仮日本語訳

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

データ保護影響評価（DPIA）及び取扱いが2016/679規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン

本書面は、ARTICLE 29 DATA PROTECTION WORKING PARTY （第29条作業部会）により2017年４月４日に採択後、修正のうえ2017年10月４日に採択された
"**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**"
の英語版の一部を個人情報保護委員会が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。

Table of content 目次

I. Introduction

I. 序

Regulation 2016/679[1] (GDPR) will apply from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA[2]), as does Directive 2016/680[3].

[1] Regulation (EU) 2016/679 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 (General Data Protection Regulation).
個人データの取扱いに関する自然人の保護、当該データの自由な移動及び指令 95/46/EC の廃止に関する 2016 年 4 月 27 日の欧州議会・欧州理事会規則(EU) 2016/679（一般データ保護規則、GDPR）。

[2] The term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept.
「プライバシー影響評価」（PIA）という用語は、しばしば、別の文脈において同様の概念を指す場合に用いられる。

[3] Article 27 of the Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, also states that a privacy impact assessment is needed for "the processing is likely to result in a high risk to the rights and freedoms of natural persons".

規則 2016/679[1] (GDPR)は 2018 年 5 月 25 日から適用される。GDPR 第 35 条は、指令 2016/680[3] と同様、データ保護影響評価（DPIA[2]）の概念を取り入れている。

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data[4] by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)[5]. In other words, **a DPIA is a process for building and demonstrating compliance.**

DPIA は取扱いとは何かを説明し、その必要性及び比例性を評価し、リスクを評価し、対処策を決定することによって個人データ取扱いに伴う自然人の権利及び自由に対するリスクを適切に管理するために設計されたプロセスである[4]。DPIA は、管理者が GDPR の義務を遵守するだけでなく、規則に遵守することを証明するために適切な手段が講じられている

犯罪防止・捜査・検知・起訴又は刑罰執行を目的とする、所轄官庁による個人データ取扱いに関する自然人の保護、及び当該データの自由な移動について、2016 年 4 月 27 日の欧州議会・欧州理事会指令 2016/680 第 27 条では、プライバシー影響評価は「取扱いが自然人の権利及び自由に対して高いリスクをもたらすことが予想される」ことから必要である、とも述べている。

[4] The GDPR does not formally define the concept of a DPIA as such, but - its minimal content is specified by Article 35(7) as follows:
GDPR は DPIA の概念そのものは正式に定義していないが、その最低限の内容は第 35 条(7)に次のように規定されている。
- "*(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
- (a) 予期される取扱作業及び取扱いの目的の体系的な記述であって、必要に応じて、データ管理者が追求する正当な利益を含む。
- *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- (b) その目的に関連して、その取扱作業の必要性及び比例性の評価。
- *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
- (c)第 1 項に定めるデータ主体の権利及び自由に対するリスクの評価。及び、
- *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned";*
- (d)個人データを確実に保護し、データ主体とその他関係者の権利及び正当な利益を考慮して、本規則に準拠していることを証明するための保護措置、安全管理措置及び仕組みなどを含むリスク対処想定手段。

- **its meaning and role is clarified by recital 84 as follows:** "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk".*
- その意味と役割は前文第 84 項で次のように説明されている。「*取扱作業が自然人の権利及び自由に対し高いリスクをもたらすことが予想される場合、本規則への準拠を強化するために、管理者はデータ保護影響評価を実施し、特にそのリスクの発生源、性質、特殊性及び重大性を評価する責任を負うものとする*」。

[5] See also **recital 84:** "*The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation*". 前文第 84 項の以下も参照のこと。「*その個人データ取扱いが本規則に準拠していることを証明するために取る適切な手段を決定する際には、評価結果を考慮するものとする*」。

ことの証明の際にも役立つことから、アカウンタビリティを果たすための重要なツールである（第 24 条も参照のこと）[5]。つまり、**DPIA とはコンプライアンスを確立し、証明するためのプロセスなのである。**

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
GDPR の下では、DPIA の義務を遵守しない場合には、所轄監督機関から罰金を科されることがある。取扱いが DPIA の対象である場合のこの不実施（第 35 条(1)及び(3)から(4)）、誤った方法での DPIA の実施（第 35 条(2)及び(7)から(9)）、又は必要であるにもかかわらず所轄監督機関との協議が行われない場合（第 36 条(3)(e)）には、1 千万ユーロ以下の制裁金、又は、事業である場合、前会計年度の全世界年間売上高の 2%までの制裁金のうち、いずれか高い方が科されることがある。

Note: the term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept.
注：「プライバシー影響評価」（PIA）という用語は、しばしば、別の文脈において同様の概念を指す場合に用いられる。

II. Scope of the Guidelines
II. 本ガイドラインの適用範囲

These Guidelines take account of:
本ガイドラインは以下を考慮する。

- the Article 29 Data Protection Working Party (WP29) Statement 14/EN WP 218[6];
- 第 29 条作業部会（WP29）声明 14/EN WP 218[6]
- the WP29 Guidelines on Data Protection Officer 16/EN WP 243[7];
- データ保護責任者に関する WP29 ガイドライン 16/EN WP 243[7]

[6] WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks adopted on 30 May 2014.
2014 年 5 月 30 日に採択された、データ保護の法的枠組みにおけるリスクに応じたアプローチの役割に関する WP29 の声明 14/EN WP 218。
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] WP29 Guidelines on Data Protection Officer 16/EN WP 243 Adopted on 13 December 2016.
2016 年 12 月 13 日に採択された、データ保護責任者に関する WP29 ガイドライン 16/EN WP243。
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A-

- the WP29 Opinion on Purpose limitation 13/EN WP 203[8];
- 目的の限定に関する WP29 意見書 13/EN WP 203[8]
- international standards[9].
- 国際規格 [9]。

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. **A DPIA is only required when the processing is** "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1)). In order to ensure a consistent interpretation of the circumstances in which a DPIA is mandatory (Article 35(3)), the present guidelines firstly aim to clarify this notion and provide criteria for the lists to be adopted by Data Protection Authorities (DPAs) under Article 35(4).
GDPR に盛込まれているリスクに応じたアプローチに沿って、DPIA の実施はすべての取扱作業で義務づけられるわけではない。**DPIA が求められるのは、取扱い**が「*自然人の権利及び自由に対し高いリスクをもたらすことが予想される場合*」(第 35 条(1)) **のみである。**DPIA が義務づけられる状況（第 35 条(3)）について、一貫性のある解釈を担保するために、本ガイドラインは何よりもこの考え方を明確にすることを目標とし、データ保護機関（DPAs）が第 35 条(4)に基づいて採択したリストの基準を提示する。

According to Article 70(1)(e), the European Data Protection Board (EDPB) will be able to issue guidelines, recommendations and best practices in order to encourage a consistent application of the GDPR. The purpose of this document is to anticipate such future work of the EDPB and therefore to clarify the relevant provisions of the GDPR in order to help controllers to comply with the law and to provide legal certainty for controllers who are required to carry out a DPIA.
第 70 条(1)(e)によると、欧州データ保護会議（EDPB）は GDPR の一貫性した適用を促進するため、ガイドライン、勧告、ベスト・プラクティスを発行することができるようになる。本文書の目的は、管理者が法を遵守するのを助け、DPIA 実施を求められる管理者に法的確実性を提供する為に、EDPB のこのような将来的作業を予想し、それによって GDPR の関連規定を明確にすることである。

These Guidelines also seek to promote the development of:

---

[8] WP29 Opinion 03/2013 on purpose limitation 13/EN WP 203Adopted on 2 April 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409
2013 年 4 月 3 日に採択された、目的制限に関する WP29 見解 13/EN WP203。

[9] e.g. ISO 31000:2009, *Risk management — Principles and guidelines*, International Organization for Standardization (ISO); ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).
例えば、ISO 発行 ISO 31000:2009「リスクマネジメント－原則及びガイドライン」、ISO 発行 ISO/IEC 29134（予定）「情報技術 - セキュリティ技術 - プライバシー影響評価 – ガイドライン、ISO」など。

本ガイドラインは以下の作成を推進することも目指している。

- a common European Union list of processing operations for which a DPIA is mandatory (Article 35(4));
- DPIA が義務づけられる取扱作業の EU 共通リスト（第 35 条(4)）。
- a common EU list of processing operations for which a DPIA is not necessary (Article 35(5));
- DPIA が必要でない取扱作業の EU 共通リスト（第 35 条(5)）。
- common criteria on the methodology for carrying out a DPIA (Article 35(5));
- DPIA 実施方法の共通基準（第 35 条(5)）。
- common criteria for specifying when the supervisory authority shall be consulted (Article 36(1));
- 監督機関と協議しなければならない場合を規定する共通基準（第 36 条(1)）。
- recommendations, where possible, building on the experience gained in EU Member States.
- 勧告、可能な場合は EU 加盟国で得られた経験に基づくもの。

III. DPIA: the Regulation explained DPIA

III. DPIA：規則における DPIA の説明

The GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the "the risks of varying likelihood and severity for the rights and freedoms of natural persons" (article 24 (1)). The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks [10] presented by the processing of personal data.

GDPR は、管理者に対し、とりわけ自然人の権利及び自由に係る可変的可能性と重大性のリスクを考慮して、GDPR 遵守の確保及び証明するを可能にする適切な措置を実施することを要求している（第 24 条 1 項）。一定の場合に DPIA を実施すべき管理者の義務は、個人データの取扱いによって生じたリスク [10] を適切に管理すべき一般的な義務の背景に照らして理解されるべきである。

A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and

[10] It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to identified, analyzed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly. Controllers cannot escape their responsibility by covering risks under insurance policies.
自然人の権利及び自由のリスクを管理するため、当該リスクは識別され、分析され、推定され、評価され、取扱い（例：軽減）され、定期的に見直されることが強調されるべきである。管理者は、保険の指針に潜むリスクをカバーすることで責任を回避することは出来ない。

likelihood. “Risk management”, on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.

