仮日本語訳

Guidelines 4/2019 on Article 25
Data Protection by Design and by Default
第 25 条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に関するガイドライン 4/2019

Version 2.0
バージョン 2.0

Adopted on 20 October 2020
2020 年 10 月 20 日採択

本書面は、欧州データ保護会議(EDPB)により 2020 年 10 月 20 日に採択された“Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”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。

Version history
バージョン履歴

Version 1.0 バージョン 1.0	13 November 2019 2019 年 11 月 13 日	Adoption of the Guidelines for public consultation パブリック・コンサルテーションのためのガイドラインの採択。
Version 2.0 バージョン 2.0	20 October 2020 2020 年 10 月 20 日	Adoption of the Guidelines by the EDPB after public consultation パブリック・コンサルテーション後の EDPB によるガイドラインの採択。

Table of contents
目次

The European Data Protection Board
欧州データ保護会議は

Having regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC], (hereinafter "GDPR"),
個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する、2016 年 4 月 27 日の欧州議会及び理事会の規則 2016/679/EU、（以下「GDPR」という）、の第 70 条(1)(e)に鑑み、

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,
2018 年 7 月 6 日の EEA 共同委員会の決定 No 154/2018 により改正された EEA 協定、特にその附属書 XI 及び議定書 37 に鑑み、

Having regard to Article 12 and Article 22 of its Rules of Procedure,
その手続規則の第 12 条及び第 22 条に鑑み、

HAS ADOPTED THE FOLLOWING GUIDELINES
次のガイドラインを採択する

Executive summary
要旨

In an increasingly digital world, adherence to Data Protection by Design and by Default requirements plays a crucial part in promoting privacy and data protection in society. It is therefore essential that controllers take this responsibility seriously and implement the GDPR obligations when designing processing operations.
デジタル化が進む世界では、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要件を遵守することが、社会におけるプライバシー及びデータ保護を促進する上で重要な役割を果たす。したがって、管理者は、この責任を真剣に受け止め、取扱業務を設計する際に GDPR の義務を実装することが不可欠である。

These Guidelines give general guidance on the obligation of Data Protection by Design and by Default (henceforth "DPbDD") set forth in Article 25 in the GDPR. DPbDD is an obligation for all controllers, irrespective of size and varying complexity of processing. To be able to implement the requirements of DPbDD, it is crucial that the controller understands the data protection principles and the data subject's rights and freedoms.
このガイドラインは、GDPR の第 25 条に規定されている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（以下「DPbDD」という）の義務に関して、一般的なガイダンスを提供するものである。 DPbDD は、取扱いの規模及び複雑さの違いに関係なく、全ての管理者にとって、義務である。 DPbDD の要件を実装できるようにするには、管理者がデータ保護の基本原則並びにデータ主体の権利及び自由を理解することが重要である。

The core obligation is the implementation of *appropriate* measures and necessary safeguards that provide *effective implementation* of the *data protection principles* and*,* consequentially*, data subjects' rights and freedoms by design and by default*. Article 25 prescribes both design and default elements that should be taken into account. Those elements, will be further elaborated in these Guidelines.

その義務の中核は、*バイデザイン及びバイデフォルトで、データ保護の基本原則の効果的な実装*、ひいては、*データ主体の権利及び自由*を提供するような、*適切な*措置及び必要な保護措置を実装することである。第 25 条は、考慮すべきデザイン及びデフォルト両方の要素を規定している。これらの要素について、当該ガイドラインのなかで更に詳しく説明する。

Article 25(1) stipulates that controllers should consider DPbDD early on when they plan a new processing operation. Controllers shall implement DPbDD *before* processing, and also *continually* at the time of processing, by regularly reviewing the effectiveness of the chosen measures and safeguards. DPbDD also applies to existing systems that are processing personal data.
第 25 条 (1) は、管理者が新規の取扱業務を計画する際に、早い段階で DPbDD を考慮する必要があると規定している。管理者は、取扱いの*前に* DPbDD を実装するものとし、また、自身が選択した措置及び保護措置の実効性を定期的に見直すことにより、取扱中の時点においても*継続的に* DPbDD を実装するものとする。DPbDD は、個人データを取扱中の既存のシステムにも適用される。

The Guidelines also contain guidance on how to effectively implement the data protection principles in Article 5, listing key design and default elements as well as practical cases for illustration. The controller should consider the appropriateness of the suggested measures in the context of the particular processing in question.
当該ガイドラインには、第 5 条のデータ保護の基本原則を効果的に実装する方法に関するガイダンスも含まれており、主要なデザイン及びデフォルトの要素並びに説明のための具体例が列挙されている。管理者は、該当の特定の取扱いに関連して、提案されている措置の適切性を考慮しなければならない。

The EDPB provides recommendations on how controllers, processors and producers can cooperate to achieve DPbDD. It encourages the controllers in industry, processors, and producers to use DPbDD as a means to achieve a competitive advantage when marketing their products towards controllers and data subjects. It also encourages all controllers to make use of certifications and codes of conduct.
EDPB は、DPbDD を達成するために、管理者、処理者及び開発者がどのように協力できるかに関する勧告を提供する。EDPB は、業界の管理者、処理者及び開発者に対し、管理者及びデータ主体に向けて自社の製品をマーケティングする際に、競争上の優位性を達成する手段として、DPbDD を使用するよう奨励する。EDPB はまた、全ての管理者に対し、認証及び行動規範を活用するよう奨励する。

1 SCOPE
範囲

1. The Guidelines focus on controllers' implementation of DPbDD based on the obligation in Article 25 of the GDPR.[1] Other actors, such as processors and producers of products, services and applications (henceforth "producers"), who are not directly addressed in Article 25, may also find these Guidelines useful in creating GDPR compliant products and services that enable controllers to fulfil their data

[1] The interpretations provided herein equally apply to Article 20 of Directive (EU) 2016/680, and Article 27 of Regulation 2018/1725.
ここで提供される解釈は、指令 (EU) 2016/680 の第 20 条、及び規則 2018/1725 の第 27 条にも同様に適用される。

protection obligations.[2] Recital 78 of the GDPR adds that DPbDD should be taken into consideration in the context of public tenders. Despite all controllers having the duty to integrate DPbDD into their processing activities, this provision fosters the adoption of the data protection principles, where public administrations should lead by example. The controller is responsible for the fulfilment of the DPbDD obligations for the processing carried out by their processors and sub-processors, they should therefore take this into account when contracting with these parties.
当該ガイドラインは、管理者が GDPR 第 25 条の義務に基づき DPbDD を実装することに焦点を当てている。[1] 第 25 条で直接対応されていない、処理者並びに製品、サービス、及びアプリケーションの開発者（以下「開発者」という）などの他の関係者にとっても、管理者らがそのデータ保護の義務を達成できるような GDPR に準拠する製品及びサービスを開発するなかで、当該ガイドラインが役立ちうる。[2] GDPR 前文第 78 項は更に、公共入札の際においても DPbDD を考慮する必要があるとしている。全ての管理者には DPbDD を自身の取扱活動に統合する義務がある一方で、この条文はデータ保護の基本原則を取り入れるよう促しており、そこでは公的機関が模範を示すべきである。 管理者は、自身の処理者及び準処理者が実行する取扱いについて DPbDD 義務が充足していることに責任があり、したがって、これらの当事者と契約する際にはこのことを考慮に入れる必要がある。

2. The requirement described in Article 25 is for controllers to have data protection designed into the processing of personal data and as a default setting and this applies throughout the processing lifecycle. DPbDD is also a requirement for processing systems pre-existing before the GDPR entered into force. Controllers must have the processing consistently updated in line with the GDPR. For more information on how to maintain an existing system in line with DPbDD, see subchapter 2.1.4 of these Guidelines. The core of the provision is to ensure *appropriate* and *effective* data protection both by *design* and by *default,* which means that controllers should be able to demonstrate that they have the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective.
第 25 条に記載されている要件は、管理者が、データ保護を個人データの取扱いの中に設計し、かつデフォルト設定としてデータを保護することであり、またこのことは、取扱いのライフサイクル全体を通して適用される。DPbDD はまた、GDPR が発効する前に存在した取扱いシステムにも要求される。管理者は、GDPR に沿って自身の取扱いを常に更新しておかなければならない。DPbDD に沿って既存のシステムを維持する方法の詳細については、当該ガイドラインの第 2.1.4 項を参照すること。この条文の中核は、*バイデザイン*及び*バイデフォルト*の両方で、*適切*かつ*効果的な*データ保護を確保することである。このことは、管理者が、データ保護の基本原則及びデータ主体の権利及び自由を実効性があるよう確保するために、取扱いの中に適切な措置及び保護措置を実装しているということを証明可能でなければならないことを意味する。

[2] Recital 78 GDPR clearly states this need: "*When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the "state of the art", to make sure that controllers and processors are able to fulfil their data protection obligations*".
GDPR 前文第 78 項は、この必要性について次のように明確に規定している。*「個人データの取扱いを基盤とし、又は、その職務を遂行するために個人データを取扱うアプリケーション、サービス及び製品を開発、設計、選択及び利用する場合、そのような製品、サービス及びアプリケーションの開発者は、そのような製品、サービス及びアプリケーションを開発及び設計する際、データ保護の権利を考慮に入れることが奨励され、また、最新技術を適正に考慮に入れた上で、管理者及び処理者がそのデータ保護義務を履行できるようにすることが奨励されなければならない」。*

3. Chapter 2 of the Guidelines focuses on an interpretation of the requirements set forth by Article 25 and explores the legal obligations introduced by the provision. Examples on how to apply DPbDD in the context of specific data protection principles are provided in Chapter 3.
当該ガイドラインの第 2 章は、第 25 条に定められた要件の解釈に焦点を当て、この条文によって導入されている法的義務について検討する。特定のデータ保護の基本原則との関連で DPbDD を適用する方法についての事例を第 3 章で提供する。

4. The Guidelines address the possibility to establish a certification mechanism to demonstrate compliance with Article 25 in Chapter 4, as well as how the Article may be enforced by supervisory authorities in Chapter 5. Finally, the Guidelines provide stakeholders with further recommendations on how to successfully implement DPbDD. The EDPB recognizes the challenges for small and medium enterprises (henceforth "SMEs") to fully comply with the obligations of DPbDD, and provides additional recommendations specifically to SMEs in Chapter 6.
当該ガイドラインは、第 25 条への遵守を証明するために、認証メカニズムを確立する可能性について第 4 章で対応し、また監督機関が同条をどのように執行させうるかについて第 5 章で言及する。最後に、当該ガイドラインは、利害関係者に対し、DPbDD の実装を達成する方法について、追加的な勧告を提供する。EDPB は、小規模及び中規模の企業（以下「SMEs」という）が DPbDD の義務を完全に遵守する場合の課題を認識しており、第 6 章において特に SMEs に対して、追加の勧告を提供する。

2 ANALYSIS OF ARTICLE 25(1) AND (2) of the GDPR
GDPR 第 25 条 (1) 及び (2) の分析

5. The aim of this Chapter is to explore and provide guidance on the requirements to data protection by design in Article 25(1) and to data protection by default in Article 25(2) respectively. Data protection by design and data protection by default are complementary concepts, which mutually reinforce each other. Data subjects will benefit more from data protection by default if data protection by design is concurrently implemented – and vice versa.
この章の目的は、第 25 条 (1) のデータ保護バイデザイン及び第 25 条 (2) のデータ保護バイデフォルトそれぞれについて、要件を調査し、ガイダンスを提供することである。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は補完的な概念であり、それらは相互に強化し合うものである。データ保護バイデザインが同時に実装されている場合、データ主体はデータ保護バイデフォルトからより多くの利益を得る。またその逆も同じである。

