Reply to public consultation – JEITA – Guidelines 3/2019 （日本語版）

September 9, 2019

Japan Electronics and Information Technology Industries Association (JEITA)

EDPB（欧州データ保護会議）のビデオ機器を通じた個人データ処理に関するガイドライン（パブコメ版）※の採択を受け、JEITA（電子情報技術産業協会）は本ガイドラインに対するコメントをぜひ共有させて頂きたい。※https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

JEITA は、素材から電子部品や半導体、また、民生電子製品から産業システム機器、さらには、IT 製品からソリューションサービス等を含む日本の代表的な電子情報産業の業界団体である。会員企業の多くは欧州市場にも展開しており、研究開発、生産、販売、サービス提供等の事業拠点を設置している。

JEITA は本ガイドライン全般については、ビデオカメラや顔認識技術を通じたデータ処理に関する GDPR の法解釈を明確化するものとして歓迎する。以下の幾つかのコメントを提出させて頂ければ幸甚である。

1. 明示的な同意を得ていないデータ主体からの生体テンプレート取得（5.1 節 82 項，84 項）

・ 82 項や 84 項（や 77 項）の事例では、生体テンプレート（顔特徴データ）の取得や顔認識の利用について明示的な同意を与えていないデータ主体から生体テンプレートを取得することは適法でないとされている。しかし、82 項や 84 項の事例において明示的な同意を得ていないデータ主体から生体テンプレートを取得することは、当該データが顔認識システムに登録されていないことを確認することが目的であり、個人を一意に識別することが目的ではない。なぜなら当該システムは、登録されていないデータ主体を識別するためのデータを何も保持していないからである。したがって、74 項の規定（生体データが GDPR 第 9 条の特別な種類の個人データとみなされるには自然人を一意に識別することを目的として処理されることが必要）に鑑みて、このようなデータ主体から取得する生体テンプレートは（個人データではあるものの）特別な種類の個人データには該当しないため、その処理の適法性は、GDPR 第 9 条 2 項ではなく、個人データ一般に関する GDPR 第 6 条 1 項によって保証されるべきである。

・ また、EU 指令 29 条作業部会「Opinion 02/2012 on facial recognition in online and mobile services」（WP192）の p5 では、

> *「生体データに伴う固有のリスクのため、顔認識のためにデジタル画像の処理を開始するに先立ち、当該個人からのインフォームドコンセントが必要とされるだろう。しかし、あるケースでは、データ管理者は当該処理の適法性の根拠として既にユーザが同意を与えているか否かを確認する目的で、顔認識処理のいくつかの段階を一時的に実行する必要があるかもしれない。このようなケースにおける顔認識の最初の処理（すなわち、画像取得、顔検出、顔照合など）は、（同意とは）異なる適法性の根拠、とりわけデータ管理者の正当な利益を根拠に持つかもしれない。このような処理の段階で処理されるデータは、利用者の同意を確認するという厳密に制限された目的でのみ利用されるべきであり、それが終わったら直ちに削除されるべきである。」*

として、顔認識（顔照合）に同意していない個人を確認するための処理について、正当な利益の根拠に基づく処理が許容されている。82 項や 84 項の事例においても、GDPR 第 6 条 1 項（f）すなわち正当な利益の根拠に基づいて、明示的な同意を得ていないデータ主体（ex. VIP 以外の顧客）からの生体テンプレートの取得を許容するべきである。（なお、それらの生体テンプレートは照合後、可能な限り短い時間内に削除される。）

2. 職場における従業員の合理的な期待、従業員の同意（3.1.3.2 節 36 項，3.3 節 46 項）

・ 36 項において、「工場 factory、倉庫 warehouse といった職場 workplace」を、安全管理目的でのビデオサーベイランスが許容される場所の例として追加するべきである。なぜなら、工場や倉庫といった身体的な危険を伴う場所では、安全管理目的でビデオ撮影がなされることについて従業員の合理的な期待があると考えられるからである。

・ また、昨今の AI 技術の進展により、従業員の安全管理以外の目的でも、例えば工場のラインにおける工員の動作分析により生産効率を向上させる取り組みや店舗における店員の動線分析により顧客満足度を向上させる取り組みなどが実用の段階にある。これらのケースにおける映像分析のための、同意に基づく個人データの取得と処理（生体テンプレートの取得は行わない）については、46 項における雇用主と従業員の間の権力の不均衡による同意の無効とは異なるケースとして、容認して欲しい。

3. 生体テンプレートの転送（5.2 節 86 項）

・ 「テンプレート（特徴データ）が転送できないことを保証する適切な措置が取られるべきである」という記載を、「テンプレート（特徴データ）が二次利用のために転送できないことを保証する適切な措置が取られるべきである」という記載に変更頂きたい。なぜなら、86 項の趣旨は、二次利用の回避のためにシステム間での転送を禁止するものであり、管理者が処理目的範囲内での利用を実現するために必要に応じてデータを転送することを制限するものではないためである。

4. 生体データの保護措置（5.2 節 88 項）

・ 生体データの保護措置として、「生体データにインテグリティコード（ハッシュや署名）を施すこと」などが挙げられているが、適切な保護措置は技術的進歩とともに変わりうるため、これらの措置は全てが shall なのではなく、あくまで例示または推奨措置であることを明確化してほしい。