「リスク」とは、出来事とその結果を記述するシナリオであり、重大性と可能性の観点から推定される。一方、「リスク管理」とは、リスクに関して、組織を指揮及び管理するための調和された活動と定義することができる。

Article 35 refers to a likely high risk “to the rights and freedoms of individuals”. As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to “the rights and freedoms” of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

第 35 条は、「個人の権利及び自由」に対する予想されるハイリスクに言及している。データ保護の法的枠組みにおけるリスクに応じたアプローチの役割に関して、29 条作業部会声明で指摘しているように、データ主体の「権利及び自由」への言及は、主としてデータ保護及びプライバシーに係る権利に関連するものであるが、同時に、言論の自由、思想の自由、移動の自由、差別の禁止、自由の権利、良心及び宗教といった他の基本的な権利にも関連している。

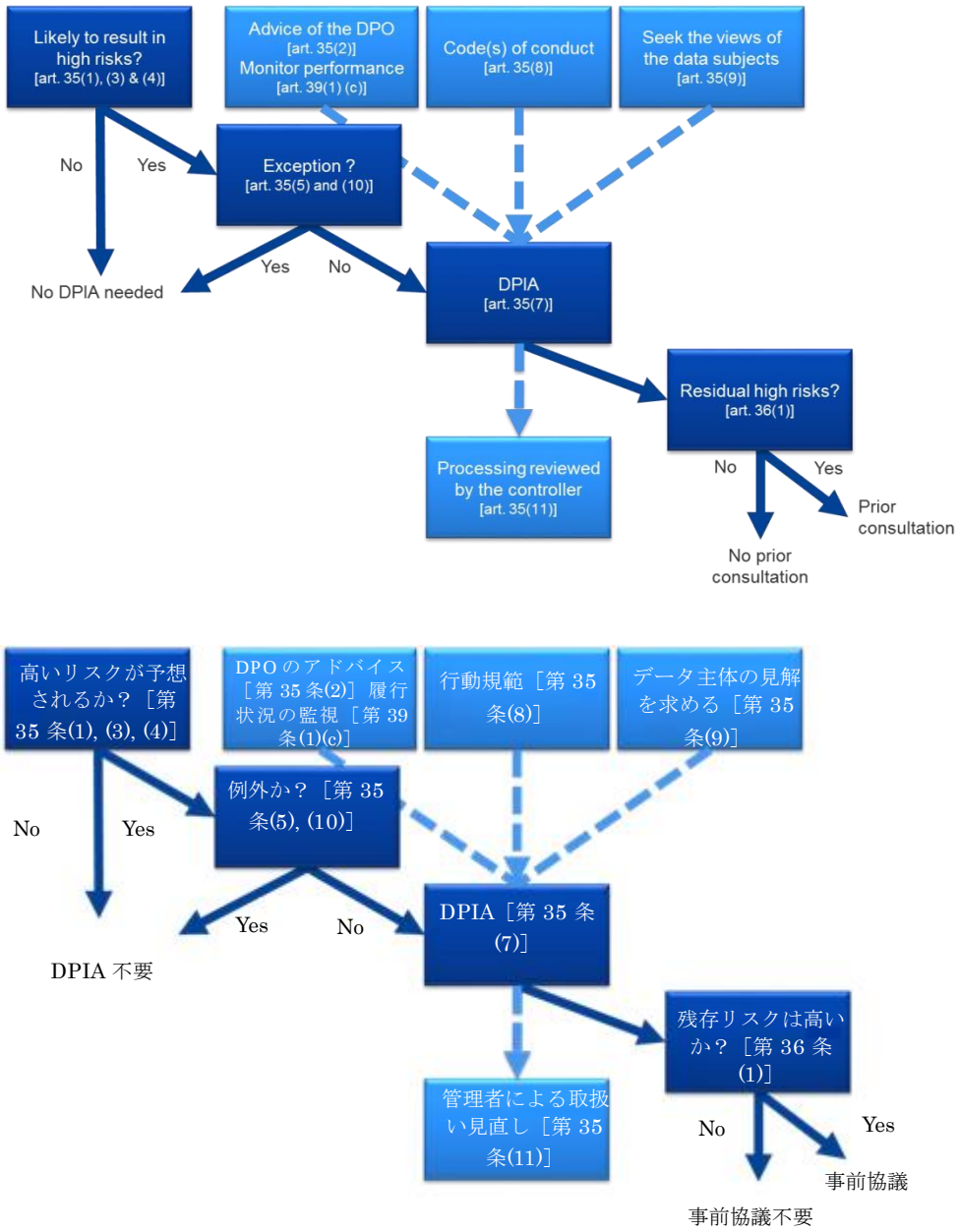
In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons” (Article 35(1)). The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers’ general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons”.

GDPR に盛込まれているリスクに応じたアプローチに沿って、DPIA の実施はすべての取扱作業において義務というわけではない。むしろ、DPIA は、ある種の取扱いが自然人の権利及び自由に対し高いリスクをもたらすことが予想される場合にのみ要求される（第 35 条 1 項）。しかしながら、DPIA を実施すべき義務の引き金となる条件を満たさないという単なる事実では、データ主体の権利及び自由に対するリスクを適切に管理するための措置を講

じるという管理者の一般的な義務を軽減することにはならない。実際に、これはある種の取扱いが「自然人の権利及び自由に高いリスクをもたらすことが予想される」場合を識別するため、管理者がその取扱活動によって発生するリスクを継続的に評価しなければならないことを意味する。

The following figure illustrates the basic principles related to the DPIA in the GDPR:

下記の図は GDPR における DPIA に関連した基本原則を図解したものである。



A. What does a DPIA address? A single processing operation or a set of similar processing operations.

A. DPIA は何を扱うのか？個別の取扱作業あるいは一連の類似した取扱作業。

A DPIA may concern a single data processing operation. However, Article 35(1) states that "*a single assessment may address a set of similar processing operations that present similar high risks*". Recital 92 adds that "*there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity*".

DPIA は個別の取扱作業に関するものである場合がある。しかし、第 35 条(1)は「*一つの評価は同種の高いリスクを示す一連の類似の取扱作業に対処することができる*」と述べている。また前文第 92 項は、「*データ保護影響評価の対象にとって、一つのプロジェクトよりも範囲を広げた方が合理的かつ経済的であるような場合がある。例えば、官庁又は公共機関が共通のアプリケーション又はプラットフォームを確立しようとする場合、複数のデータ管理者が、ある業界若しくは産業部門全体で、又は広く利用される横断的活動のために、共通のアプリケーション又は取扱環境を導入しようと企図する場合などである*」と付言している。

A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided.

単一の DPIA は、性質、範囲、文脈、目的及びリスクにおいて**類似する複数の取扱作業を評**

価するために、利用してもよいということである。実際、DPIA は自然人の権利及び自由につき、高いリスクをもたらすことが予想される新しい状況を体系的に研究することを目的としており、既に研究されたケース（すなわち、特定の文脈及び特定の目的において実施される取扱作業）においては DPIA を実施する必要はない。これは、同一目的のために類似技術を用いて同種のデータを収集する場合と考えられる。例えば、それぞれ同種の監視カメラ・システムを設置している地方自治体のグループは、この別々のデータ管理者による取扱いを対象とする単一の DPIA を実施することができるし、鉄道運行事業者（単一のデータ管理者）は一つの DPIA でそのすべての駅のビデオ監視を対象にすることができる。これは、また、様々なデータ管理者によって行われる類似の取扱作業にも適用されよう。そのようなケースでは、参考になる DPIA は共有され、公にアクセスできるようにされるべきであり、DPIA に記載されている措置が実施されなければならず、単一の DPIA を実施した正当性を与えなければならない。

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

取扱作業に共同管理者が関与する場合、共同管理者はそれぞれの義務を明確に規定する必要がある。共同管理者の DPIA は、リスクに対処し、データ主体の権利及び自由を保護するための各種の措置について、どの関係者が責任を負うのかを定めるべきである。各データ管理者は秘密を損なうことなく（例：企業秘密、知的財産、機密のビジネス情報の保護）又は脆弱性を開示することなく、自己の必要性を表明し、有効な情報を共有すべきである。

A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate. An example could be the relationship between manufacturers of smart meters and utility companies. Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities.

DPIA は技術製品についてデータ保護影響度を評価することにも有用となりうる。例えば、異なるデータ管理者があるハードウェア又はソフトウェアを用いて、異なる取扱作業を行う場合などが考えられる。もちろん、その製品を使用するデータ管理者に、特定の取扱いの実施について独自に DPIA を行う義務があることに変わりはないが、適切な場合は、その製品の提供者の作成した DPIA から情報が得られる可能性がある。スマートメーターのメーカーと公益事業会社との関係がこの例と言えよう。各製品提供者又は処理者は、秘密を損なうことなく、また、脆弱性の開示によるセキュリティ・リスクを導くことなく、有効な情報を共有すべきである。

B. Which processing operations are subject to a DPIA? Apart from exceptions, where they are "likely to result in a high risk".

B. どの取扱作業が DPIA の対象になるのか？例外は別にして、「高いリスクがもたらされることが予想される」場合

This section describes when a DPIA is mandatory, and when it is not necessary to carry out a DPIA.

本セクションでは、どのような場合に DPIA が義務づけられるか、そして、どのような場合に DPIA を実施する必要がないかについて説明する。

Unless the processing operation meets an exception (III.B.a), a DPIA has to be carried out where a processing operation is "*likely to result in a high risk*" (III.B.b).

取扱作業が例外（Ⅲ.B.a）に該当しない限り、取扱作業が「高いリスクをもたらすことが予想される」場合、DPIA は実施されなければならない(III.B.b)。

a) When is a DPIA mandatory? When processing is "*likely to result in a high risk*".

a) DPIA が義務化されるのはどのような場合か？取扱いが「*高いリスクをもたらすことが予想される*」場合

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4)). It is particularly relevant when a new data processing technology is being introduced[11].