6. DPbDD is a requirement for all controllers, including small businesses and multinational companies alike. That being the case, the complexity of implementing DPbDD may vary based on the individual processing operation. Regardless of the size however, in all cases, positive benefits for controller and data subject can be achieved by implementing DPbDD.
DPbDD は、小規模ビジネス及び多国籍企業にも同様に求められる、全ての管理者にとっての要件である。そのため、DPbDD の実装の複雑さは、個々の取扱業務により異なる可能性がある。一方、規模に関係なく、全ての場合において、DPbDD を実装することで、管理者及びデータ主体にとって、好ましい利益が得られる。

2.1 Article 25(1): Data protection by design
第 25 条(1) ：データ保護バイデザイン

2.1.1 Controller's obligation to implement appropriate technical and organisational measures and necessary safeguards into the processing

その取扱いの中に適切な技術的措置及び組織的措置並びに必要な保護措置を実装する管理者の義務

7. In line with Article 25(1) the controller shall implement *appropriate* technical and organisational *measures* which are designed to implement the data protection principles and to integrate the *necessary safeguards* into the processing in order to meet the requirements and protect the rights and freedoms of data subjects. Both appropriate measures and necessary safeguards are meant to serve the same purpose of protecting the rights of data subjects and ensuring that the protection of their personal data is built into the processing.
第 25 条 (1) に沿って、管理者は、本規則の要件に適合し、かつ、データ主体の権利及び自由を保護するため、その取扱いの中に、データ保護の基本原則を実装し、*必要な保護措置*を統合するように設計された、*適切な*技術的及び組織的*措置*を実装するものとする。適切な措置及び必要な保護措置はどちらも、データ主体の権利を保護すること、また、その個人データの保護がその取扱いの中に組み込まれるよう確保することという同じ目的を果たすことを目指している。

8. *Technical and organizational measures* and necessary safeguards can be understood in a broad sense as any method or means that a controller may employ in the processing. Being *appropriate* means that the measures and necessary safeguards should be suited to achieve the intended purpose, i.e. they must implement the data protection principles *effectively*[3]. The requirement to appropriateness is thus closely related to the requirement of effectiveness.
*技術的措置及び組織的措置*並びに必要な保護措置は、管理者がその取扱いの中で使用しうるあらゆる方法又は手段として、広い意味で解釈されることができる。*適切*であるとは、措置及び必要な保護措置が意図された目的を達成するのに適していること、つまり、データ保護の基本原則を*効果的に* [3] 実装しなければならないことを意味する。したがって、適切性の要件は実効性の要件と密接に関連している。

9. A technical or organisational measure and safeguard can be anything from the use of advanced technical solutions to the basic training of personnel. Examples that may be suitable, depending on the context and risks associated with the processing in question, includes pseudonymization of personal data[4]; storing personal data available in a structured, commonly machine readable format; enabling data subjects to intervene in the processing; providing information about the storage of personal data; having malware detection systems; training employees about basic “cyber hygiene”; establishing privacy and information security management systems, obligating processors contractually to implement specific data minimisation practices, etc.
技術的措置及び組織的措置並びに必要な保護措置には、高度な技術的ソリューションの使用から要員の基本的なトレーニングまで、あらゆるものが該当しうる。該当の取扱いに伴う過程及びリスクに応じて、適切となりうる例には、次のようなものが含まれる。個人データの仮名化 [4]、構造化された、一般的に機械読取り可能な形式で個人データを利用可能にし、保存すること、データ主体が取扱いに介在できるようにすること、個人データの記録保存に関する情報を提供すること、マルウェア検出システムを備えること、基本的な「サイバー衛生」について従業員を訓練すること、プライバシー及び情報セキュリティ管理システムを設けること、処理者に特定のデータ最小化の慣行を実装するよう契約上で義務付けること、など。

---

[3] “Effectiveness” is addressed below in subchapter 2.1.2.
「実効性（効果的）」については、以下の第 2.1.2 項において対応する。

[4] Defined in Article 4(5) GDPR.
GDPR 第 4 条(5)において定義されている。

10. Standards, best practices and codes of conduct that are recognized by associations and other bodies representing categories of controllers can be helpful in determining appropriate measures. However, the controller must verify the appropriateness of the measures for the particular processing in question.
様々な類型の管理者を代表する団体及びその他の組織によって認められている基準、ベスト・プラクティス、及び行動規範は、適切な措置を決定する際に役立ちうる。ただし、管理者は、該当の特定の取扱いについて、その措置の適切性を検証しなければならない。

2.1.2 Designed to implement the data protection principles in an effective manner and protecting data subjects' rights and freedoms
データ保護の基本原則を効果的な態様で実装し、データ主体の権利及び自由の保護を実装するよう設計された

11. The *data protection principles* are in Article 5 (henceforth "the principles"), the *data subjects' rights and freedoms* are the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data, whose protection is named in Article 1(2) as the objective of the GDPR (henceforth "the rights")[5]. Their precise formulation can be found in the EU Charter of Fundamental Rights. It is essential for the controller to have an understanding of the meaning of *the principles* and *the rights* as the basis for the protection offered by the GDPR, specifically by the DPbDD obligation.
*データ保護の基本原則*は第 5 条にあり（以下「基本原則」という）、データ主体の権利及び自由は、自然人の基本的な権利及び自由であり、特にその個人データの保護に対する権利である。その保護は、GDPR の目的として第 1 条 (2) に明示されている（以下「権利」という）[5]。その正確な記述は、欧州連合の基本権憲章にある。管理者は、GDPR、特に DPbDD の 義務により提供される保護の基礎となる、*基本原則*及び*権利*の意味について理解することが不可欠である。

12. When implementing the appropriate technical and organisational measures, it is with respect to the effective implementation of each of the aforementioned principles and the ensuing protection of rights that the measures and safeguards should be *designed*.
適切な技術的措置及び組織的措置を実装する際には、前述の基本原則のそれぞれについて効果的な実装をしていること及び権利の保護を確保していることという観点から、当該措置及び保護措置が*設計*されなければならない。

Addressing effectiveness
実効性（効果的）への対応

13. Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller. This observation has two consequences.
実効性は、データ保護バイデザインの概念の中心となる。基本原則を効果的な態様で実装するという要件は、データ主体の権利が確保されるには、管理者が、これらの基本原則を保護するために、必要な措置及び保護措置を実装しなければならないことを意味する。実装された各措置は、管理者が予見する取扱いにとって、意図された結果をもたらさなければならない。このことは、二つの結論を導く。

[5] See Recital 4 of the GDPR.
GDPR 前文第 4 項参照。

14. First, it means that Article 25 does not require the implementation of any specific technical and organizational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk[6]. Whether or not measures are effective will therefore depend on the context of the processing in question and an assessment of certain elements that should be taken into account when determining the means of processing. The aforementioned elements will be addressed below in subchapter 2.1.3.
第一に、このことは、第 25 条が特定の技術的措置及び組織的措置を実装するよう要求しているということを意味するのではなく、むしろ、該当の特定の取扱いの中にデータ保護の基本原則を実装するために、選ばれる措置及び保護措置が特定されなければならないということを意味する。その際、当該措置及び保護措置は、強固なものとなるように設計する必要があり、また管理者は、リスクの増加に対応するために追加的な措置を実装可能でなければならない [6]。したがって、措置が効果的かどうかは、該当の取扱いの過程及び取扱いの手段を決定する際に考慮に入れるべき特定の要素の評価次第である。これら要素については、以下の第 2.1.3 項で対応する。

15. Second, controllers should be able to demonstrate that the principles have been maintained.
第二に、管理者は、基本原則が継続的に維持されているということを証明できなければならない。

16. The implemented measures and safeguards should achieve the desired effect in terms of data protection, and the controller should have documentation of the implemented technical and organizational measures.[7] To do so, the controller may determine appropriate key performance indicators (KPI) to demonstrate the effectiveness. A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves their data protection objective. KPIs may be *quantitative*, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or *qualitative*, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.
実装された措置及び保護措置は、データ保護の観点から望ましい効果を達成する必要があり、また管理者は、実装された技術的措置及び組織的措置を文書化しておく必要がある。[7] そうするために、管理者は、実効性を証明する適切な重要業績評価指数 (KPI) を決定しうる。KPI は、管理者がデータ保護の目的をどの程度効果的に達成しているかを証明する、管理者によ

[6] "Fundamental principles applicable to the controllers (i.e. legitimacy, data minimisation, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable." Article 29 Working Party. "Statement on the role of a risk-based approach in data protection legal frameworks". WP 218, 30 May 2014, p. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf
「管理者に適用される基本の原則（つまり、正当性、データの最小化、目的の限定、透明性、データの完全性、データの正確性）は、データ主体にとって、その取扱い及びリスクがどのようなものであっても、同じでなければならない。一方、そのような取扱いの性質及び範囲を適切に考慮することは、これらは本質的に拡大可能なものであるため、これらの基本原則を適用する上で常に不可欠な部分である。」第 29 条 作業部会、「データ保護の法的枠組みにおけるリスクベースのアプローチの役割に関する声明」、WP 218、2014 年 5 月 30 日、3 ページ参照。
ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] See Recitals 74 and 78.
前文第 74 項及び第 78 項参照。

って選択される測定可能な値である。KPI には、偽陽性又は偽陰性の割合、苦情の減少、データ主体が権利を行使する際の回答時間の短縮など、*定量的*なもの、又は、パフォーマンスの評価、等級スケールの使用、専門家による評価などの*定性的*なものがありうる。KPI に代わるものとして、管理者は、自身が選択した措置及び保護措置の実効性の評価の背後にある理論的根拠を提供することで、基本原則の効果的な実装を証明できる場合がある。

2.1.3 Elements to take into account
考慮に入れる要素

17. Article 25 (1) lists elements that the controller has to take into account when determining the measures of a specific processing operation. In the following, we will provide guidance on how to apply these elements in the design process, which includes design of the default settings. These elements all contribute to determine whether a measure is appropriate to effectively implement the principles. Thus, each of these elements is not a goal in and of themselves, but are factors to be considered together to reach the objective.
第 25 条 (1) には、特定の取扱業務の措置を決定する際に、管理者が考慮しなければならない要素が列挙されている。以下では、デフォルト設定の設計を含む設計過程において、これらの要素を適用する方法についてのガイダンスを提供する。これらの要素は全て、基本原則を効果的に実装するために、措置が適切であるかどうかを判断するのに役立つ。したがって、これらの各要素はそれ自体が目的ではなく、目的を達成するために一緒に考慮されるべき要因である。

2.1.3.1 "state of the art"
「先端技術」

18. The concept of "state of the art" is present in various EU acquis, e.g. environmental protection and product safety. In the GDPR, reference to the "state of the art"[8] is made not only in Article 32, for security measures,[9] [10] but also in Article 25, thus extending this benchmark to all technical and organisational measures embedded in the processing.
「先端技術」の概念は、環境保護及び製品の安全性など、様々な EU の法令に存在する。GDPR では、「先端技術」[8] への言及は、安全管理措置 [9] [10] に関する第 32 条だけでなく、第 25 条においてもなされている。つまり、このベンチマークは、取扱いに組み込まれる全ての技術的措置及び組織的措置に及ぶということである。