5. 生体テンプレートの複製（5.2 節 89 項）

・ 管理者が生体テンプレートを保存する場合には「テンプレートの複製を無効にする」という記載があるが、「管理者によるテンプレートの複製を必要最小限にとどめ、無権限者による複製を無効にする」という表現に変更頂きたい。なぜなら、管理者が利用者に対する可用性維持のため、必要最小限の範囲でテンプレートをバックアップとして複製する必要があるためである。

6. 警告表示の例（7.1.2 節 114 項）

・ 第一階層の情報提供内容について、警告表示の具体例の記載は歓迎する。なぜなら、記載すべき項目が明確になることで管理者と個人の間での誤認識を減らすことができるためである。

以　上

Reply to public consultation – JEITA – Guidelines 3/2019

September 9, 2019

Japan Electronics and Information Technology Industries Association (JEITA)

Following the adoption of the public consultation version of Guidelines 3/2019 on processing of personal data through video devices, JEITA, the Japan Electronics and Information Technology Industries Association, is keen to share with you its comments on the Guidelines.

JEITA is the association of Japanese electronics and information technology industries, ranging from materials to electronic components and semiconductors, from consumer electronics to industrial system devices, from IT products to solution services. JEITA represents a large number of companies in these sectors, many of which are active on the European market, both through local manufacturing plants and research centers and through trade with the European Union.

Overall, JEITA warmly welcomes the Guidelines as it clarifies legal interpretation of GDPR on data processing through video camera and facial recognition technology. JEITA would be pleased to be given the opportunity to submit the following comments on the Guidelines.

1. Capturing of biometric templates from non-consenting data subjects (5.1 Paragraph 82 and 84)

- In the examples of paragraph 82 and 84 (and 77), these processing systems of biometric data are considered as unlawful if they capture visitors or passer-by who have not consented to creation of their biometric templates. However, in these examples, the purpose for capturing of biometric templates from non-consenting data subjects is to check that they are not enlisted in these biometric systems, rather than to "uniquely identify a natural person", because these systems do not have any personal data about them for identification. Therefore, given paragraph 74, such biometric templates from non-consenting data subjects are not considered as "special categories of personal data", so every legal ground under Article 6 (1) GDPR can provide a legal basis for processing such templates rather than Article 9 (2).
- Furthermore, in Article 29 Data Protection Working Party's "Opinion 02/2012 on facial recognition in online and mobile services (WP192)", they recognize that the initial processing such as image comparison for the purpose of assessing whether a user has provided consent or not may have a legal basis of the legitimate interest of the controller (*). Similarly, in the examples of paragraph 82 and 84, capturing of biometric templates from non-consenting data subjects should be able to have a legal basis of the legitimate interest under Article 6 (1) (f) GDPR. (In such cases, their templates should be deleted within the shortest possible period.)

> * *"Because of the particular risks involved with biometric data, this is will therefore require the informed consent of the individual prior to commencing the processing of digital images for facial recognition. However, in some cases, the data controller may temporarily need to perform some facial recognition processing steps precisely for the purpose of assessing whether a user has provided consent or not as a legal basis for the processing. This initial processing (i.e. image acquisition, face detection, comparison, etc) may in that case have a separate legal basis, notably the legitimate interest of the data controller to comply with data protection rules. Data processed during these stages should only be used for the strictly limited purpose to verify the user's consent and should therefore be deleted immediately after".* (WP192, p.5)

2. **Employees' reasonable expectations and consents** (3.1.3.2 paragraph 36, 3.3 paragraph 46)

- "The employees in their workplace such as factory or warehouse might also expect that they are monitored inside the factory or warehouse for security purpose" should be added after the last sentence of paragraph 36, because there might be employees' reasonable expectations to be monitored for security purpose in such places in physical danger.
- Besides security purpose, new initiatives using AI technologies such as employees' motion analyses for raising production efficiency in factory production lines or store staffs' moving line analyses for customer satisfaction improvement in shops are also in practical use. Any biometric template is not captured in the both cases. Such personal data processing for video image analyses based on employees' consents should be allowed in paragraph 46 rather than considered as invalid consent cases under the imbalance of power between employers and employees.

3. **Transfer of biometric templates** (5.2 Paragraph 86)

- The sentence "Measures should be put in place to guarantee that templates cannot be transferred across biometric systems" in paragraph 86 should be replaced by "Measures should be put in place to guarantee that templates cannot be transferred across biometric systems for further processing", because the intent of paragraph 86 is to prohibit transfer of templates for further processing rather than to prohibit transfer of template within originally specified purpose of processing.

4. **Measures to protect biometric data** (5.2 Paragraph 88)

- The phrase "the controller shall notably take the following measures" (such as associate an integrity code with the data) in paragraph 88 should be replaced by "the controller should notably take the following measures", because appropriate measures may change with advancement of technology.

5. **Copy of biometric templates** (5.2 Paragraph 89)

- The phrase "which would render the creation of the template ineffective" in paragraph 89 should be replaced by "which would render the creation of the template by unauthorized person ineffective and render the creation of the template by the controller minimum necessary", because the controller may need to copy the templates for back-up purpose to ensure the availability of the system.

6. **Example of warning sign** (7.1.2 Paragraph 114)

- We highly welcome the example of warning sign in paragraph 114, because it clarifies the way of displaying the content of the first layer information and it can reduce possible miscommunication between controller and data subjects.

We sincerely hope that you will find the above-mentioned comments useful. Thank you very much.