[11] See recitals 89, 91 and Article 35(1) and (3) for further examples.
他の例については前文第 89 項、第 91 項、及び第 35 条(1)及び(3)を参照のこと。

GDPR は自然人の権利及び自由にリスクをもたらすおそれのあるあらゆる取扱作業に DPIA の実施を求めてはいない。DPIA の実施が義務づけられるのは、取扱いが「*自然人の権利及び自由に高いリスクをもたらすことが予想される*」場合のみである（第 35 条(1)、第 35 条(3)図、第 35 条(4)による補足）。これは特に、新規のデータ取扱技術が導入される場合に該当する[11]。

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.

DPIA が必要かどうか明確でない場合に、WP29 がそれでもなお、DPIA の実施を勧告しているのは、DPIA が管理者によるデータ保護法の遵守を助ける有益なツールだからである。

Even though a DPIA could be required in other circumstances, Article 35(3) provides some examples when a processing operation is "*likely to result in high risks*":
DPIA が他の状況で要求される場合もあるが、第 35 条(3)は取扱作業が「*高いリスクをもたらすことが予想される*」例をいくつか挙げている。

- "*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*[12]*;*
- *(a) プロファイリングを含む自動化された取扱いに基づき、かつそれが自然人に法的影響又は同様の重大な影響を与えるような判断に基づいて、自然人の個人的な側面を体系的かつ広範に評価する場合*[12]*。*
- *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10*[13]*; or*

[12] See recital 71: "*in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles*".
[12] 前文第 71 項を参照。「*個人のプロファイルを作成又は利用するために、特に業務実績、経済的状況、健康状態、個人的嗜好又は関心、信頼性又は行動、所在地又は移動に関する面を分析又は予想すること*」。
[13] See recital 75: "*where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures*".
前文第 75 項を参照。「*個人の人種若しくは民族的素性、政治的思想、宗教的又は哲学的信条、労働組合員資格、遺伝データ、健康に関するデータ、自然人の性生活若しくは性的指向に関するデータ、刑法上の有罪判決及び犯罪又は関連する安全管理措置を明らかにするような個人データを取扱う場合*」。

- *(b) 第 9 条(1)に示す特別な種類のデータ、又は第 10 条[13]に示す刑法上の有罪判決及び犯罪に関わる個人データを大規模に取扱う場合、又は*
- *(c) a systematic monitoring of a publicly accessible area on a large scale*".
- *(c) 公衆のアクセス可能な地域で大規模に体系的な監視を行う場合。*

As the words "*in particular*" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to DPIAs. For this reason, the criteria developed below sometimes go beyond a simple explanation of what should be understood by the three examples given in Article 35(3) GDPR.

GDPR 第 35 条(3)の導入文の「特に」という語が示す通り、これは非網羅的なリストと考えるべきものである。このリストに掲載されていないが、同様に高いリスクをもたらす「高いリスクの」取扱作業もありうる。このような取扱作業も DPIA の対象となるべきである。この理由で、下記に記載する基準は、GDPR 第 35 条(3)の 3 つの例から解釈すべき内容についての単純な説明より踏み込んだものとなる場合もある。

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91, and other GDPR references to "*likely to result in a high risk*" processing operations[14], the following nine criteria should be considered:
それらが内在している高いリスクのために DPIA が必要な取扱作業について、より具体的な例を挙げるために、第 35 条(1)及び(3)(a)から(c)の特有の要素、第 35 条(4)及び前文第 71 項、第 75 項、第 91 項に基づいて国内レベルで採択されるべきリスト、そしてその他の「*高いリスクをもたらすことが予想される*」取扱作業との GDPR の言及[14]を考慮して、以下の 9 つの基準を検討するべきである。

1. Evaluation or scoring, including profiling and predicting, especially from *"aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements"* (recitals 71 and 91).

[14] See e.g. recitals 75, 76, 92, 116.
例えば前文第 75 項、第 76 項, 第 92 項、第 116 項も参照のこと。

Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.

1. 評価又は採点。プロファイリング及び予想を含む。特に、「*データ主体の業務実績、経済的状況、健康状態、個人的嗜好又は関心、信頼性又は行動、所在地又は移動に関する側面*」に関するもの（前文第 71 項及び第 91 項）。この例としては、金融機関が顧客を信用照会データベース、又はマネーロンダリング対策及びテロ資金調達対策（AML/CTF）又は虚偽データベースでスクリーニングする場合、又は疾病・健康上のリスクを評価・予想するためにバイオテクノロジー企業が直接消費者に遺伝子検査を売り込む場合、あるいは企業がサイト上での利用・誘導に基づいて行動、又はマーケティングのプロファイルを作成する場合などがある。

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling.
2. 法的又は同種の重大な影響のある自動化された意志決定：「*自然人に法的な影響*」をもたらす又は「*自然人に同等の重大な影響*」（第 35 条(3)(a)）をもたらすデータ主体について意志決定することを目的とする取扱い。例えば、取扱いが個人の排除又は差別につながるような場合が挙げられる。個人への影響が皆無又はわずかな取扱いはこの基準に当てはまらない。この説明についての更なる解説は、今後の WP29 のプロファイリング・ガイドラインに提供される予定である。

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))[15]. This type of monitoring is a criterion because the

[15] The WP29 interprets "*systematic*" as meaning one or more of the following (see the WP29 Guidelines on Data Protection Officer 16/EN WP 243):
WP29 は「*体系的*」とは下記の 1 つ又は複数を指すと解釈している（データ保護責任者に関する WP29 ガイドライン 16/EN WP 243 を参照）。
- occurring according to a system;
- pre-arranged, organised or methodical;

personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

3. 体系的な監視：データ主体を観察、監視又は管理するための取扱い、ネットワーク又は「*公衆がアクセス可能な地域での大規模で体系的な監視*」（第 35 条(3)(c)）を行ってデータ収集することを含む[15]。この種の監視は、データ主体が、本人のデータを収集しているのが誰か、また、どのようにデータが使用されるのか気づかないまま個人データが収集される場合がありうるため、基準の 1 つとなる。また、公共の（又は公衆がアクセス可能な）場所でそのような取扱いの対象となるのを避けることは、個人には不可能な場合があるからでもある。

4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion

---

- taking place as part of a general plan for data collection;
- carried out as part of a strategy.
- システムによって発生する。
- 前もって準備され、手配され、又は手順に則っている。
- データ収集の一般的プランの一環として行われる。
- 戦略の一環として行われる。

The WP29 interprets "*publicly accessible area*" as being any place open to any member of the public, for example a piazza, a shopping centre, a street, a market place, a train station or a public library.
WP29 は「*公衆がアクセス可能な場所*」とは、一般社会の誰に対しても開かれた場所と解釈している。例えば広場、ショッピングセンター、通り、市場、鉄道駅、公共図書館などである。

may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.

4. センシティブ・データ又は高度に個人的な性質を有するデータ：これには第 9 条で定める特別な種類のデータ（個人の政治的見解に関する情報など）、及び第 10 条に定義する有罪判決又は犯罪に関する個人データがある。例としては、患者の医療記録を保存する一般の病院、犯罪者の詳細記録を保存する私立探偵などが挙げられる。GDPR のこれらの規定を超えて、いくつかの種類のデータは、個人の権利及び自由に対する潜在リスクを増加させると考えられる。これらの個人データは、家庭内及び個人的活動（その秘密性が保護されるべき電子通信など）にリンクしていること、又は基本的権利（その収集が移動の自由に疑問を呈する位置情報など）の行使に影響を与えること、又はその違反は明らかにデータ主体の日々の生活（支払詐欺に使用されるかもしれない財務データなど）に重大な影響を与えることから、センシティブ（この用語が一般に理解されているように）とされる。この点で、そのデータが本人又は第三者によって既に公開されているかが問題となるだろう。個人データが公開されているという事実は、そのデータが何らかの目的でさらに利用されることが見込まれるかという評価において、1 つの要素と見なされうる。またこの基準には、個人文書、電子メール、日記、ノート機能のある電子書籍リーダーの記録及びライフ・ログ・アプリに含まれている極めて個人的な情報などが含まれるであろう。

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale[16]:

5. 大規模なデータ取扱い：GDPR は何を持って大規模とするか定めていないが、前文第 91 項にいくつかガイダンスがある。いずれにせよ、WP29 は、取扱いが大規模に実施されているかを判断する際、特に以下の要素を考慮することを勧告している[16]。

   a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
   b. the volume of data and/or the range of different data items being processed;
   c. the duration, or permanence, of the data processing activity;
   d. the geographical extent of the processing activity.

[16] See the WP29 Guidelines on Data Protection Officer 16/EN WP 243.
データ保護責任者に関する WP29 ガイドライン 16/EN WP 243 を参照。

a. 関係するデータ主体数。特定の人数、又は該当する人口に対する割合として示される。
b. データ量、及び／又は取扱われる様々なデータの範囲。
c. データ取扱活動の期間又は存続時間。
d. 取扱活動の地理的範囲。

6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject[17].
6. データセットの照合又は合成、例えば様々な目的で、及び／又は様々なデータ管理者がデータ主体の合理的な予想を超えるような方法で行った、2 つ以上の取扱作業から作成されたデータ[17]。

7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
7. 立場の弱いデータ主体に関するデータ（前文第 75 項）: この種のデータの取扱いは、データ主体とデータ管理者の力関係のアンバランスが増すため、一つの基準となる。つまり、個人が自分のデータ取扱いに容易に同意、拒否又は権利の行使をできない可能性があるということである。立場の弱いデータ主体には、子供（彼らは、自分のデータ取扱いに、意味を理解した上でよく考えて、拒否又は同意することはできないと考えられる）、従業員、特別な保護が必要な弱者（精神障害者、亡命希望者、高齢者、患者など）、及びデータ主体とデータ管理者の立場の関係がアンバランスな場合が含まれうる。

[17] See explanation in the WP29 Opinion on Purpose limitation 13/EN WP 203, p.24.
目的制限に関する WP29 見解 13/EN WP203, P. 24 における説明を参照。

8. Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology defined in "accordance with the achieved state of technological knowledge" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.