---

[8] See German Federal Constitutional Court's "Kalkar" decision in 1978: https://germanlawarchive.iuscomp.org/?p=67 may provide the foundation for a methodology for an objective definition of the concept. On that basis, the "state of the art" technology level would be identified between the "existing scientific knowledge and research" technology level and the more established "generally accepted rules of technology". The "state of the art" can hence be identified as the technology level of a service or technology or product that exists in the market and is most effective in achieving the objectives identified.
1978 年のドイツ連邦憲法裁判所の「カルカー」判決を参照のこと。
https://germanlawarchive.iuscomp.org/?p=67 は、当該概念の客観的な定義のための方法論の基礎を提供しうる。それに基づき、「最先端」の技術レベルは、「現存の科学的知識及び研究」の技術レベルと、より確立された「一般的に認められた技術の法則」との間で特定されることになる。したがって、「先端技術」とは、市場に存在し、特定された目的を達成するのに最も効果的なサービス、技術、又は製品の技術水準としてみなされうる。

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security
https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security 参照。

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/
www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/参照。

19. In the context of Article 25, the reference to "state of the art" imposes an obligation on controllers, when determining the appropriate technical and organisational measures, **to take account of the current progress in technology** that is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that *secure effective implementation* of the principles and rights of data subjects taking into account the evolving technological landscape.
第 25 条の文脈において、「先端技術」への言及は、適切な技術的措置及び組織的措置を判断する際に、市場で入手可能な**最新の技術進歩を考慮に入れるよう、**管理者に対し義務を課すものである。当該要件は、技術の進歩について、具体的には、技術が取扱業務に対し、どのようなデータ保護のリスク又は機会をもたらしうるか、また、基本原則及びデータ主体の権利について*効果的な実装を確保するための*措置及び保護措置を、進化する技術的状況を考慮した上で、どのように実装し更新していくかについて、管理者が、知識を持ち、常に最新の情報を把握することである。

20. The "state of the art" is a dynamic concept that cannot be statically defined at a fixed point in time, but should be assessed *continuously* in the context of technological progress. In the face of technological advancements, a controller could find that a measure that once provided an adequate level of protection no longer does. Neglecting to keep up to date with technological changes could therefore result in a lack of compliance with Article 25.
「先端技術」は動的な概念であり、一定の時点で静的に定義することはできず、技術進歩の過程で*継続的に*評価していく必要がある。技術の進歩に直面して、管理者は、以前は適切なレベルの保護を提供していた措置が、もはや機能していないことに気付く可能性がある。したがって、技術的な変化の最新を維持することを怠ると、第 25 条に遵守していないという結果になる可能性がある。

21. The "state of the art" criterion does not only apply to technological measures, but also to organisational ones. Lack of appropriate organisational measures can lower or even completely undermine the effectiveness of a chosen technology. Examples of organisational measures can be adoption of internal policies; up-to date training on technology, security and data protection; and IT security governance and management policies.
「先端技術」の基準は技術的措置だけでなく、組織的措置にも適用される。適切な組織的措置が欠如していると、選択した技術の実効性が低下したり、完全に損なわれたりさえする可能性がある。組織的措置の例としては、内部方針の導入、技術、セキュリティ及びデータ保護に関する最新の訓練、並びに IT セキュリティガバナンス及び管理方針が挙げられる。

22. Existing and recognized frameworks, standards, certifications, codes of conduct, etc. in different fields may play a role in indicating the current "state of the art" within the given field of use. Where such standards exist and provide a high level of protection for the data subject in compliance with – or go beyond – legal requirements, controllers should take them into account in the design and implementation of data protection measures.
様々な分野における、現存の、認知された枠組み、基準、認証、行動規範などが、特定の使用分野における、現時点での「先端技術」を示す役割を果たしうる。このような基準等が存在し、データ主体に対し、法律上の要件を遵守した、又は法律上の要件を超えた、高い水準の保護を当該基準等が提供する場合、管理者は、データ保護措置の設計及び実装において、これらを考慮に入れなければならない。

2.1.3.2 "cost of implementation"
「実装費用」

23. The controller may take the cost of implementation into account when choosing and applying appropriate technical and organisational measures and necessary safeguards that effectively implement the principles in order to protect the rights of data subjects. The cost refers to resources in general, including time and human resources.
管理者は、データ主体の権利を保護するため、基本原則を効果的に実装する適切な技術的措置及び組織的措置並びに必要な保護措置を選択し適用する際、実装費用を考慮する場合がある。ここでの費用とは、時間及び人的資源を含む、リソース全般を指す。

24. The cost element does not require the controller to spend a disproportionate amount of resources when alternative, less resource demanding, yet effective measures exist. However, the cost of implementation is a factor to be considered to implement data protection by design rather than a ground to not implement it.
よりリソース要求が少ないが効果的である代替措置が存在する場合、費用面の要素は、管理者に対し、過大な量のリソースを費やすことを要求していない。一方、実装費用は、データ保護バイデザインを実装しない理由ではなく、データ保護バイデザインを実装するために考慮されるべき要因である。

25. Thus, the chosen measures shall ensure that the processing activity foreseen by the controller does not process personal data in violation of the principles, independent of cost. Controllers should be able to manage the overall costs to be able to effectively implement all of the principles and, consequentially, protect the rights.
したがって、選択された措置は、費用に関係なく、管理者が予見する取扱活動が基本原則に違反して個人データの取扱いをしないことを確保するものとする。管理者は、全ての基本原則を効果的に実装し、その結果、権利を保護できるように、全体的な費用を管理できなければならない。

2.1.3.3 "nature, scope, context and purpose of processing"
「取扱いの性質、範囲、過程及び目的」

26. Controllers must take into consideration the nature, scope, context and purpose of processing when determining needed measures.
管理者は、必要な措置を決定する際、取扱いの性質、範囲、過程及び目的を考慮しなければならない。

27. These factors should be interpreted consistently with their role in other provisions of the GDPR, such as Articles 24, 32 and 35, with the aim of designing data protection principles into the processing.
データ保護の基本原則を取扱いの中に設計することを目的としたこれらの要因は、第 24 条、第 32 条、第 35 条などの GDPR の他の条文における役割と一貫性があるように解釈されなければならない。

28. In short, the concept of **nature** can be understood as the inherent[11] characteristics of the processing. The **scope** refers to the size and range of the processing. The **context** relates to the circumstances of the processing, which may influence the expectations of the data subject, while the **purpose** pertains to the aims of the processing.

[11] Examples are special categories personal data, automatic decision-making, skewed power relations, unpredictable processing, difficulties for the data subject to exercise the rights, etc.
例としては、特別な種類の個人データ、自動的な意思決定、歪んだ力関係、予測不可能な取扱い、データ主体にとってのその権利の行使の困難性などが挙げられる。

つまり、**性質**という概念は、取扱いの本質的な[11]特性として解釈されうる。**範囲**とは、取扱いの規模及び範囲を指す。**過程**は、データ主体の期待に影響を与えうる、取扱いの状況に関連しており、**目的**は取扱いの目的に関連している。

2.1.3.4 "risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing"
「取扱いによって引き起こされる自然人の権利及び自由に対する様々な蓋然性と深刻度のリスク」

29. The GDPR adopts a coherent risk based approach in many of its provisions, in Articles 24, 25, 32 and 35, with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR. The assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights), taking into account the same conditions (nature, scope, context and purposes of processing).
GDPR は、個人、つまりその個人データを保護するための適切な技術的措置及び組織的措置を特定し、また GDPR の要件を遵守するという目的のために、その条項の多くに、つまり第 24 条、第 25 条、第 32 条及び第 35 条において、一貫性のあるリスクベースのアプローチを採用している。保護すべき資産（個人データの保護を通じて、個人）は常に同じであり、同じリスク（個人の権利にとってのリスク）に対して、同じ条件（性質、範囲、過程及び取扱いの目的）を考慮に入れている。

30. When performing the risk analysis for compliance with Articles 25, the controller has to identify the risks to the rights of data subjects that a violation of the principles presents, and determine their likelihood and severity in order to implement measures to effectively mitigate the identified risks. A systematic and thorough evaluation of the processing is crucial when doing risk assessments. For example, a controller assesses the particular risks associated with a lack of freely given consent, which constitutes a violation of the lawfulness principle, in the course of the processing of personal data of children and young people under 18 as a vulnerable group, in a case where no other legal ground exists, and implements appropriate measures to address and effectively mitigate the identified risks associated with this group of data subjects.
第 25 条を遵守するためのリスク分析を実行する際、管理者は、基本原則の違反がもたらすデータ主体の権利に対するリスクを特定し、その蓋然性及び深刻度を判断し、特定されたリスクを効果的に低減する措置を講じる必要がある。リスク評価を行う際には、取扱いの体系的かつ徹底的な評価が極めて重要である。例えば、管理者は、脆弱なグループとして 18 歳未満の子どもや青年の個人データを取扱う過程で、他の法的根拠が存在しない際に、適法性の原則の違反となる、自由に与えられた同意の欠如から生じる特定のリスクについて評価し、このグループのデータ主体に関連して特定されるリスクに対応し、それを効果的に低減するための適切な措置を講じる。

31. The "EDPB Guidelines on Data Protection Impact Assessment (DPIA)",[12] which focus on determining whether a processing operation is likely to result in a high risk to the data subject or not, also provide guidance on how to assess data protection risks and how to carry out a data protection risk assessment.

---

[12] Article 29 Working Party "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". WP 248 rev.01, 4 October 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 - endorsed by the EDPB.
第 29 条作業部会「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」、WP 248 rev.01、2017 年 10 月 4 日、ec.europa.eu/newsroom/document.cfm?doc_id=47711 、EDPB 承認版。

These Guidelines may also be useful during the risk assessment in all the articles mentioned above, including Article 25.
「データ保護影響評価(DPIA)に関する EDPB ガイドライン」[12] は、取扱業務がデータ主体に対し高いリスクを発生させるおそれがあるかどうかの判断に焦点を当てており、データ保護のリスクを評価する方法及びデータ保護のリスク評価を実施する方法に関するガイダンスも提供している。当該ガイドラインは、第 25 条を含む、上記の全ての条項におけるリスク評価の際にも役立ちうる。

32. The risk based approach does not exclude the use of baselines, best practices and standards. These might provide a useful toolbox for controllers to tackle similar risks in similar situations (nature, scope, context and purpose of processing). Nevertheless, the obligation in Article 25 (as well as Articles 24, 32 and 35(7)(c)) to take into account "*risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*" remains. Therefore, controllers, although supported by such tools, must always carry out a data protection risk assessment on a case by case basis for the processing activity at hand and verify the effectiveness of the appropriate measures and safeguards proposed. A DPIA, or an update to an existing DPIA, may then additionally be required.
リスクベースのアプローチは、ベースライン、ベストプラクティス、及び基準の使用を除外していない。これらは、管理者が、同様の状況（性質、範囲、過程及び取扱いの目的）において、同様のリスクに対応する際の有用な道具箱を提供する可能性がある。それでもなお、第 25 条（並びに第 24 条、第 32 条及び第 35 条(7)(c)）における *「取扱いによって引き起こされる自然人の権利及び自由に対する様々な蓋然性と深刻度のリスク」* を考慮する義務は残る。したがって、管理者は、そのような道具による支援があったとしても、常に、予定する取扱活動について、ケースごとにデータ保護のリスク評価を実施し、提案されている適切な措置及び保護措置の実効性を検証しなければならない。その際、DPIA、又は既存の DPIA の更新が、追加的に必要となるかもしれない。

2.1.4 Time aspect
時間的側面

2.1.4.1 At the time of the determination of the means for processing
取扱いの方法を決定する時点において

33. Data protection by design shall be implemented "*at the time of determination of the means for processing*".
データ保護バイデザインは、*「取扱いの方法を決定する時点において」* 実装されるものとする。

34. The "*means for processing*" range from the general to the detailed design elements of the processing, including the architecture, procedures, protocols, layout and appearance.
「取扱いの方法」 は、構成、手順、プロトコル、レイアウト、及び外観など、取扱いに関する一般的なものから詳細な設計要素まで多岐にわたる。

35. The *"time of determination of the means for processing*" refers to the period of time when the controller is deciding how the processing will be conducted and the manner in which the processing will occur and the mechanisms which will be used to conduct such processing. It's in the process of making such decisions that the controller must assess the appropriate measures and safeguards to effectively implement the principles and rights of data subjects into the processing, and take into account elements such as the state of the art, cost of implementation, nature, scope, context and purpose, and risks. This includes the time of procuring and implementing data processing software, hardware, and services.

