev.01、データ保護影響評価(DPIA)に関する、及び2016/679規則の目的に即して処理が『高リスクになる可能性が高い』かどうかに関するガイドライン - EDPBにより承認

DPIAに関するガイドライン²⁷では、さらなるアドバイスとより詳細な例(例えば「高速道路における運転行動を監視するためのカメラシステムの利用」など)を提供する。GDPR第35条第4項は、各監督機関が、自国内でDPIAが義務づけられている取扱業務の種類のリストを公表することを求めている。これらのリストは通常、監督機関のウェブサイトに掲載されている。ビデオ監視の典型的な目的(人と財産の保護、犯罪の検知・防止・管理、証拠の収集、被疑者の生体認証)を考えると、ビデオ監視の多くのケースでDPIAが必要になると考えることが妥当である。したがって、データ管理者は、DPIAが必要かどうかを判断するために、これらの文書を注意深く参照する必要がある。実行されたDPIAの結果によって、管理者が実施するデータ保護措置の選択が決まるはずである。

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.

また、DPIAの結果が、管理者が計画したセキュリティ対策にもかかわらず、取扱いにより著しいリスクが生ずることを示す場合には、取扱う前に関連する監督機関と協議する必要がある点に留意することも重要である。事前協議の詳細は、第36条に規定されている。

For the European Data Protection Board

欧州データ保護会議

The Chair

議長

(Andrea Jelinek)

(アンドレア・イエルニク)