8. 新たなテクノロジー又は組織的なソリューションの革新的利用又は適用。物理的なアクセス管理を強化するために、指紋と顔認識とを組み合わせて利用するなど。GDPR は、「達成された技術的知識」（前文第 91 項）に従って定義された新たなテクノロジーの利用によって、DPIA 実施の必要性が生じる場合があると明記している（第 35 条(1)及び前文第 89 項と第 91 項）。これは、このようなテクノロジーの利用が新しい形のデータ収集と利用を伴い、個人の権利及び自由に高いリスクをもたらしえるためである。事実、新たなテクノロジーの利用が個人と社会にどのように影響するか、解らない場合がある。DPIA はデータ管理者がこのようなリスクを理解し、対処する上で役立てることのできるものである。例えば、ある種の「モノのインターネット（IOT）」アプリケーションは個人の日常生活やプライバシーに重大な影響を与えることが考えられる。だからこそ DPIA が必要なのである。

9. When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract"* (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

9. 取扱いそのものが「*データ主体の権利の行使又はサービスや契約の利用を妨げる*」場合（第 22 条及び前文第 91 項）。これには、データ主体のサービス利用又は契約締結を許可・改変・拒否する目的で行われる取扱作業が含まれる。この例としては、銀行が顧客に貸し出しを行うか否かを決定するために、信用照会データベースでスクリーニングする場合が挙げられる。

In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.
多くの場合、データ管理者は、2 つの基準に該当する取扱いには、DPIA の実施が必要と考えることができる。一般に、WP29 は取扱いがより多くの基準に該当するほど、データ主体の権利及び自由に対して高いリスクをもたらす可能性が高いと考えるので、DPIA を管理者が導入を考えている措置にかかわらず、要求する。

However, in some cases, **a data controller can consider that a processing meeting only one of these criteria requires a DPIA**.

しかし、場合によっては、**データ管理者は、1 つの基準しか該当しない取扱いも DPIA が求められると考えることができる。**

The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:

以下の事例は、特定の取扱作業に DPIA が必要か否かを評価するに当たり、基準がどのように使用されるべきかを説明するものである。

Examples of processing **取扱いの例**	**Possible Relevant criteria** **該当する可能性のある基準**	**DPIA likely to be required?** **DPIA の必要性が高いか？**
A hospital processing its patients' genetic and health data (hospital information system). 病院が患者の遺伝子及び健康データを取扱う場合（病院の情報システム）	-Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects - Data processed on a large-scale. - センシティブ・データ又は高度に個人的性質を有するデータ - 立場の弱いデータ主体に関するデータ	Yes 必要

	- 大規模に取扱われたデータ	
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates. 高速道路で運転行動を監視するためカメラ・システムを利用する場合。管理者は車を絞り込み、ナンバープレートを自動認識するためにインテリジェント・ビデオ分析システムの利用を予定している。	-Systematic monitoring - Innovative use or applying technological or organisational solutions - 体系的な監視 - テクノロジー又は組織的なソリューションの革新的利用又は適用	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc. 企業が雇用者の活動を体系的に監視する場合。雇用者の仕事場、インターネットの利用などの監視を含む。	- Systematic monitoring - Data concerning vulnerable data subjects - 体系的な監視 - 立場の弱いデータ主体に関するデータ	
The gathering of public social media data for generating profiles. プロフィールを生み出す一般のソーシャルメディアデータの収集。	- Evaluation or scoring. - Data processed on a large scale. -Matching or combining of datasets. -<u>Sensitive data or data of a highly personal nature:</u> - 評価又は採点 - 大規模なデータ取扱い - データセットの照合又は合成 - <u>センシティブ・データ又は高度に個人的な性質を有するデータ</u>	
An institution creating a national level credit rating or fraud database.	-Evaluation or scorning. -Automated decision making with	

国レベルの信用格付又は虚偽データベース認定を行う機関。	legal or similar significant effect. -Prevents data subject from exercising a right or using a service or a contract. - Sensitive data or data of a highly personal nature: -評価又は採点 -法的又は同様の重要な効果を有する自動化された意思決定 -データ主体の権利行使の阻止あるいはサービスの利用又は契約利用の阻止 -センシティブ・データ又は高度に個人的な性質を有するデータ	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials 研究プロジェクト又は臨床試験における地位の弱いデータ主体に関する仮名化された個人のセンシティブ・データの保管目的の保存。	-Sensitive data. -Data concerning vulnerable data subjects. -Prevents data subjects from exercising a right or using a service or a contract -センシティブ・データ -社会的地位の弱いデータ主体 -データ主体の権利行使の阻止あるいはサービスの利用又は契約利用の阻止	
A processing of "personal data from patients or clients by an individual physician, other health care professional or lawyer" (Recital 91). 「個々の医師、他の健康管理専門家又は弁護士が患者及び顧客から得る個人データ」の取扱い（前文第 91 項）	-Sensitive data or data of a highly personal nature. -Data concerning vulnerable data subjects. -センシティブ・データ又は高度に個人的性質を有するデータ -社会的地位の弱いデータ主体に関するデータ	No 不要

An online magazine using a mailing list to send a generic daily digest to its subscribers. オンライン・マガジンがメーリングリストを使って毎日一般的なダイジェスト情報を加入者に送信する場合。	- Data processed on a large scale. - 大規模に取扱われたデータ	
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website. 電子商取引サイトが限定的なプロファイリングを伴うヴィンテージ・カーのパーツの広告を、自身のサイトで閲覧又は購入されたアイテムに基づいて表示する場合。	- Evaluation or scoring. - 評価又は採点	

Conversely, a processing operation may correspond to the above mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.

逆に、ある取扱作業が上記のケースに該当するも、管理者としては、依然として「高いリスクをもたらすことが予測され」ないと考える場合がある。そのようなケースでは、管理者は、DPIA を実施しない理由の正当化及び文書化を行うべきであり、データ保護責任者の見解を収録／記録すべきである。

In addition, as part of the accountability principle, every data controller "*shall maintain a record of processing activities under its responsibility*" including inter alia the purposes of processing, a description of the categories of data and recipients of the data and "*where possible, a general description of the technical and organisational security measures referred to in Article 32(1)*" (Article 30(1)) and must assess whether a high risk is likely, even if they ultimately decide not to carry out a DPIA.

さらに、アカウンタビリティの原則の一部として、すべてのデータ管理者は、「*その責任に*

おいて取扱作業の記録を保存しなければならない」。特にその取扱いの目的、データの種類の詳細、データの取得者、そして「*可能な場合には、第32条(1)に述べた技術的及び組織的な安全管理措置の一般的な説明*」（第30条(1)）を保存し、最終的にDPIAを実施しない決定をしようとも、高いリスクが予想されるかどうかの評価を行わなければならない。

Note: supervisory authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA to the European Data Protection Board (EDPB) (Article 35(4))[18]. The criteria set out above can help supervisory authorities to constitute such a list, with more specific content added in time if appropriate. For example, the processing of any type of biometric data or that of children could also be considered as relevant for the development of a list pursuant to article 35(4).

注：監督機関は DPIA に必要な取扱作業のリストを作成し、公開し、欧州データ保護会議（EDPB）に伝達することが求められる（第35条(4)[18]。上記の基準は、監督機関がそのようなリストを作成し、適宜具体的な内容を付加する役に立つだろう。例えば、いかなる種類でも生体データの取扱い又は子どものデータの取扱いは、第35条(4)に基づくリストの作成に該当すると考えられる。

b) When isn't a DPIA required? When the processing is not "*likely to result in a high risk*", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required.

b)DPIAが必要ないのはどのような場合か？取扱いが「*高いリスクをもたらすことが予想されない*」場合、又は類似のDPIAが存在する場合、又は2018年5月より前においてそれが正当と認められてきた場合、又は法的根拠がある場合、又はDPIAが必要とされない取扱作業のリストにある場合。

WP29 considers that a DPIA is not required in the following cases:
WP29は、DPIAは次の場合には必要ないと考える。

[18] In that context, "*the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union*" (Article 35(6)).
この意味で、「*そのリストがデータ主体への物品又はサービスの提供に関わる取扱作業、又は一部加盟国でのデータ主体の行為の監視に関わる取扱作業を伴う場合、あるいはEU域内での自由な個人データの移転に重大な影響を与えるような場合、所轄監督機関は第63条に記載された一貫性メカニズムを適用しなければならない*」（第35条(6)）。

- **where the processing is not "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1));**
- **その取扱いが「*自然人の権利及び自由に対し高いリスクをもたらすことが予想され*」ない場合（第 35 条(1)）**
- **when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out.** In such cases, results of DPIA for similar processing can be used (Article 35(1)[19]);
- **その取扱いの性質、範囲、文脈、及び目的が、既に DPIA が実施された取扱いと極めて似ている場合。**このような場合には、同種の取扱いの DPIA 結果を用いることができる（第 35 条(1)[19]）。
- when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed[20] (see III.C);
- 取扱作業のチェックが、監督機関により、2018 年 5 月前に変更されていない特定の状況下で行われている場合[20]（III.C 参照）。
- **where a processing operation, pursuant to point (c) or (e) of article 6(1), has a legal basis** in EU or Member State law, where the law regulates the specific processing operation **and where a DPIA** has already been carried out as part of the establishment of that legal basis (Article 35(10)) [21], except if a Member state has stated it to be necessary to carry out a DPIA prior processing activities;
- **ある取扱作業に第 6 条（1）のポイント(c)又は(e)に従って、**EU 又は加盟国において**法的根拠がある場合、**法律が特定の取扱作業を規制し、**かつ、DPIA** が当該法的根拠

---

[19] ***"A single assessment may address a set of similar processing operations that present similar high risks".***
「*単一の評価は同等の高いリスクを提示する一連の類似の取扱作業を扱うことができる*」。

[20] "Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed" (recital 171).
採択された委員会決定及び指針 95/46/EC に基づく監督機関による承認は、改正、差替又は廃止されるまで有効である（前文第 171 項）。