*「取扱いの方法を決定する時点」*とは、管理者が、取扱いを実行する方法、並びに、取扱いが行われる際の態様及びそのような取扱いを実行するために使用される仕組みを決定している期間を指す。管理者が、その取扱いの中に基本原則及びデータ主体の権利を効果的に実装するための適切な措置及び保護措置を評価し、技術水準、実装費用、性質、範囲、過程、目的、及びリスクなどの要素を考慮しなければならないのは、このような決定をする工程においてである。これには、データ処理のソフトウェア、ハードウェア、及びサービスを調達し、実装する時間が含まれる。

36. Early consideration of DPbDD is crucial for a successful implementation of the principles and protection of the rights of the data subjects. Moreover, from a cost-benefit perspective, it is also in controllers' interest to take DPbDD into account sooner rather than later, as it could be challenging and costly to make later changes to plans that have already been made and processing operations that have already been designed.
DPbDD を早期に検討することは、基本原則及びデータ主体の権利の保護の実装を成功させるために極めて重要である。さらに、費用対効果の観点から、既に立案されている計画や既に設計されている取扱業務に対し、後に変更を加えるのは困難であり、かつ費用がかかる可能性があるため、DPbDD を早急に考慮しておくことは、管理者の利益にもなる。

2.1.4.2 At the time of the processing itself (maintenance and review of data protection requirements) 取扱中の時点（データ保護要件の維持及び見直し）

37. Once the processing has started the controller has a continued obligation to maintain DPbDD, i.e. the continued effective implementation of the principles in order to protect the rights, staying up to date on the state of the art, reassessing the level of risk, etc. The nature, scope and context of processing operations, as well as the risk may change over the course of processing, which means that the controller must re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards.
一旦取扱いが開始されると、管理者は DPbDD を維持するという継続的な義務を負う。具体的には、権利を保護するために基本原則の効果的な実装を継続的に維持すること、先端技術について最新を維持すること、リスクレベルを再評価することなどである。取扱業務の性質、範囲及び過程、並びにリスクは、取扱いの過程において変化しうる。このことは、管理者は、自身が選択した措置及び保護措置の実効性を定期的に見直し、評価することを通じて、自身の取扱業務を再評定しなければならないことを意味する。

38. The obligation to maintain, review and update, as necessary, the processing operation also applies to pre-existing systems. This means that legacy systems designed before the GDPR entered into force are required to undergo reviews and maintenance to ensure the implementation of measures and safeguards that implement the principles and rights of data subjects in an effective manner, as outlined in these Guidelines.
必要に応じて、取扱業務を維持管理し、見直し、また更新する義務は、既存のシステムに対しても適用される。このことは、このガイドラインで概説されているように、GDPR が発効する前に設計されたレガシー システムに対して、基本原則及びデータ主体の権利を効果的な態様で実装する措置及び保護措置の実装を確保するための見直し及び維持管理の実施が要求されることを意味する。

39. This obligation also extends to any processing carried out by means of data processors. Processors' operations should be regularly reviewed and assessed by the controllers to ensure that they enable continuous compliance with the principles and allow the data controller to fulfil its obligations in this respect.

この義務は、データ処理者によって実行されるあらゆる取扱いにも適用される。処理者の取扱いが基本原則を継続的に遵守していること、またデータ管理者がこの点においてその義務の履行ができていることを確保するために、処理者の業務は管理者により定期的に見直し、評価されなければならない。

2.2 Article 25(2): Data protection by default
第 25 条(2): データ保護バイデフォルト

2.2.1 By default, only personal data which are necessary for each specific purpose of the processing are processed
デフォルトで、その取扱いの個々の特定の目的のために必要な個人データのみが取り扱われること

40. A “default”, as commonly defined in computer science, refers to the pre-existing or preselected value of a configurable setting that is assigned to a software application, computer program or device. Such settings are also called “presets” or “factory presets”, especially for electronic devices.
コンピュータサイエンスにおいて一般的に定義されるように、「デフォルト」とは、ソフトウェアのアプリケーション、コンピュータプログラム、又はデバイスに割り当てられる、構成変更可能な設定の既存の値又は事前に選択された値を指す。このような設定は、特に電子機器では「プリセット」又は「ファクトリープリセット」とも呼ばれる。

41. Hence, the term “by default” when processing personal data, refers to making choices regarding configuration values or processing options that are set or prescribed in a processing system, such as a software application, service or device, or a manual processing procedure that affect the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
したがって、個人データを取り扱う際の「デフォルトで」という用語は、ソフトウェアのアプリケーション、サービス、若しくはデバイスなどの処理システム、又は手動の取扱いの手順において、設定若しくは規定される構成値又は取扱いオプションに関する選択を行うことを指す。これは、収集される個人データの分量、 その取扱いの範囲、その記録保存期間及びアクセス可能性に影響する。

42. The controller should choose and be accountable for implementing default processing settings and options in a way that only processing that is strictly necessary to achieve the set, lawful purpose is carried out by default. Here, controllers should rely on their assessment of the necessity of the processing with regards to the legal grounds of Article 6(1). This means that by default, the controller shall not collect more data than is necessary, they shall not process the data collected more than is necessary for their purposes, nor shall they store the data for longer than necessary. The basic requirement is that data protection is built into the processing by default.
管理者は、設定された適法な目的を達成するために厳密に必要な取扱いのみがデフォルトで実行されるように、デフォルトの取扱い設定及びオプションを選択し、実装する責任を負う。ここで、管理者は、第 6 条(1)の取扱いの法的根拠に関する取扱いの必要性についての自身の評価に頼らなければならない。このことは、デフォルトで管理者は、必要のあるもの以上のデータを収集しないこと、収集したデータをその目的にとって必要である以上に取扱いをしないこと、更に、必要な期間より長くデータを記録保存しないことを意味する。その基礎となる要件は、データ保護がデフォルトで取扱いに組み込まれていることである。

43. The controller is required to predetermine for which specified, explicit and legitimate purposes the personal data is collected and processed.[13] The measures must by default be appropriate to ensure that only personal data which are necessary for each specific purpose of processing are being processed. The EDPS "Guidelines to assess necessity and proportionality of measures that limit the right to data protection of personal data" can be useful also to decide which data is necessary to process in order to achieve a specific purpose.[14][15][16]
管理者は、個人データがどの特定され、明確であり、かつ、正当な目的のために収集され、取り扱われるのかを、事前に決定する必要がある。[13] その取扱いの個々の特定の目的のために必要な個人データのみが取扱われていることを確保するよう、そのための措置は、デフォルトで適切なものでなければならない。EDPS の「個人データのデータ保護に対する権利を制限する措置の必要性及び比例性を評価するためのガイドライン」は、特定の目的を達成するためにどのデータを取り扱う必要があるかを決定する際にも役立つ可能性がある。[14][15][16]

44. If the controller uses third party software or off-the-shelf software, the controller should carry out a risk assessment of the product and make sure that functions that do not have a legal basis or are not compatible with the intended purposes of processing are switched off.
管理者が第三者のソフトウェア又は市販のソフトウェアを使用する場合、管理者は、当該製品のリスク評価を実行し、法的根拠がない機能又は意図した取扱いの目的に適合しない機能が切断されていることを確認する必要がある。

45. The same considerations apply to organisational measures supporting processing operations. They should be designed to process, at the outset, only the minimum amount of personal data necessary for the specific operations. This should be particularly considered when allocating data access to staff with different roles and different access needs.
同じ考慮事項が、取扱業務を支援する組織的措置にも適用される。最初は、特定の業務に必要な最小限の個人データのみを取り扱うように設計しておく必要がある。異なる役割及び異なるアクセスの必要性を持つスタッフに対し、データのアクセスを割り当てる際、特にこのことを考慮する必要がある。

46. Appropriate "technical and organisational measures" in the context of data protection by default is thus understood in the same way as discussed above in subchapter 2.1.1, but applied specifically to implementing the principle of data minimisation.

---

[13] Art. 5(1)(b), (c), (d), (e) GDPR.
GDPR 第 5 条(1)(b)、(c)、(d)、(e)。

[14] EDPS. "Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection". 25 February 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf
EDPS、「データ保護に対する権利を制限する措置の必要性及び比例性を評価するためのガイドライン」、 2019 年 2 月 25 日。edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] See also EDPS. "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit" https://edps.europa.eu/data-protection/our-work/publications/papers/necessitytoolkit_en
EDPS、「個人データの保護に対する基本的権利を制限する措置の必要性の評価: ツールキット」 も参照。https://edps.europa.eu/data-protection/our-work/publications/papers/necessitytoolkit_en

[16] For more information on necessity, see Article 29 Working Party. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC". WP 217, 9 April 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
必要性の詳細については、第 29 条作業部会「指令 95/46/EC の第 7 条に基づくデータ管理者の正当な利益の概念に関する意見 06/2014」、WP 217、2014 年 4 月 9 日を参照のこと。ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

したがって、データ保護バイデフォルトとの関連における適切な「技術的措置及び組織的措置」は、上記の第 2.1.1 項で説明されているものと同じように理解されるが、特にデータの最小化の原則の実装に対し適用される。

47. The aforementioned obligation to only process personal data which are necessary for each specific purpose applies to the following elements.
個々の特定の目的のために必要な個人データのみが取扱われるという前述の義務は、以下の要素に適用される。

2.2.2 Dimensions of the data minimisation obligation
データの最小化の義務の範囲

48. Article 25 (2) lists the dimensions of the data minimisation obligation for default processing, by stating that the obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
第 25 条 (2) は、デフォルトでの取扱いにおけるデータの最小化の義務の範囲を列挙しており、この義務は、収集される個人データの分量、 その取扱いの範囲、その記録保存期間及びアクセス可能性に適用されると規定している。

2.2.2.1 "amount of personal data collected"
「収集される個人データの分量」

49. Controllers should consider both the volume of personal data, as well as the types, categories and level of detail of personal data required for the processing purposes. Their design choices should take into account the increased risks to the principles of integrity and confidentiality, data minimisation and storage limitation when collecting large amounts of detailed personal data, and compare it to the reduction in risks when collecting smaller amounts and/or less detailed information about data subjects. In any case, the default setting shall not include collection of personal data that is not necessary for the specific processing purpose. In other words, if certain categories of personal data are unnecessary or if detailed data isn't needed because less granular data is sufficient, then any surplus personal data shall not be collected.
管理者は、取扱いの目的のために必要な個人データの量、並びに個人データの種類、類型及び詳細レベルの両方を考慮する必要がある。その設計上の選択では、大量の詳細な個人データを収集する場合の完全性及び機密性、データの最小化、記録保存の制限の原則に対するリスクの増加度を考慮に入れ、それをデータ主体についてのより少量及び／又はより詳細ではない情報を収集する場合のリスクの軽減度と比較する必要がある。いかなる場合においても、デフォルト設定では、特定の取扱い目的にとって必要のない個人データの収集は含まれないものとする。言い換えれば、一定の種類の個人データが不要な場合、又はより少ない詳細度のデータで十分であり詳細なデータが必要ない場合は、超過する個人データは収集されない。