[21] When a DPIA is carried out at the stage of the elaboration of the legislation providing a legal basis for a processing, it is likely to require a review before entry into operations, as the adopted legislation may differ from the proposal in ways that affect privacy and data protection issues. Moreover, there may not be sufficient technical details available regarding the actual processing at the time of adoption of the legislation, even if it was accompanied by a DPIA. In such cases, it may still be necessary to carry out a specific DPIA prior to carrying out the actual processing activities.
DPIA が取扱いの法的根拠を規定する法律の推敲の段階で実施される場合、採択された法律は法案とはプライバシー及びデータ保護問題に影響を与える部分で異なりえることから、執行される前に見直される可能性が高い。更に、当該法律の採択時には、それが DPIA を伴っていたしても、実際の取扱いに関して、入手可能な十分な技術的詳細はないであろう。そのような場合には、実際の取扱活動を実施する前に特定の DPIA を実施する必要があろう。

確立の一環として既に実施されている場合（第 35 条(10)）。ただし、加盟国が取扱活動に先立ち DPIA が必要と述べている場合を除く [21]。

- **where the processing is included on the optional list (established by the supervisory authority) of processing operations** for which no DPIA is required (Article 35(5)). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorizations, compliance rules, etc. (e.g. in France, authorizations, exemptions, simplified rules, compliance packs…). In such cases, and subject to re-assessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with the relevant requirements of the GDPR.
- **ある取扱いが、DPIA を必要としない取扱作業の選択リスト（監督機関が作成）に含まれている場合**（第 35 条(5) ）。このリストには、当該機関が定める条件を満たすデータ取扱作業を掲載してもよい。特に、ガイドライン、特定の決定又は承認、コンプライアンス規則などによって定めてよい（例えばフランスでは、承認、例外、簡略化規則、コンプライアンス用パッケージなど）。このような場合、及び所轄監督機関の再評価を受ける場合、DPIA は必要ではない。ただし、その取扱いが厳密にそのリストで言及されている手続の範囲に該当し、GDPR の要件を完全に満たし続けることを条件とする。

C. What about already existing processing operations? DPIAs are required in some circumstances.

C. 既に行われている取扱作業についてはどうか？DPIA は状況によっては求められる。

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

DPIA 実施の要件は、自然人の権利及び自由に高いリスクがもたらされることが予想される現行の取扱作業であって、当該取扱いの性質、範囲、文脈及び目的を考慮した上でそのリスクが変化している取扱作業に適用される。

A DPIA is not needed for processing operations that have been checked by a supervisory authority or

the data protection official, in accordance with Article 20 of Directive 95/46/EC, and that are performed in a way that has not changed since the prior checking. Indeed, "Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed" (recital 171).

DPIA は、監督機関又はデータ保護オフィサーによって指針 95/46/EC 第 20 条に従いチェックを受けた取扱作業及び前回のチェック以降変更ない方法で実行されている取扱作業には必要とされない。採択された委員会決定及び指針 95/46/EC 第 20 条に基づく監督機関による承認は、改正、差替又は廃止されるまで有効である（前文第 171 項）。

Conversely, this means that any data processing whose conditions of implementation (scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the supervisory authority or the data protection official and which are likely to result in a high risk should be subject to a DPIA.

逆に、このことは、その実施の条件（範囲、目的、収集された個人データ、データ管理者又は取得者の身元、データ保持期間、技術的かつ組織的措置等）が監督機関又はデータ保護オフィサーによる前回のチェック以降に変わった場合及び高いリスクがもたらされることが予想される場合には、DPIA の対象となるべきことを意味する。

Moreover, a DPIA could be required after a change of the risks resulting from the processing operations[22], for example because a new technology has come into use or because personal data is being used for a different purpose. Data processing operations can evolve quickly and new vulnerabilities can arise. Therefore, it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination. Each of these examples could be an element that leads to a change of the risk resulting

[22] In terms of the context, the data collected, purposes, functionalities, personal data processed, recipients, data combinations, risks (supporting assets, risk sources, potential impacts, threats, etc.), security measures and international transfers.
文脈、収集されたデータ、目的、機能、取扱われた個人データ、取得者、データの組み合わせ、リスク（支援資産、リスク源、潜在的影響、脅威等）、安全管理措置及び国際的移転の観点から。

from processing activity concerned.

さらに、DPIA は取扱作業に起因するリスクの変動後に要求される場合があろう[22]。例えば、新しいテクノロジーが利用されるようになったこと、又は個人データが別の目的に使われるようになったことなどに伴う変動である。データ取扱作業は急激に進化し、新しい脆弱性が現れうる。したがって、DPIA の改訂は継続的な改善に有効であるのみならず、経時的に変化する環境下におけるデータ保護のレベルを維持するに不可欠であることに留意すべきである。DPIA は、また、取扱活動に係る組織的又は社会的文脈に変化が生じた場合、例えば、ある自動化された決定の影響がより重要となった場合、又は新しい分類のデータ主体が差別に対し、脆弱となった場合に必要となろう。これらの例の夫々は、関連する取扱活動に起因するリスクの変動につながる要素となりうる。

Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

逆に、ある変化はまたリスクを軽減する可能性がある。例えば、取扱作業は、決定がもはや自動的でなくなる又は監視活動がもはや体系的でなくなるまで進化する可能性がある。その場合には、実施したリスク分析の見直しは、DPIA の実施は、もはや必要ないことを示すことができる。

As a matter of good practice, **a DPIA should be continuously reviewed and regularly re-assessed** Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.

望ましい慣行の問題として、**DPIA は継続的に見直され、かつ、定期的に再評価されるべきである。**したがって、DPIA が 2018 年 5 月 25 日の時点において必要とされない場合においても、管理者はそのような DPIA を一般的なアカウンタビリティの原則の一環として実施することは、適切な時期に必要であろう。

D. How to carry out a DPIA?

D. DPIA の実施はどのように行うのか？

a) At what moment should a DPIA be carried out? Prior to the processing.

a) DPIA はどの段階で実施しなければならないか？取扱前である。

The DPIA should be carried out "*prior to the processing*" (Articles 35(1) and 35(10), recitals 90 and 93)[23]. This is consistent with data protection by design and by default principles (Article 25 and recital 78). The DPIA should be seen as a tool for helping decision-making concerning the processing.

DPIA は「取扱前」に実施しなければならない（第 35 条(1)及び(10)、前文 90 項及び第 93 項）[23]。これはデータ保護バイ・デザイン及びデータ保護バイ・デフォルトの原則によるデータ保護に合致する（第 25 条及び前文第 78 項）。DPIA は取扱いに関する意思決定を支援するツールとして捉えられるべきである。

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA is updated throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

DPIA は、取扱作業の一部が不明であったとしても、取扱作業の設計時に実行可能な限り、速やかに開始すべきである。プロジェクトのライフサイクルを通じて更新される DPIA の更新は、データ保護とプライバシーへの考慮を確保し、コンプライアンスを推進するソリューションの作成を奨励することになろう。また、開発プロセスの進捗に合わせ、個々の評価段階を繰り返す必要が出てくる場合もあるだろう。なぜなら、ある技術又は組織的手段の選択が、その取扱いによって提示されるリスクの重大性又は可能性に影響しうるからである。

The fact that the DPIA may need to be updated once the processing has actually started is not a valid

[23] Except when it is an already existing processing that has been prior checked by the Supervisory Authority, in which case the DPIA should be carried out before undergoing significant changes.
監督機関による事前のチェックが行われている既存の取扱いである場合を除き、重大な変更を行う前に DPIA を実施する必要がある。

reason for postponing or not carrying out a DPIA. The DPIA is an on-going process, especially where a processing operation is dynamic and subject to ongoing change. **Carrying out a DPIA is a continual process, not a one-time exercise.**

取扱いが実際に始まれば、DPIA を更新する必要があるかも知れないという事実は、DPIA の延期や実施しないことについての有効な理由にはならない。DPIA は、とりわけ、取扱作業が変動的で、進行中の変化に影響を受ける場合において、進行中のプロセスである。**DPIA の実施は一度きりではなく、継続的なプロセスである。**

b) Who is obliged to carry out the DPIA? The controller, with the DPO and processors.

b) DPIA の実施義務者は誰か？DPO と処理者と一体となって、管理者が実施義務を負う。

The controller is responsible for ensuring that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.

管理者は、DPIA が確実に実施されるよう責任を負う（第 35 条(2)）。DPIA は組織内外の別の者によって実施されてもよいが、この任務の最終的なアカウンタビリティの責任を負うのがデータ管理者であることは変わらない。

The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2)) and this advice, and the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c)). Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243.

管理者は、指定された場合（第 35 条(2)）**、データ保護責任者（DPO）のアドバイスも求めなければならない。**また、このアドバイスと管理者により下された決定は DPIA の中で文書化されるべきである。DPO はまた DPIA の履行を監視すべきである（第 39 条(1)(c)）。さらなるガイダンスがデータ保護責任者に関する WP29 ガイドライン 16/EN WP 243 に定められている。

If the processing is wholly or partly performed by a data processor, **the processor should assist the controller in carrying out the DPIA** and provide any necessary information (in line with Article 28(3)(f)).

取扱いの全体又は一部がデータ処理者によって行われる場合、**処理者は DPIA 実施につい**

て管理者を支援し、いかなる必要な情報も（第 28 条(3)(f)に従って）提供すべきである。

The controller must "*seek the views of data subjects or their representatives*" (Article 35(9)), "*where appropriate*". The WP29 considers that:

データ管理者は「適切な場合、データ主体又はその代理人の見解を求め」なければならない（第 35 条(9)）。WP29 は次のように考えている。

- those views could be sought through a variety of means, depending on the context (e.g. a generic study related to the purpose and means of the processing operation, a question to the staff representatives or usual surveys sent to the data controller's future customers) ensuring that the controller has a lawful basis for processing any personal data involved in seeking such views. Although it should be noted that consent to processing is obviously not a way for seeking the views of the data subjects;
- これらの見解は、その文脈により、管理者がその見解を得るに当たり関係する個人データの取扱いに法的根拠を有していることを保証する様々な手段で求めることができる（例えば、取扱いの目的と手段に関する一般的な研究、スタッフの代理人への問合せ、又はデータ管理者の将来の顧客への通常調査など)。もっとも、取扱いに対する同意は明らかにデータ主体の見解を求める手段ではないことに留意すべきである。
- if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented;
- データ管理者の最終決定がデータ主体の見解と異なる場合は、継続又は非継続の理由を文書化すべきである。
- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable.
- 管理者はデータ主体の見解を求めることが適切でないと判断した場合、例えば、そのようにすると会社の事業計画における秘密が漏れる可能性がある場合、又は不均衡又は実行不可能となる可能性がある場合、その正当な理由も文書化すべきである。

Finally, it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.:

最後に、内部方針、手順、ルールなどに応じて、他の具体的な役割と責任も規定、文書化す

るのが望ましい慣行である。例えば次のようなものである。

- where specific business units may propose to carry out a DPIA, those units should then provide input to the DPIA and should be involved in the validation process;
- 特定の部署が DPIA 実施を提案できる場合、この部署は DPIA へのインプットを提供し、検証プロセスに参加するべきである。
- where appropriate, it is recommended to seek the advice from independent experts of different professions[24] (lawyers, IT experts, security experts, sociologists, ethics, etc.).
- 適切な場合、別の職業の独立した専門家[24]（弁護士、IT 専門家、セキュリティ専門家、社会学者、倫理学者など）のアドバイスを求めることが勧告される。
- the roles and responsibilities of the processors must be contractually defined; and the DPIA must be carried out with the processor's help, taking into account the nature of the processing and the information available to the processor (Article 28(3)(f));
- 処理者の役割と責任は契約で規定しなければならない。DPIA はその取扱いの性質と処理者の利用できる情報を考慮して、処理者の助けを得て、実施しなければならない（第 28 条(3)(f)）。
- the Chief Information Security Officer (CISO), if appointed, as well as the DPO could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context;
- 最高情報セキュリティ責任者（CISO）が任命されている場合、最高情報セキュリティ責任者（CISO）及び DPO は、管理者が特定の取扱作業について DPIA を行うよう提案することができる。また、その方法について利害関係者を助け、リスク評価の質及び残存リスクが許容できるかどうかの評価を助け、データ管理者に特有な知識の進展を助けるべきである。
- the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3: EU へのプライバシー影響評価枠組み勧告、成果物 D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

- 最高情報セキュリティ責任者（CISO）が任命されている場合、最高情報セキュリティ責任者（CISO）及び／又はIT部門は、セキュリティ上又は運用上の必要に応じてデータ管理者を支援すべきであり、DPIAの実施を提案することができる。

c) What is the methodology to carry out a DPIA? Different methodologies but common criteria.

c) DPIA実施方法とは何か？様々な方法があるが、共通基準がある。

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

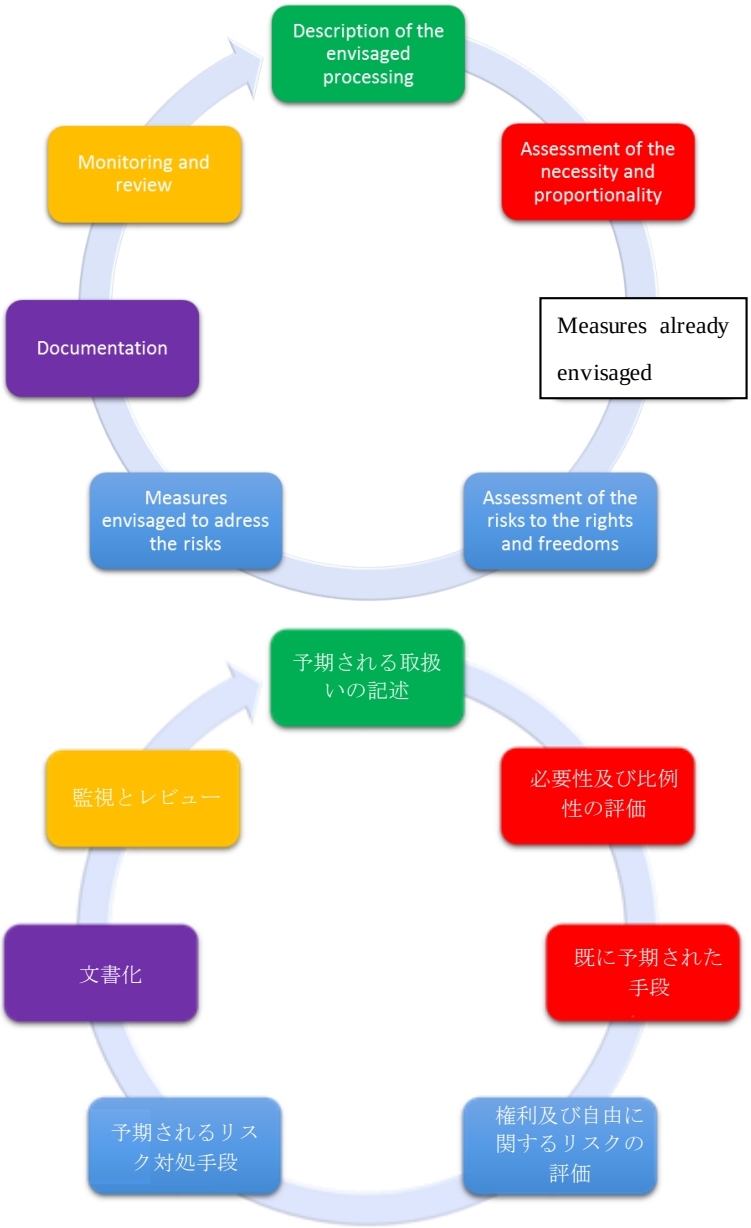
GDPRはDPIAの最低限の特性を定めている（第35条(7)及び前文第84項、第90項）。

- "*a description of the envisaged processing operations and the purposes of the processing*";
- *予期される取扱作業と取扱いの目的についての記述*
- "*an assessment of the necessity and proportionality of the processing*";
- *取扱いの必要性及び比例性の評価*
- "*an assessment of the risks to the rights and freedoms of data subjects*";
- *データ主体の権利及び自由に関するリスクの評価*
- "*the measures envisaged to:*
    - o "*address the risks*";
    - o "*demonstrate compliance with this Regulation*".
- *予期される措置*
    - o *リスク対処*
    - o *本規則の遵守の証明*

The following figure illustrates the generic iterative process for carrying out a DPIA[25]:

下図はDPIA実施の一般的反復プロセスを図示したものである[25]。

[25] It should be underlined that the process depicted here is iterative: in practice, it is likely that each of the stages is revisited multiple times before the DPIA can be completed.
ここに図示したプロセスは反復的であることに留意すべきである。実際には、DPIA完了までに各段階を複数回踏むことが予想される。



Compliance with a code of conduct (Article 40) has to be taken into account (Article 35(8)) when assessing the impact of a data processing operation. Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors (Article 42), as well as Binding Corporate Rules (BCR), should be taken into account as well.

データ取扱作業の影響評価の際、行動規範の遵守（第 40 条）を考慮しなければならない（第 35 条(8)）。管理者及び処理者が、取扱作業において GDPR 及び拘束的企業準則（BCR）を遵守していることを証明するための認証、シール及びマーク（第 42 条）もまた考慮されるべきである。

All the relevant requirements set out in the GDPR provide a broad, generic framework for designing and carrying out a DPIA. The practical implementation of a DPIA will depend on the requirements set out in the GDPR which may be supplemented with more detailed practical guidance. The DPIA implementation is therefore scalable. This means that even a small data controller can design and implement a DPIA that is suitable for their processing operations.

GDPR に定めた関連ある義務はすべて、DPIA の作成と実施について、広範で一般的な枠組みを定めたものである。実際の DPIA の実施は、GDPR に定める要求によるが、より詳細な実務のガイダンスで補うことができる。したがって、DPIA の実施には拡張性がある。これは、小規模な管理者も、自己の取扱作業に適切な DPIA を作成・実施できることを意味する。

Recital 90 of the GDPR outlines a number of components of the DPIA which overlap with welldefined components of risk management (e.g. ISO 31000[26]). In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following three processes, by:
GDPR の前文第 90 項は、明確に規定されたリスク管理要素（ISO 31000 など [26]）と重なる DPIA の要素の多数を概説している。リスク管理用語では、DPIA は次の 3 つのプロセスによって、自然人の権利及び自由に関する「*リスク管理*」を目的とする。

- establishing the context: "*taking into account the nature, scope, context and purposes of the processing and the sources of the risk*";
- 文脈を認識する。「*取扱いの性質、範囲、文脈、目的、及びリスクの発生源を考慮する*」。
- assessing the risks: "*assess the particular likelihood and severity of the high risk*";
- リスクを評価する。「*高いリスクの特有の可能性と重大性を評価する*」。
- treating the risks: "*mitigating that risk*" and "*ensuring the protection of personal data*", and "*demonstrating compliance with this Regulation*".
- リスクに対処する。「*そのリスクの低減*」、「*個人データの確実な保護*」、及び「*本規則の遵守の証明*」。

Note: the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, as is the case in certain fields (e.g. societal security).Conversely, risk

[26] Risk management processes: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review (see terms and definitions, and table of content, in the ISO 31000 preview:
リスク管理プロセス：対話と協議、文脈の認識、リスク評価、リスク対処、監視とレビュー（ISO 31000 プレビューの用語と定義、目次を参照のこと）
https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

management in other fields (e.g. information security) is focused on the organization.

注：GDPR に基づく DPIA は、データ主体の権利に対するリスク管理のツールであるため、ある分野（社会セキュリティなど）の場合と同様に、データ主体の視点を考慮する。逆に、別の分野（情報セキュリティなど）におけるリスク管理は組織に焦点が置かれる。

The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them.