50. The same default requirements apply to services independent of what platform or device in use, only the necessary personal data for the given purpose can be collected.
どのようなプラットフォーム又はデバイスが使用されているかに関係なく、同じデフォルト要件がサービスに対し適用され、特定の目的のために必要な個人データのみを収集することができる。

2.2.2.2 "the extent of their processing"
「その取扱いの範囲」

51. Processing[17] operations performed on personal data shall be limited to what is necessary. Many processing operations may contribute to a processing purpose. Nevertheless, the fact that certain personal data is necessary to fulfil a purpose does not mean that all types of, and frequencies of, processing operations may be carried out on the data. Controllers should also be careful not to extend the boundaries of "compatible purposes" of Article 6(4), and have in mind what processing will be within the reasonable expectations of data subjects.
個人データに対して行われる取扱[17]業務は、必要な範囲のものに限定されるものとする。一つの取扱いの目的のために多くの取扱業務を実施しうる。一方、一定の個人データがある目的を達成するために必要であるという事実は、当該データを使用して、あらゆる種類、及び頻度の取扱業務を実行することが許されることを意味するものではない。管理者はまた、第6条(4)の「適合する目的」の範囲を拡大しないように注意し、どのような取扱いがデータ主体の合理的な期待の範囲内となるかについて留意する必要がある。

2.2.2.3 "the period of their storage"
「その記録保存期間」

52. Personal data collected shall not be stored if it is not necessary for the purpose of the processing and there is no other compatible purpose and legal ground according to Article 6(4). Any retention should be objectively justifiable as necessary by the data controller in accordance with the accountability principle.
収集された個人データは、取扱いの目的のために必要がなく、第6条(4)に基づく他の適合する目的及び法的根拠がない場合、記録保存されないものとする。いかなる保持も、アカウンタビリティの原則に従い、データ管理者が必要性について客観的に正当化できるものでなければならない。

53. The controller shall limit the retention period to what is necessary for the purpose. If personal data is no longer necessary for the purpose of the processing, then it shall by default be deleted or anonymized. The length of the period of retention will therefore depend on the purpose of the processing in question. This obligation is directly related to the principle of storage limitation in Article 5(1)(e), and shall be implemented by default, i.e. the controller should have systematic procedures for data deletion or anonymization embedded in the processing.
管理者は、保持期間を目的のために必要な期間に制限するものとする。個人データが該当の取扱いの目的にとって必要ではなくなる場合、当該個人データはデフォルトで消去又は匿名化されるものとする。したがって、保存期間の長さは、該当の取扱いの目的により異なる。この義務は、第5条(1)(e)の記録保存の制限の原則と直接関連しており、デフォルトで実装されるものとする。つまり、管理者は、データの消去又は匿名化のための体系的な手順を取扱いの中に組み込む必要がある。

[17] According to Art. 4(2) GDPR, this includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
GDPR 第4条(2)によると、これには、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外の方法で利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊が含まれる。

54. Anonymization[18] of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of reidentification, are regularly assessed.[19]
個人データの匿名化 [18] は、関連する全ての過程の要素が考慮され、再識別のリスクを含むリスクの蓋然性及び深刻度が定期的に評価されることを条件に、消去の代替手段となる。[19]

2.2.2.4 "their accessibility"
「アクセス可能性」

55. The controller should limit who has access and which types of access to personal data based on an assessment of necessity, and also make sure that personal data is in fact accessible to those who need it when necessary, for example in critical situations. Access controls should be observed for the whole data flow during the processing.
管理者は、必要性の評価に基づいて、個人データに対しアクセス権を持つ者及びアクセスの種類を制限しなければならない。また、必要な場合、例えば危機的状況の際に、個人データが実際にそれを必要とする者にアクセス可能であることを確認する必要もある。取扱いの間のデータフロー全体について、アクセス制御を遵守する必要がある。

56. Article 25(2) further states that personal data shall not be made accessible, without the individual's intervention, to an indefinite number of natural persons. The controller shall by default limit accessibility and give the data subject the possibility to intervene before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons.
第 25 条 (2)はさらに、個人 データが、その個人の関与なく、不特定の自然人からアクセス可能なものとされないと規定している。管理者は、デフォルトでアクセス可能性を制限し、データ主体に関する個人データを不特定の自然人に対し公開又はその他の方法で利用可能なものとする前に、データ主体に対し、介在する可能性を与えるものとする。

57. Making personal data available to an indefinite number of persons may result in even further dissemination of the data than initially intended. This is particularly relevant in the context of the Internet and search engines. This means that controllers should by default give data subjects an opportunity to intervene before personal data is made available on the open Internet. This is particularly important when it comes to children and vulnerable groups.
個人データを不特定の自然人に対し利用可能なものとすると、当初意図した以上にデータが拡散する結果となりうる。このことは、インターネット及び検索エンジンの場合において特に関連する。このことは、個人データがオープンなインターネット上で利用可能になる前に、管理者はデフォルトでデータ主体に対し、介在の機会を与える必要があることを意味する。このことは、子ども及び脆弱性のあるグループに関して、特に重要である。

---

[18] Article 29 Working Party. "Opinion 05/2014 on Anonymisation Techniques". WP 216, 10 April 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
第 29 条 作業部会、「匿名化技術に関する意見 05/2014」、WP216、2014 年 4 月 10 日。ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[19] Please see Art. 4(1) GDPR, Recital 26 GDPR, Article 29 Working Party "Opinion 05/2014 on Anonymisation Techniques". Please also see the subsection on "storage limitation" in section 3 of this document, referring to the need for the controller to ensure the effectiveness of the implemented anonymisation technique(s).
GDPR 第 4 条(1)、GDPR 前文第 26 項、第 29 条作業部会「匿名化技術に関する意見 05/2014」を参照のこと。また、管理者が実装された匿名化技術の実効性を確保する必要性について言及している、この文書の第 3 章内、「記録保存の制限」に関するサブセクション（第 3.7 節）も参照のこと。

58. Depending on the legal grounds for processing, the opportunity to intervene could vary based on the context of the processing. For example, to ask for consent to make the personal data publicly accessible, or to have privacy settings so that data subjects themselves can control public access.
取扱いの法的根拠により、介在の機会は、取扱いの過程に応じて変わる可能性がある。例えば、個人データを公共にアクセス可能とするために同意を求めること、データ主体が自身で公共のアクセスを制御できるようにプライバシー設定を設けること、など。

59. Even in the event that personal data is made available publicly with the permission and understanding of a data subject, it does not mean that any other controller with access to the personal data may freely process it themselves for their own purposes – they must have their own legal basis.[20]
データ主体の許可及び理解を得て個人データが公共に利用可能なものにされたとしても、当該個人データにアクセス可能な他の管理者が自らの目的のために、自由に当該データを取り扱いうることを意味するものではない。つまり、他の管理者は、自身の法的根拠を保持しなければならない。[20]

3 IMPLEMENTING DATA PROTECTION PRINCIPLES IN THE PROCESSING OF PERSONAL DATA USING DATA PROTECTION BY DESIGN AND BY DEFAULT
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を用いて個人データの取扱いの中にデータ保護の基本原則を実装する

60. In all stages of design of the processing activities, including procurement, tenders, outsourcing, development, support, maintenance, testing, storage, deletion, etc., the controller should take into account and consider the various elements of DPbDD which will be illustrated by examples in this chapter in the context of implementation of the principles.[21] [22] [23]
調達、入札、アウトソーシング、開発、サポート、保守、テスト、記録保存、消去などを含む取扱活動の設計の全ての段階において、管理者は、DPbDD の様々な要素を考慮に入れ、検討する必要がある。この章では、基本原則の実装という観点から、このことについて事例で説明する。[21] [22] [23]

61. Controllers need to implement the principles to achieve DPbDD. These principles include: transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. These principles are outlined in Article 5 and Recital 39 of the GDPR. To have a complete understanding of how to implement DPbDD, the importance of understanding the meaning of each of the principles is emphasised.

---

[20] See Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland no. 931/13.
Satakunnan Markkinapörssi Oy と Satamedia Oy 対 Finland 931/13 番のケース、参照。

[21] More examples can be found in Norwegian Data Protection Authority. "Software Development with Data Protection by Design and by Default". 28 November 2017.
www.datatilsynet.no/en/aboutprivacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729
ノルウェーデータ保護機関の次の文書に他の事例がある。「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を活用したソフトウェア開発」、2017 年 11 月 28 日。
www.datatilsynet.no/en/aboutprivacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers
https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers 参照。

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf
https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf 参照。

管理者は、DPbDD を達成するため、基本原則を実装する必要がある。基本原則には、透明性、適法性、公正性、目的の限定、データの最小化、正確性、記録保存の制限、完全性及び機密性、アカウンタビリティの原則が含まれる。これらの基本原則は、GDPR の第 5 条及び前文第 39 条に概説されている。DPbDD の実装方法を完全に理解するために、それぞれの基本原則の意味を理解する重要性を強調する。

62. When presenting examples of how to operationalize DPbDD we have made lists of **key DPbDD elements** for each of the principles. The examples, while highlighting the specific data protection principle in question, may overlap with other closely related principles as well. The EDPB underlines that the key elements and the examples presented hereunder are neither exhaustive nor binding, but are meant as guiding elements for each of the principles. Controllers need to assess how to guarantee compliance with the principles in the context of the concrete processing operation in question.
DPbDD を運用する方法の事例を提示する際に、EDPB は、各基本原則について**主要な DPbDD の要素**のリストを作成した。事例は、該当の特定のデータ保護の基本原則を強調している一方、密接に関連する他の基本原則とも重複しうる。EDPB は、以下に示す主要な要素及び事例は網羅的なものでも拘束力のあるものでもなく、各基本原則の指針となる要素を意図したものであることを強調する。管理者は、該当の具体的な取扱業務との関連において、基本原則の遵守を保証する方法を評価する必要がある。

63. While this section focuses on the implementation of the principles, the controller should also implement *appropriate* and *effective* ways to protect data subjects' rights, also according to Chapter III in the GDPR where this is not already mandated by the principles themselves.
この章は基本原則の実装について焦点を当てているが、管理者はまた、基本原則自体により義務化されていないが GDPR 第 3 章に従い、データ主体の権利を保護するための*適切かつ効果的な方法*も実装しなければならない。

64. The accountability principle is overarching: it requires the controller to be responsible choosing the necessary technical and organisational measures.
アカウンタビリティの原則は包括的に適用される。つまり、アカウンタビリティの原則は管理者に対し、必要な技術的措置及び組織的措置を選択する責任を要求しているのである。

3.1 Transparency[24]
透明性 [24]

65. The controller must be clear and open with the data subject about how they will collect, use and share personal data. Transparency is about enabling data subjects to understand, and if necessary, make use of their rights in Articles 15 to 22. The principle is embedded in Articles 12, 13, 14 and 34. Measures and safeguards put in place to support the principle of transparency should also support the implementation of these Articles.
管理者は、個人データをどのように収集、使用、共有するかについて、データ主体に対し、明確かつ開かれたものにしなければならない。透明性とは、データ主体が第 15 条から第 22 条までの自身の権利を理解し、必要に応じて利用できるようにすることである。この基本原則は、第 12 条、第 13 条、第 14 条、及び第 34 条に盛り込まれている。透明性の原則を支援

[24] Elaboration on how to understand the concept of transparency can be found in Article 29 Working Party. "Guidelines on transparency under Regulation 2016/679". WP 260 rev.01, 11 April 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 - endorsed by the EDPB
透明性の概念を理解する方法に関する詳細は、第 29 条作業部会、「規則 2016/679 に基づく透明性に関するガイドライン」、WP260 rev.01、2018 年 4 月 11 日にある。
ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 、EDPB 承認版。