GDPR はデータ管理者に、既存の作業慣行に合わせられるようにするため、DPIA の詳細な構造と形式を定める柔軟性を与えている。EU と世界には、確立された様々なプロセスが多数あり、それらは前文第 90 項で説明された要素を考慮している。しかし形式がどのようなものであれ、DPIA は管理者がリスク対処手段を取れるように、純粋なリスク評価でなければならない。

Different methodologies (see Annex1 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR.

GDPR に定める基本的要件の実施を助けるため、様々な方法（データ保護とプライバシー影響評価方法の例は、付録 1 を参照）を利用することができる。

In order to allow these different approaches to exist, whilst allowing controllers to comply with the GDPR, common criteria have been identified (see Annex 2). They clarify the basic requirements of the Regulation, but provide enough scope for different forms of implementation. These criteria can be used to show that a particular DPIA methodology meets the standards required by the GDPR. It is up to the data controller to choose a methodology, but this methodology should be compliant with the criteria provided in Annex 2.

管理者が GDPR を遵守できるようにしながら、これらの様々なアプローチを提供するため、共通基準が設けられた（付録 2 参照）。これらは本規則の基本的要件を明確にするものであ

るが、異なる実施形式にも十分な範囲を与えている。これらの基準は、特定の DPIA 方法が GDPR の求める標準を満たすことを示すのに用いることができる。方法を選択するのはデータ管理者であるが、その方法は付録 2 に規定された基準に適合したものであるべきである。

The WP29 encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectoral knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures). This means the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies or carrying out particular types of processing operation.

WP29 は特定分野用の DPIA の枠組み作成を推奨する。そうすれば特定の分野知識を利用できるからであり、つまり DPIA が特定のタイプの取扱作業の具体的内容に対応できることになる（例えば特定の種類のデータ、企業資産、潜在的影響、脅威、手段など）。このことは、DPIA が特定の経済分野に生じる問題、又は特定の技術利用時や特定の種類の取扱作業実施時に生じる問題に対処できることを意味する。

Finally, where necessary, "the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operation" (Article 35(11)[27]).

最後に、必要に応じ、「管理者は、取扱作業によって表されるリスクに変化がある場合には、少なくとも、取扱いがデータ保護影響評価に従って実施されているかを評価するため、見直しをしなければならない」（第 35 条（11）[27]）。

d) Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA.

d) DPIA を公開する義務はあるか？義務はないが、概要を公開することは信頼性を高めうる。また、DPIA 全体は事前協議の場合、又は DPA から要求があった場合には監督機関に伝えなければならない。

Publishing a DPIA is not a legal requirement of the GDPR. It is the controller´s decision to do

[27] Article 35(10) explicitly excludes only the application of article 35 paragraphs 1 to 7.
第 35 条 10 項は、第 35 条 1 項から 7 項の適用のみ明確に除外している。

so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.

DPIA の公開は GDPR の法的義務ではない。公開はデータ管理者の決定である。しかし、管理者は DPIA の少なくとも一部、概要又は結論などの公開を検討すべきである。

The purpose of such a process would be to help foster trust in the controller's processing operations, and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA.

このようなプロセスの目的は、管理者の取扱作業の信頼性の助成や、アカウンタビリティ及び透明性の証明に役立つであろう。一般社会の構成員がその取扱作業で影響を受ける場合には、DPIA の公開は特に望ましい慣行となる。これは特に公的機関が DPIA を実施する場合に、当てはまるであろう。

The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. In these circumstances, the published version could consist of just a summary of the DPIA's main findings, or even just a statement that a DPIA has been carried out.

公開される DPIA は、必ずしも評価全体を含んでいる必要はない。特に DPIA がデータ管理者のセキュリティ・リスクに関わる特定情報を提示しうる場合や、商業上の秘密又は商業的なセンシティブ情報を与えてしまう可能性がある場合はその必要はない。そのような場合には、公開版は DPIA の主な発見事項の概要だけ、あるいは DPIA が実施されたとの記述のみであっても構わない。

Moreover, where a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be fully provided (Article 36(3)(e)). The supervisory authority may provide its advice[28], and will not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable in

[28] Written advice to the controller is only necessary when the supervisory authority is of the opinion that the intended processing is not in line with the regulation as per Article 36(2).
書面による管理者へのアドバイスは、監督機関が意図された取扱いは、第 36 条 2 項に規定する規制に従っていないとの見解を持つ場合にのみ必要とされる。

each Member State on public access to official documents.

さらに、DPIA が高い残存リスクを明らかにする場合には、データ管理者は監督機関に取扱いについて事前の協議を求めることが要求される（第 36 条(1)）。この一環として、DPIA 全体が提供されなければならない（第 36 条(3)(e)）。監督機関は、各加盟国における公文書に対するアクセスに関し、適用される原則に従って、アドバイス[28]をすることができ、企業秘密の漏えいやセキュリティの脆弱性を明らかにすることはしない。

E. When shall the supervisory authority be consulted? When the residual risks are high

E. どのような場合、監督機関との協議を行うべきか？残存リスクが高い場合である。

As explained above:

上記の通り、

- a DPIA is required when a processing operation "*is likely to result in a high risk to the rights and freedoms of natural person*" (Article 35(1), see III.B.a). As an example, the processing of health data on a large scale is considered as likely to result in a high risk, and requires a DPIA;
- 取扱作業が「*自然人の権利及び自由に高いリスクをもたらすことが予想される*」場合に DPIA が求められる（第 35 条(1)、III.B.a.参照）。その例として、大規模な健康状態データの取扱いは高いリスクをもたらすことが予想され、DPIA が必要である。
- then, it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures[29] envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR (Article 35(7), see III.C.c). An example could be for the storage of personal data on laptop computers the use of appropriate technical and organisational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, etc.) in addition to existing policies (notice, consent, right of access, right to object, etc.).
- このため、データ主体の権利及び自由に対するリスクを評価し、それらのリスクを容認できるレベルまで低減して、GDPR の遵守を証明するために予期される手段[29]を特定するのはデータ管理者の責任である（第 35 条(7)、III.C.c.参照）。その例としては、ノートパソコンに保存に関しては、既存の方針（通知、同意、アクセス権、拒否権など）に加えて、適切な技術的・組織的な安全管理措置（効果的な完全なディスク暗号化、強固な

[29] Including taking account of existing guidance from EDPB and supervisory authorities and taking account of the state of the art and the costs of implementation as prescribed by Article 35(1).
EDPB 及び監督機関の既存ガイドラインを考慮すること、及び第 35 条(1)で規定されている実施の現状とコストを考慮することを含む。

カギの管理、適切なアクセス制限、安全なバックアップなど）の使用が挙げられるだろう。

In the laptop example above, if the risks have been considered as sufficiently reduced by the data controller and following the reading of Article 36(1) and recitals 84 and 94, the processing can proceed without consultation with the supervisory authority. It is in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remains high) that the data controller must consult the supervisory authority.

上記のノートパソコンの例では、リスクがデータ管理者及び第 36 条(1)及び前文第 84 項と第 94 項に従うことにより十分に軽減されたと思われる場合には、取扱いは監督機関との協議を行うことなく進められる。識別されたリスクがデータ管理者によって十分に対処できない場合（つまり残存リスクが高いままの場合）には、データ管理者は監督機関と協議しなければならない。

An example of an unacceptable high residual risk includes where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well-known vulnerability is not patched).

残存リスクの高さが許容できない例としては、データ主体が重大又は非可逆的な結果を被ってそれが克服できないかも知れない場合（例：データ主体の生命の脅威、一時解雇、財政的危機に繋がるデータへの違法なアクセス）、及び／又はリスクの発生が明白と思われる場合（例：データの共有、使用又は配布モード、周知の脆弱性に手当がされていないためデータにアクセスする人数を減少させることができないことによる）などがある。

Whenever the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high), consultation with the supervisory authority is required[30].

[30] Note: "pseudonymization and encryption of personal data" (as well as data minimization, oversight mechanisms, etc.) are not necessarily appropriate measures. They are only examples. Appropriate measures depend on the context

データ管理者がリスクを許容できるレベルまで軽減するための十分な手段を見出せない場合（つまり残存リスクが高いまま）はいつでも、監督機関との協議が必要とされる[30]。

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5)).

さらに、加盟国の法律が、管理者に、公共の利益のために実施する任務の履行について、監督機関との協議を要求している場合、及び／又は同機関から事前承認を得るよう要求している場合はいつでも、データ管理者は、監督機関と協議しなければならない。この公共の利益のために実施する任務には、社会的保護及び公衆衛生に関する取扱いを含む（第 36 条(5)）。

It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

ただし、残存リスクレベルに基づいて監督機関との協議が必要か否かに関わらず、DPIA 記録を保持し、いずれ DPIA を更新する義務は常にあるものとする。

IV. Conclusions and recommendations

IV. 結論と勧告

DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processing operations. They are scalable and can take different forms, but the GDPR sets out the basic requirements of an effective DPIA. Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance.

DPIA は、データ管理者が GDPR に準拠したデータ取扱システムを実施するのに有用な方法であり、一部の取扱作業には義務化される場合がある。DPIA は拡張可能で様々な形式がありうるが、GDPR は効果的な DPIA の基本的要件を定めている。データ管理者は DPIA 実施

and the risks, specific to the processing operations.
注：「個人データの仮名化及び暗号化」（及びデータの最少化、監督の仕組み等）は必ずしも適切な方法ではない。これらは例に過ぎない。適切な方法は、取扱作業に固有の文脈及びリスクによる。

を法の遵守を助ける有用でポジティブな作業だと見なすべきである。

Article 24(1) sets out the basic responsibility of the controller in terms of complying with the GDPR: "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*".