するために設けられた措置及び保護措置はまた、これらの条文の実装も支援するものでなければならない。

66. Key design and default elements for the principle of transparency may include:
透明性の原則のための主要なデザイン及びデフォルトの要素には、以下が含まれうる。

- Clarity – Information shall be in clear and plain language, concise and intelligible.
明瞭さ – 情報は、明確かつ平易な文言で、簡潔で、理解しやすいものであること。

- Semantics – Communication should have a clear meaning to the audience in question.
意味論 – 連絡は、該当する聴衆にとって明確な意味を持つものでなければならない。

- Accessibility - Information shall be easily accessible for the data subject.
アクセス可能性– 情報は、データ主体にとって容易にアクセス可能であること。

- Contextual – Information should be provided at the relevant time and in the appropriate form.
過程に応じた – 情報は、適切なタイミングで、適切な形式で提供されなければならない。

- Relevance – Information should be relevant and applicable to the specific data subject.
関連性 – 情報は、特定のデータ主体に関連したものであり、当該データ主体にとって適用可能なものでなければならない。

- Universal design – Information shall be accessible to all data subjects, include use of machine readable languages to facilitate and automate readability and clarity.
ユニバーサルデザイン – 情報は、全てのデータ主体に対しアクセス可能なものであること。可読性及び明瞭性を促進し自動化するため、機械可読性の文言を使用することを含む。

- Comprehensible – Data subjects should have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.
理解可能な – データ主体が、自身の個人データの取扱いに関して何を期待できるかについて、公正に理解していなければならない。特にデータ主体が子供ども又はその他の脆弱性のあるグループの場合。

- Multi-channel – Information should be provided in different channels and media, not only the textual, to increase the probability for the information to effectively reach the data subject.
多様なチャネル – 情報がデータ主体に効果的に届く可能性を高めるために、情報は、テキストだけでなく、様々なチャネル及びメディアで提供されなければならない。

- Layered – The information should be layered in a manner that resolves the tension between completeness and understanding, while accounting for data subjects' reasonable expectations.
階層化 – データ主体の合理的な期待を考慮しながら、完全性と理解の間の緊張を解決するような方法で、情報を階層化しなければならない。

Example[25]
事例 [25]

A controller is designing a privacy policy on their website in order to comply with the requirements of transparency. The privacy policy should not contain a lengthy bulk of information that is difficult for the average data subject to penetrate and understand. It shall be written in clear and concise language and make it easy for the user of the website to understand how their personal data is processed. The controller therefore provides information in a layered manner, where the most important points are highlighted. More detailed information is made easily available. Drop-down menus and links to other pages are provided to further explain the various items, and concepts used in the policy. The controller also makes sure that the information is provided in a multi-channel manner, providing video clips to explain the most important points of the written information. Synergy between the various pages is vital to ensure that the layered approach does not heighten confusion, rather reduce it.
管理者は、透明性の要件を満たすために、自身の Web サイトに関するプライバシーポリシーを設計しているところである。プライバシーポリシーには、平均的なデータ主体が洞察し理解するのが困難であるような長々しい大量の情報を含めるべきではない。それは明確かつ簡潔な文言で書かれ、ウェブサイトのユーザーが自身の個人データがどのように取り扱われるかについて容易に理解できるようにする必要がある。したがって、管理者は、階層化した方法で情報を提供し、最も重要なポイントを強調表示する。より詳細な情報を、容易に利用可能にする。ドロップダウンのメニュー及び他のページへのリンクから、様々な項目及び当該ポリシーにおいて使用されている概念について、追加的な説明が提供される。また、管理者は、情報が多様なチャネルで提供されるよう確認し、書面での情報の最も重要な点を説明するビデオクリップを提供する。階層化のアプローチが混乱を増大させず、むしろ軽減させるよう確保するには、複数ページ間のシナジーが不可欠である。

The privacy policy should not be difficult for data subjects to access. The privacy policy is thus made available and visible on all web-pages of the site in question, so that the data subject is always only one click away from accessing the information. The information provided is also designed in accordance with the best practices and standards of universal design to make it accessible to all.
プライバシーポリシーは、データ主体にとってアクセスが困難なものであってはならない。したがって、データ主体が常に 1 回クリックするだけで情報にアクセスできるよう、プライバシーポリシーは、該当のサイトの全ての Web ページで利用可能かつ視認可能なものにする。提供される情報はまた、誰もがアクセス可能であるように、ユニバーサルデザインのベストプラクティス及び基準に従って設計される。

Moreover, necessary information should also be provided in the right context, at the appropriate time. Since the controller carries out many processing operations using the data collected on the website, a general privacy policy on the website alone is not sufficient for the controller to meet the requirements of transparency. The controller therefore designs an information flow, presenting the data subject with relevant information within the appropriate contexts using e.g. informational snippets or pop-ups. For example, when asking the data subject to enter personal data, the controller informs the data subject of how the personal data will be processed and why that personal data is necessary for the processing.
さらに、必要な情報は、適切なタイミングで、適切な形式で提供されなければならない。管理者は、Web サイト上で収集したデータを使用し多くの取扱業務を実行するため、当該 Web サイトに関する一般的なプライバシーポリシーだけでは、管理者が透明性の要件を満たすには十分ではない。したがって、管理者は、例えば、情報のスニペット又はポップアップを使

[25] The French Data Protection Authority has published several examples illustrating best practices in informing users as well as other transparency principles: https://design.cnil.fr/en/.
フランスのデータ保護機関は、ユーザーへの情報提供におけるベストプラクティス及びその他の透明性の原則を説明するいくつかの事例を公開している。 https://design.cnil.fr/en/参照。

用して、データ主体に適切な過程の中で関連の情報を提示する、情報フローを設計する。例えば、データ主体に対し個人データの入力を求める際、管理者は、当該個人データがどのように取り扱われるのか、また何故その個人データが取扱いに必要なのかについて、データ主体に通知する。

3.2 Lawfulness
適法性

67. The controller must identify a valid legal basis for the processing of personal data. Measures and safeguards should support the requirement to make sure that the whole processing lifecycle is in line with the relevant legal grounds of processing.
管理者は、個人データの取扱いに関する有効な法的根拠を特定しなければならない。措置及び保護措置は、取扱いのライフサイクル全体が取扱いに関連する法的根拠に沿ったものであることを確認するという要件を支援するものでなければならない。

68. Key design and default elements for lawfulness may include:
適法性のための主要なデザイン及びデフォルトの要素には、以下が含まれうる。

- Relevance – The correct legal basis shall be applied to the processing.
関連性 – 取扱いに対し、正しい法的根拠が適用されていること。

- Differentiation[26] – The legal basis used for each processing activity shall be differentiated.
差別化 [26] – 取扱活動ごとに使用される法的根拠が差別化されていること。

- Specified purpose – The appropriate legal basis must be clearly connected to the specific purpose of processing. [27]
特定の目的 – 適切な法的根拠は、取扱いの特定の目的と明確に関連付けられていなければならない。[27]

- Necessity– Processing must be necessary and unconditional for the purpose to be lawful.
必要性 – 目的が適法であるためには、取扱いが必要かつ無条件なものでなければならない。

- Autonomy – The data subject should be granted the highest degree of autonomy as possible with respect to control over personal data within the frames of the legal basis.
自主性 – データ主体には、法的根拠の枠内で、個人データの管理に関して可能な限り高い自主性が与えられなければならない。

---

[26] EDPB. "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects". Version 2.0, 8 October 2019.
edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-badopted_after_public_consultation_en.pdf
EDPB、「データ主体へのオンライン サービスの提供に関連した GDPR 第 6 条 (1) (b) に基づく個人データの取扱いに関するガイドライン 2/2019」、バージョン 2.0、2019 年 10 月 8 日。
edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-badopted_after_public_consultation_en.pdf

[27] See section on purpose limitation below.
以下の目的の限定に関するセクション（第 3.4 節）を参照。

- Gaining consent – consent must be freely given, specific, informed and unambiguous.[28] Particular consideration should be given to the capacity of children and young people to provide informed consent.
  同意の取得 – 同意は自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではないものでなければならない。[28] 子ども及び青年が説明を受けた上での同意を提供する場合、その能力に対し、特別な配慮がなされなければならない。

- Consent withdrawal – Where consent is the legal basis, the processing should facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, then the consent mechanism of the controller does not comply with the GDPR.[29]
  同意の撤回 – 同意が法的根拠である場合、その取扱いは、同意の撤回を容易にするものでなければならない。同意の撤回は、同意を与えるのと同程度、容易なものでなければならない。そうでない場合、その同意の仕組みは、 GDPR を遵守していない。[29]

- Balancing of interests – Where legitimate interests is the legal basis, the controller must carry out a weighted balancing of interest, giving particular consideration to the power imbalance, specifically children under the age of 18 and other vulnerable groups. There shall be measures and safeguards to mitigate the negative impact on the data subjects.
  利益の衡量 – 正当な利益が法的根拠である場合、管理者は、力関係の不均衡、特に 18 歳未満の子ども及びその他の脆弱性のあるグループに対し特別に配慮し、加重付けした利益の衡量を図らなければならない。データ主体に対する悪影響を低減するための措置及び安全措置が講じられること。

- Predetermination – The legal basis shall be established before the processing takes place.
  事前の決定 – 法的根拠は、取扱いが行われる前に確立されること。

- Cessation – If the legal basis ceases to apply, the processing shall cease accordingly.
  停止 – 法的根拠が適用されなくなった場合、取扱いをそれに応じて停止すること。

- Adjust – If there is a valid change of legal basis for the processing, the actual processing must be adjusted in accordance with the new legal basis.[30]
  調整 – 取扱いの法的根拠に有効な変更がある場合、実際の取扱いは、新しい法的根拠に従い調整されなければならない。[30]

---

[28] See Guidelines 05/2020 on consent under Regulation 2016/679. https://edpb.europa.eu/our-worktools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
規則 2016/679 に基づく同意に関するガイドライン 05/2020 参照。https://edpb.europa.eu/our-worktools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] See Guidelines 05/2020 on consent under Regulation 2016/679, p. 24. https://edpb.europa.eu/our-worktools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
規則 2016/679 に基づく同意に関するガイドライン 05/2020、24 ページ参照。https://edpb.europa.eu/our-worktools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] If the original legal basis is consent, see Guidelines 05/2020 on consent under Regulation 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-underregulation-2016679_en
当初の法的根拠が同意である場合、規則 2016/679 に基づく同意に関するガイドライン 05/2020 参照。https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-underregulation-2016679_en

- Allocation of responsibility – Whenever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject, and design the measures of the processing in accordance with this allocation.
  責任の割当て – 共同管理関係が想定される場合は常に、当事者は、データ主体に対するそれぞれの責任を、明確かつ透明性のある方法で割り当て、この割当てに従って取扱いの手段を設計しなければならない。

Example
事例
A bank plans to offer a service to improve efficiency in the management of loan applications. The idea behind the service is that the bank, by requesting permission from the customer, is able to retrieve data about the customer directly from the public tax authorities. This example does not consider processing of personal data from other sources.
ある銀行が、ローン申請管理のなかで、効率性を向上するサービスの提供を計画している。このサービスの背後にある考え方は、銀行が顧客から許可を求めることで、顧客に関するデータを税務当局から直接取得可能にするというものである。この例では、他の情報源からの個人データの取扱いについては考慮しない。

Obtaining personal data about the data subject's financial situation is necessary in order to take steps at the request of the data subject prior to entering into a loan contract.[31] However, gathering personal data directly from the tax administration is not considered necessary, because the customer is able to enter into a contract by providing the information from the tax administration him or herself. Although the bank may have a legitimate interest in acquiring the documentation from the tax authorities directly, for example to ensure efficiency in the loan processing, giving banks such direct access to the personal data of applicants presents a risks related to the use or potential misuse of access rights
ローンの契約締結の前に、データ主体の要求に対し手続を進めるためには、データ主体の財務状況に関する個人データを取得することが必須である。[31] 一方、顧客は自身で税務管理当局からの情報を提供することで契約を締結することができるため、税務管理当局から直接個人データを収集することは必須とは見なされない。銀行は、例えば、ローン手続きの効率性を確保するといった目的で、税務当局から直接書類を取得することについて、正当な利益を有しうる。一方で、銀行に対し、そのような申請者の個人データへの直接的なアクセス権を与えることは、当該アクセス権の利用又は潜在的な悪用に関連したリスクを伴う。

When implementing the principle of lawfulness, the controller realizes that in this context, they cannot use the "necessary for contract" basis for the part of the processing that involves gathering personal data directly from the tax authorities. The fact that this specific processing presents a risk of the data subject becoming less involved in the processing of their data is also a relevant factor in assessing the lawfulness of the processing itself. The bank concludes that this part of the processing has to rely on another legal basis of processing. In the particular Member State where the controller is located, there are national laws that permits the bank to gather information from the public tax authorities directly, where the data subject consents to this beforehand.
適法性の原則を実装する際、管理者は、この状況では、税務当局から直接個人データを収集することを含む取扱いの部分に「契約上の必要性」の根拠を使用できないことを認識する。この特定の取扱いが、データ主体による自身のデータの取扱いに対する関与をより少なくするというリスクをもたらす事実も、取扱いの適法性自体を評価する際の関連要因となる。銀行は、取扱いのこの部分は、取扱いの別の法的根拠に依存する必要があると結論付ける。管

[31] See Article 6(1)(b) GDPR.
GDPR 第 6 条(1)(b)参照。

理者が拠点を置く加盟国によっては、データ主体が事前にこのことに同意している場合、銀行が税務当局から直接情報を収集することを許可する国内法がある。

The bank therefore presents information about the processing on the online application platform in such a manner that makes it easy for data subjects to understand what processing is mandatory and what is optional. The processing options, by default, do not allow retrieval of data directly from other sources than the data subject herself, and the option for direct information retrieval is presented in a manner that does not deter the data subject from abstaining. Any consent given to collect data directly from other controllers is a temporary right of access to a specific set of information.
したがって、銀行は、データ主体がどの取扱いが必須で、どの取扱いが選択であるかを容易に理解できるような方法で、オンライン・アプリケーションのプラットフォーム上で取扱いに関する情報を提示する。取扱いの選択肢は、デフォルトで、データ主体自身以外の情報源から直接データを取得することを許可していない。また、他の情報源から直接的に情報を取得するための選択肢は、データ主体が選択しないことを妨げないような方法で提示されている。他の管理者から直接データを収集するために与えられた同意は、特定の一連の情報に対する、一時的なアクセスの権限である。

Any given consent is processed electronically in a documentable manner, and data subjects are presented with an easy way of controlling what they have consented to and to withdraw their consent. The controller has assessed these DPbDD requirements beforehand and includes all of these criteria in their requirements specification for the tender to procure the platform. The controller is aware that if they do not include the DPbDD requirements in the tender, it may either be too late or a very costly process to implement data protection afterwards.
データ主体が与えた同意は、文書化可能な態様で電子的に処理され、データ主体には、自身が同意した内容を管理し、また自身の同意を撤回するための容易な方法が提供される。管理者はこれらの DPbDD 要件を事前に評価し、プラットフォームを調達するための入札の要求仕様書にこれらの基準を全て含める。管理者は、DPbDD の要件を入札に盛り込まない場合、その後にデータ保護を実装するのに手遅れになるか、又は非常に費用のかかるプロセスになる可能性があることを認識している。

3.3 Fairness
公正性

69. Fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be subject to automated individual decision-making and non-discrimination of data subjects in such processes).
公正性は、包括的な原則であり、データ主体に対して不当に不利益を与えたり、違法に差別的であったり、予期しないものであったり、又は誤解を招くような方法で、個人データが取り扱われることがないよう、要求している。公正性の原則を実装する措置及び保護措置は、データ主体の権利及び自由、特に情報に対する権利（透明性）、介在する権利（アクセス、消去、データポータビリティ、訂正）、及び取扱いを制限する権利（自動化された取扱いに基づいた決定の対象とされない権利及びそのようなプロセスのなかでデータ主体が差別されないこと）も支援するものである。

70. Key design and default fairness elements may include:
公正性の主要なデザイン及びデフォルトの要素には、以下が含まれうる。

- Autonomy – Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing.
  自主性 – データ主体には、自身の個人データの利用の決定、並びにその使用又は取扱いの範囲及び条件についての決定に対し、可能な限り高い自主性が与えられなければならない。

- Interaction – Data subjects must be able to communicate and exercise their rights in respect of the personal data processed by the controller.
  双方向性 – データ主体は、管理者によって取り扱われる個人データに関して、自身の権利を連絡すること、またその権利を行使することが可能でなければならない。

- Expectation – Processing should correspond with data subjects' reasonable expectations.
  期待 – 取扱いは、データ主体の合理的な期待と一致するものでなければならない。

- Non-discrimination – The controller shall not unfairly discriminate against data subjects.
  非差別 – 管理者はデータ主体に対し、不公正な差別をしないこと。

- Non-exploitation – The controller should not exploit the needs or vulnerabilities of data subjects.
  悪用の禁止 – 管理者はデータ主体の事情又は脆弱性を悪用してはならない。

- Consumer choice – The controller should not "lock in" their users in an unfair manner. Whenever a service processing personal data is proprietary, it may create a lock-in to the service, which may not be fair, if it impairs the data subjects' possibility to exercise their right of data portability in accordance with Article 20.
  消費者の選択 – 管理者は、不公正な方法でユーザーの「囲い込み」をしてはならない。個人データを取り扱うサービスが独自のものであるとき、このことが当該独自サービスへの囲い込みを構成する可能性がある。データ主体にとって、第 20 条に従ったデータポータビリティの権利を行使する可能性が損なわれる場合、この行為は公正ではない。

- Power balance – Power balance should be a key objective of the controller-data subject relationship. Power imbalances should be avoided. When this is not possible, they should be recognised and accounted for with suitable countermeasures.
  力関係の均衡 – 力関係の均衡は、管理者とデータ主体の関係の主要な目標でなければならない。力関係の不均衡を避けなければならない。このことが可能ではない場合、適切な対策を講じたうえで、その力の不均衡について認識され、説明されなければならない。

- No risk transfer – Controllers should not transfer the risks of the enterprise to the data subjects.
  リスク移転の禁止 – 管理者は、自身の企業リスクをデータ主体に移転してはならない。

- No deception – Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.
  欺瞞の禁止 – データ取扱いの情報及び選択肢は、欺瞞的若しくは操作的な文言又は設計を避け、客観的かつ中立的な方法で提供されなければならない。

- Respect rights – The controller must respect the fundamental rights of data subjects and implement appropriate measures and safeguards and not impinge on those rights unless expressly justified by law.
  権利の尊重 – 管理者は、データ主体の基本的権利を尊重し、適切な措置及び保護措置を講じなければならず、また、法律によって明示的に正当化されない限り、これらの権利を侵害してはならない。

- Ethical – The controller should see the processing's wider impact on individuals' rights and dignity.
  倫理的 – 管理者は、自身の取扱いについて、個人の権利及び尊厳に及ぼす、より広範な影響を理解しておかなければならない。

- Truthful – The controller must make available information about how they process personal data, they should act as they declare they will and not mislead the data subjects.
  誠実 – 管理者は、個人データの取扱いの方法に関する情報を利用可能なものとしなければならず、宣言したとおりに行動し、データ主体を誤解させてはならない。

- Human intervention – The controller must incorporate *qualified* human intervention that is capable of uncovering biases that machines may create in accordance with the right to not be subject to automated individual decision making in Article 22.[32]
  人的介在 – 管理者は、第 22 条の自動化された取扱いに基づいた決定の対象とされない権利に従って、機械が生み出す可能性のあるバイアスを明らかにすることが可能な*適格*な人間の介在を組み込まなければならない。[32]

- Fair algorithms – Regularly assess whether algorithms are functioning in line with the purposes and adjust the algorithms to mitigate uncovered biases and ensure fairness in the processing. Data subjects should be informed about the functioning of the processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements.[33]
  公正なアルゴリズム – アルゴリズムが取扱いの目的に沿って機能しているかどうかを定期的に評価し、アルゴリズムを調整して、明らかになったバイアスを低減し、取扱いの公正性を確保すること。データ主体は、業務遂行能力、経済状態、健康、個人的な嗜好、信頼性又は行動、位置又は移動など、自身について分析又は予測を行うアルゴリズムに基づく個人データの取扱いの機能について知らされなければならない。[33]

Example 1
事例 1
A controller operates a search engine that processes mostly user-generated personal data. The controller benefits from having large amounts of personal data and being able to use that personal data for targeted advertisements. The controller therefore wishes to influence data subjects to allow more extensive collection and use of their personal data. Consent is to be collected by presenting processing options to the data subject.

[32] See Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826
規則 2016/679 の目的のための自動化された個人に対する意思決定とプロファイリングに関するガイドライン参照。
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] See Recital 71 GDPR.
GDPR 前文第 71 項参照。

管理者は、主にユーザーにより生成される個人データを取り扱う検索エンジンを運営している。管理者は、大量の個人データを保有し、その個人データをターゲット広告に使用できることにより利益を得る。したがって、管理者は、個人データのより広範な収集及び使用を許可するよう、データ主体に対し影響を与えたい。同意は、データ主体に対し、取扱いの選択肢を提示することにより収集される予定である。

When implementing the fairness principle, taking into account the nature, scope, context and purpose of the processing, the controller realizes that they cannot present the options in a way that nudges the data subject in the direction of allowing the controller to collect more personal data than if the options were presented in an equal and neutral way. This means that they cannot present the processing options in such a manner that makes it difficult for data subjects to abstain from sharing their data, or make it difficult for the data subjects to adjust their privacy settings and limit the processing. These are examples of dark patterns, which are contrary to the spirit of Article 25. The default options for the processing should not be invasive, and the choice for further processing should be presented in a manner that does not pressure the data subject to give consent. Therefore, the controller presents the options to consent or abstain as two equally visible choices, accurately representing the ramifications of each choice to the data subject.

取扱いの性質、範囲、過程及び目的を考慮し、公正性の原則を実装する際、平等かつ中立的な方法で選択肢を提示する場合に比べ、より多くの個人データを収集することを管理者に許可する方向にデータ主体を誘導するような方法で選択肢を提示することはできない旨、管理者は認識する。このことは、管理者は、データ主体がデータの共有をしない選択をするのが困難であったり、又はデータ主体がプライバシー設定を調整して取扱いを制限するのが困難であるような態様で取扱いの選択肢を提示できないことを意味する。これらはダークパターンの例であり、第 25 条の精神に反する。デフォルトでの取扱いの選択肢は侵襲的であってはならず、また追加的な取扱いの選択肢は、データ主体に対し、同意を与えるよう圧力を掛けない方法で提示されなければならない。したがって、管理者は、同意又は同意しない選択肢について、データ主体に対し各選択の影響を正確に伝え、二つの等しく視認できる選択肢として提示する。

Example 2

事例 2

Another controller processes personal data for the provision of a streaming service where users may choose between a regular subscription of standard quality and a premium subscription with higher quality. As part of the premium subscription, subscribers get prioritized customer service.