第 24 条(1)は、GDPR 遵守の観点で、管理者の基本的責任を次のように定めている。「*取扱いの性質、範囲、文脈、目的並びに自然人の権利及び自由に関するリスクの様々な可能性及び重大性を考慮し、管理者は本規則に従って取扱いが実行されていることを保証及び証明するため適切な技術的及び組織的対策を実施しなければならない。これら対策は、見直され、必要に応じて更新されなければならない*」。

The DPIA is a key part of complying with the Regulation where high risk data processing is planned or is taking place. This means that data controllers should use the criteria set out in this document to determine whether or not a DPIA has to be carried out. Internal data controller policy could extend this list beyond the GDPR's legal requirements. This should result in greater trust and confidence of data subjects and other data controllers.

DPIA は、リスクの高いデータ取扱いが計画又は実行されている場合、本規則の遵守の重要部分である。つまり、データ管理者は、DPIA を実施する必要があるか否かを判断するために、本ガイドラインに定める基準を利用すべきである。組織内のデータ管理者に関する方針によって、この基準リストを GDPR の法的義務以上に拡大してもよい。そうすればデータ主体と他のデータ管理者の信頼と安心を拡大するに違いない。

Where a likely high risk processing is planned, the data controller must:
リスクが高いと予期される取扱いが計画されている場合、データ管理者は以下を行わなければならない。

- choose a DPIA methodology (examples given in Annex 1) that satisfies the criteria in Annex 2, or specify and implement a systematic DPIA process that:

- 付録 2 の基準を満たす DPIA の方法（例は付録 1 に記載）を選択する、又は以下の体系的な DPIA のプロセスを規定し、実施すること。
    - is compliant with the criteria in Annex 2;
    - 付録 2 の基準を準拠するプロセス
    - is integrated into existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture;
    - 組織内のプロセス、文脈、文化に合わせて既存の設計、開発、変更、リスク、及び組織的レビュー・プロセスに統合されたプロセス
    - involves the appropriate interested parties and clearly define their responsibilities (controller, DPO, data subjects or their representatives, business, technical services, processors, information security officer, etc.);
    - 適切な利害関係者を関与させ、それらの責任を明確に規定するプロセス（管理者、DPO、データ主体又はその代理人、企業、技術サービス、処理者、情報セキュリティ担当責任者など）。
- provide the DPIA report to the competent supervisory authority when required to do so;
- 求められた場合には所轄監督機関に DPIA 報告書を提供すること。
- consult the supervisory authority when they have failed to determine sufficient measures to mitigate the high risks;
- 高いリスクを低減するために十分な手段を決定できなかった場合、監督機関と協議すること。
- periodically review the DPIA and the processing it assesses, at least when there is a change of the risk posed by processing the operation;
- 定期的に DPIA とその評価する取扱いを見直すこと。少なくとも取扱作業で提示されるリスクに変化があった時には見直すこと。
- document the decisions taken.
- 決定事項を文書化すること。

Annex 1 – Examples of existing EU DPIA frameworks
付録 1 - 既存の EU の DPIA 枠組み例

The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). Such a framework can be bespoke to the data controller or common across a particular industry. Previously published frameworks developed by EU DPAs and EU sector-specific frameworks include (but are not limited to):

GDPR はどの DPIA プロセスを取らなければならないか明記していない。しかし、その代りとして既存の作業慣行が、第 35 条(7)に記載の要素を考慮する限り、データ管理者がその既存の慣行を補完する枠組みを導入することを認めている。このような枠組みはデータ管理者にとって、又は特定の業界全体にとって示しうる。EU の DPA が作成し、これまでに公開した枠組みと EU の分野別枠組みは以下の通りである。(しかし、これに限られるものではない。)

Examples of EU generic frameworks:
EU の一般的枠組み例

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31].
- ドイツ：標準データ保護モデル、V.1.0 - トライアル・バージョン、2016 年 [31] https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
- スペイン：*個人データ保護の影響評価ガイド (EIPD)*、データ保護庁（AGPD）、2014 年。 https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
- フランス：*プライバシー影響評価 (PIA)*、情報処理の自由に関する国会委員会（CNIL）、2015 年。

[31] Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.
2016 年 11 月 9～10 日、キュールングスボルンでの連邦・州独立データ保護当局第 92 回会議において、満場一致で承認（バイエルン州棄権）。

https://www.cnil.fr/fr/node/15798

- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
- イギリス：*プライバシー影響評価実施行動規範*、情報コミッショナー事務局（ICO）、2014 年。
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Examples of EU sector-specific frameworks:
EU の分野別枠組み例

- Privacy and Data Protection Impact Assessment Framework for RFID Applications [32].
- RFID アプリケーションに関するプライバシー及びデータ保護影響評価枠組み [32]。
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems [33]
- スマート・グリッド及びスマート・メータリング・システムのデータ保護影響評価テンプレート [33]。
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

An international standard will also provide guidelines for methodologies used for carrying out a DPIA (ISO/IEC 29134[34]).

---

[32] See also:
下記も参照のこと。
-Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification.
RFID を利用したアプリケーションにおけるプライバシー及びデータ保護の原則実施に関する、2009 年 5 月 12 日付け欧州委員会勧告。
https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
-Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications.
RFID アプリケーションに関するプライバシー及びデータ保護影響評価枠組みへの業界提案改訂版に関する意見書 9/2011。
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33] See also the Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force.
欧州委員会スマート・グリッド・タスクフォース専門家グループ 2 が作成した、スマート・グリッド及びスマート・メータリング・システムのデータ保護影響評価テンプレート（DPIA テンプレート）に関する意見書 07/2013 も参照のこと。
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

[34] ISO/IEC 29134 (project), Information technology – Security techniques – Privacy impact assessment – Guidelines, International Organization for Standardization (ISO).
ISO 発行 ISO/IEC 29134（予定）「情報技術 - セキュリティ技術 - プライバシー影響評価 – ガイドライ

国際標準も DPIA 実施に利用できる方法のガイドラインを提供する予定である（ISO/IEC 29134[34]）。

Annex 2 – Criteria for an acceptable DPIA

付録 2 - 容認できる DPIA の基準

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

データ管理者が DPIA を実施するか否か、又は DPIA 実施の方法を評価する際に利用できる以下の基準が、GDPR 遵守のために十分に網羅的であることを WP29 は提言している。

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
- ☐ 取扱いの体系的な記述がなされている（第 35 条(7)(a)）。
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ 取扱いの性質、範囲、文脈、目的が考慮されている（前文第 90 項）。
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ 個人データ、取得者、個人データの保存期間が記録されている。
  - ☐ a functional description of the processing operation is provided;
  - ☐ 取扱作業の機能上の説明がなされている。
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ 個人データが依拠する資産（ハードウェア、ソフトウェア、ネットワーク、人材、書類又は書類送信チャンネル）が識別されている。
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
  - ☐ 承認された行動規範の遵守が考慮されている（第 35 条(8)）。
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
- ☐ 必要性及び比例性が評価されている（第 35 条(7)(b)）。

ン、ISO」。

- ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
- ☐ 本規則遵守のために予期される手段が、以下を考慮して決定されている（第 35 条(7)(d)及び前文第 90 項）。
  - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
  - ☐ 以下の事項を根拠として、取扱いの必要性及び比例性に寄与する手段。
    - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
    - ☐ 規定され、明白で合法的な目的（第 5 条(1)(b)）。
    - ☐ lawfulness of processing (Article 6);
    - ☐ 取扱いの合法性（第 6 条）。
    - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
    - ☐ 適切で、関連性があり、必要なデータだけに限定されていること（第 5 条(1)(c)）。
    - ☐ limited storage duration (Article 5(1)(e));
    - ☐ 保存期間が限定されていること（第 5 条(1)(e)）。
  - ☐ measures contributing to the rights of the data subjects:
  - ☐ データ主体の権利に寄与する手段。
    - ☐ information provided to the data subject (Articles 12, 13 and 14);
    - ☐ データ主体に提供される情報（第 12 条、第 13 条、14 条）。
    - ☐ right of access and to data portability (Articles 15 and 20);
    - ☐ アクセス権とデータポータビリティの権利（第 15 条及び 20 条）。
    - ☐ right to rectification and to erasure (Articles 16, 17 and 19);
    - ☐ 訂正及び消去権（第 16 条、17 条及び第 19 条）。
    - ☐ right to object and to restriction of processing (Article 18, 19 and 21);
    - ☐ 異議を唱える権利及び取扱い制限の権利（第 18 条、19 条及び 21 条）。
    - ☐ relationships with processors (Article 28);
    - ☐ 処理者との関係（第 28 条）。

- ☐ safeguards surrounding international transfer(s) (Chapter V);
- ☐ 国際移転に伴う保護措置（第 5 章）。
- ☐ prior consultation (Article 36).
- ☐ 事前協議（第 36 条）。

☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):

☐ データ主体の権利及び自由に対するリスクが管理されていること（第 35 条(7)(e)）。

- ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
- ☐ リスクの発生源、性質、特殊性、重大性が評価されていること（前文第 84 項と比較）、又はより具体的には、それぞれのリスク（違法アクセス、データの意図しない改変・消失）がデータ主体の視点から評価されていること。
  - ☐ risks sources are taken into account (recital 90);
  - ☐ リスクの発生源が考慮されていること（前文第 90 項）。
  - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
  - ☐ 違法アクセスを含むイベント、データの意図しない改変・消失があった場合のデータ主体の権利及び自由に対する潜在的影響が識別されていること。
  - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
  - ☐ 違法アクセス、データの意図しない改変・消失につながる脅威が識別されていること。
  - ☐ likelihood and severity are estimated (recital 90);
  - ☐ 可能性と重大性が試算されていること（前文第 90 項）。
- ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);

- ☐ これらのリスクに対処するために予期される手段が決まっていること（第 35 条(7)(d)及び前文第 90 項）。

☐ interested parties are involved:

☐ 利害関係者が関与していること。

- ☐ the advice of the DPO is sought (Article 35(2));
- ☐ DPO のアドバイスを求めていること（第 35 条(2)）。
- ☐ the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).
- ☐ 必要に応じ、データ主体又はその代理人の見解を求めていること（第 35 条(9)）。