別の管理者は、ストリーミングサービスを提供するために個人データを取り扱う。当該サービスでは、ユーザーは標準品質の通常購読と、より高品質のプレミアム購読のいずれかを選択しうる。プレミアム購読の一環として、加入者は、優先的なカスタマー サービスを受ける。

With regard to the fairness principle, the prioritized customer service granted to premium subscribers cannot discriminate the regular subscribers' access to exercise their rights according to the GDPR Article 12. This means that although the premium subscribers get prioritized service, such prioritization cannot result in a lack of appropriate measures to respond to request from regular subscribers without undue delay and in any event within one month of receipt of the requests.

公正性の原則に関して、プレミアム加入者に付与される優先的なカスタマーサービスは、GDPR 第 12 条に従った通常加入者によるアクセスの権利の行使を差別することはできない。このことは、プレミアム加入者は優先的なサービスを受けるものの、そのような優先付けにより、通常加入者からの要求に、不当な遅滞なく、いかなる場合も要求を受けてから 1 か月以内に応じるための、適切な措置が欠如する結果となってはならないことを意味する。

Prioritized customers may pay to get better service, but all data subjects shall have equal and indiscriminate access to enforce their rights and freedoms as required under Article 12.
プレミアム加入者は、より良いサービスを受けるために料金を支払うかもしれないが、全てのデータ主体は、第 12 条で要求されているように、自身の権利及び自由を行使するための、平等かつ無差別なアクセスの権利をもつ。

3.4 Purpose Limitation[34]
目的の限定 [34]

71. The controller must collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which they were collected.[35] The design of the processing should therefore be shaped by what is necessary to achieve the purposes. If any further processing is to take place, the controller must first make sure that this processing has purposes compatible with the original ones and design such processing accordingly. Whether a new purpose is compatible or not, shall be assessed according to the criteria in Article 6(4).
管理者は、データを特定され、明確であり、かつ、正当な目的のために収集するものとし、かつ、収集された目的に適合しない態様でその追加的取扱いをしてはならない。[35] したがって、取扱いの目的を達成するために何が必要かにより、取扱いの設計が決まる。追加的な取扱いが行われる予定の場合、管理者はまず、当該取扱いが当初の目的と適合する目的を持っていることを確認し、それに応じてそのような取扱いを設計しなければならない。新たな目的が適合するかどうかは、第 6 条(4)の基準に従って評価されるものとする。

72. Key design and default purpose limitation elements may include:
目的の限定の主要なデザイン及びデフォルトの要素には、以下が含まれうる。

- Predetermination – The legitimate purposes shall be determined before the design of the processing.
  事前の決定 – 正当な目的は、取扱いの設計が行われる前に決定されること。

- Specificity – The purposes shall be specified and explicit as to why personal data is being processed.
  特定性 – 個人データが取り扱われる理由について、目的が特定され、明確であること。

- Purpose orientation – The purpose of processing should guide the design of the processing and set processing boundaries.
  目的指向 – 取扱いの目的は、取扱いの設計の指針となり、取扱いの境界を設定するものでなければならない。

---

[34] The Article 29 Working Party provided guidance for the understanding of the principle of purpose limitation under Directive 95/46/EC. Although the Opinion is not adopted by the EDBP, it may still be relevant as the wording of the principle is the same under the GDPR.
Article 29 Working Party. "Opinion 03/2013 on purpose limitation". WP 203, 2 April 2013.
ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf
第 29 条作業部会は、指令 95/46/EC に基づく目的の限定の原則を理解するためのガイダンスを提供した。この意見書は EDBP により採択されていないが、当該原則の文言は GDPR の下でも同じであるため、GDPR においても関連しうる。
第 29 条 作業部会、「目的の限定に関する意見 03/2013」、WP 203、2013 年 4 月 2 日。
ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf

[35] Art. 5(1)(b) GDPR.
GDPR 第 5 条(1)(b)。

- Necessity – The purpose determines what personal data is necessary for the processing.
  必要性 – 目的により、どのような個人データがその取扱いにとって必要であるかについて判断される。

- Compatibility – Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.
  適合性 – 新たな目的は、データが収集された当初の目的に適合し、関連する設計の変更の指針となるものでなければならない。

- Limit further processing – The controller should not connect datasets or perform any further processing for new incompatible purposes.
  追加的な取扱いの制限 – 管理者は、適合しない新たな目的のために、データに接続し、又は追加的な取扱いを実行してはならない。

- Limitations of reuse – The controller should use technical measures, including hashing and encryption, to limit the possibility of repurposing personal data. The controller should also have organisational measures, such as policies and contractual obligations, which limit reuse of personal data.
  再利用の制限 – 管理者は、ハッシュ化及び暗号化などの技術的措置を使用し、個人データの再利用の可能性を制限しなければならない。管理者はまた、個人データの再利用を制限する方針及び契約上の義務など、組織的措置を講じなければならない。

- Review – The controller should regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.
  見直し – 管理者は、データが収集された目的にとって、その取扱いが必要なものであるか定期的に見直し、目的の限定に照らして設計をテストしなければならない。

Example
事例

The controller processes personal data about its customers. The purpose of the processing is to fulfil a contract, i.e. to be able to deliver goods to the correct address and obtain payment. The personal data stored is the purchase history, name, address, e-mail address and telephone number.
管理者は、自身の顧客に関する個人データを取り扱う。取扱いの目的は、契約を履行すること、つまり、商品を正しい住所に配送し、支払いを受け取ることができるようにすることである。記録保存される個人情報は、購入履歴、氏名、住所、電子メールアドレス及び電話番号である。

The controller is considering buying a Customer Relationship Management (CRM) product that gathers all the customer data about sales, marketing and customer service in one place. The product gives the opportunity of storing all phone calls, activities, documents, emails and marketing campaigns to get a 360-degree view of the customer. Moreover, the CRM is capable of automatically analysing the customers' purchasing power by using public information. The purpose of the analysis is to better target advertising activities. Those activities do not form part of the original lawful purpose of the processing.
同管理者は、販売、マーケティング、顧客サービスに関する全ての顧客データを 1 か所に収集する顧客管理システム(CRM)製品の購入を検討している。この製品は、顧客を 360 度把握するために、全ての入電、活動、文書、電子メール、マーケティング・キャンペーンを保存する機会を提供するものである。さらに、この CRM は、公開情報を使用して顧客の購買力を自動的に分析することができる。この分析の目的は、広告活動のターゲットを絞り込むことである。これらの活動は、当初の取扱いの目的の適法性の一部を形成するものではない。

To be in line with the principle of purpose limitation, the controller requires the provider of the product to map the different processing activities that use personal data to the purposes relevant for the controller.
目的の限定の原則に沿うべく、管理者は、当該製品のプロバイダーに対し、個人データを使用する様々な取扱活動を自身にとって関連する目的に対応付けるよう要求する。

After receiving the results of the mapping, the controller assesses whether the new marketing purpose and the targeted advertisement purpose are compatible with the original purposes defined when the data was collected, and whether there is a sufficient legal basis for the respective processing. If the assessment does not return a positive answer, the controller shall not proceed to use the respective functionalities. Alternatively, the controller could choose to forego the assessment and simply not make use of the described functionalities of the product.
当該対応付けの結果を受け取った後、管理者は、新しいマーケティング目的及びターゲットを絞った広告目的が、データの収集時に定義された当初の目的と適合するかどうか、またそれぞれの取扱いについて、十分な法的根拠があるかどうかについて評価する。当該評価で肯定的な回答が得られない場合、管理者は、それぞれの機能の使用を続行しないこととする。あるいは、管理者は評価をせず、単に前述の製品の機能を利用しないという選択をすることも可能である。

3.5 Data Minimisation
データの最小化

73. Only personal data that is adequate, relevant and limited to what is **necessary** for the purpose shall be processed.[36] As a result, the controller has to predetermine which features and parameters of processing systems and their supporting functions are permissible. Data minimisation substantiates and operationalises the principle of necessity. In the further processing, the controller should periodically consider whether processed personal data is still adequate, relevant and necessary, or if the data shall be deleted or anonymized.
その個人データが取扱われる目的にとって、十分であり、関連性があり、かつ、**必要**のあるものに限定された個人データに限り取り扱われるものとする。[36] その結果、管理者は、処理システム及びそのサポート機能のどの機能及びパラメータが許容されるかを事前に決定しなければならない。データの最小化は、必要性の原則を具体化し、運用するものである。追加的な取扱いにおいて、管理者は、取り扱われた個人データが依然として適切であり、関連性があり、かつ、必要のあるものであるかどうか、又はデータを消去又は匿名化するかどうかについて、定期的に検討しなければならない。

74. Controllers should first of all determine whether they even need to process personal data for their relevant purposes. The controller should verify whether the relevant purposes can be achieved by processing less personal data, or having less detailed or aggregated personal data or without having to process personal data at all[37]. Such verification should take place before any processing takes place, but could also be carried out at any point during the processing lifecycle. This is also consistent with Article 11.

[36] Art. 5(1)(c) GDPR.
GDPR 第 5 条(1)(c)。
[37] Recital 39 GDPR so states: "...Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means."
GDPR 前文第 39 項は、次のように規定している。「(略) 個人データは、その取扱いの目的が他の手段によっては合理的に満たされない場合においてのみ、取扱われるものとしなければならない。」

管理者は、まず第一に、関連する目的のために個人データを取り扱う必要自体あるかどうかを判断しなければならない。管理者は、より少ない個人データを取り扱うことにより、又は、詳細度合いをより少なくした若しくは集約した個人データを使用することにより、若しくは個人データを全く取り扱う必要なく、関連する目的を達成することが可能かどうかを検証する必要がある [37]。このような検証は、取扱いが行われる前に実行しなければならないが、取扱いのライフサイクルのどの時点においても実行可能であろう。このことはまた、第 11 条とも一貫性のあるものである。

75. Minimising can also refer to the degree of identification. If the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g. before data aggregation), then the controller shall delete or anonymize personal data as soon as identification is no longer needed. Or, if continued identification is needed for other processing activities, personal data should be pseudonymized to mitigate risks for the data subjects' rights.
最小化することは、識別の程度を指すこともある。取扱いの目的が、（統計など）最終的なデータセットにおいて特定の又は特定可能な個人が参照されることを要求しないが、（データ集計の前など）最初の取扱いで個人が参照されることを要求する場合、管理者は、識別が不要となり次第、個人データを消去又は匿名化するものとする。あるいは、他の取扱活動のために継続的な識別が必要な場合、データ主体の権利にとってのリスクを低減するために、個人データを仮名化しなければならない。

76. Key design and default data minimisation elements may include:
データの最小化の主要なデザイン及びデフォルトの要素には、以下が含まれうる。

- Data avoidance – Avoid processing personal data altogether when this is possible for the relevant purpose.
データの回避 – 関連する目的にとってこのことが可能な場合、個人データの取扱いを完全に回避すること。

- Limitation – Limit the amount of personal data collected to what is necessary for the purpose.
制限 – 収集される個人データの量は、取扱いの目的のために必要な範囲に限定すること。

- Access limitation – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.
アクセスの制限 – 職務を遂行するために個人データへのアクセスを必要とする人数が最小限となるようにデータの取扱いを形成し、それに応じてアクセスを制限すること。

- Relevance – Personal data should be relevant to the processing in question, and the controller should be able to demonstrate this relevance.
関連性 – 個人データは該当の取扱いに関連していなければならず、また管理者は、この関連性を証明可能でなければならない。

- Necessity – Each personal data category shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means.
必要性 – それぞれの個人データの種類は、特定の目的にとって必要であり、かつ他の手段によっては当該目的を達成できない場合においてのみ、取扱われるものとしなければならない。

- Aggregation – Use aggregated data when possible.

集約 – 可能な場合、集約したデータを使用すること。

- Pseudonymization – Pseudonymize personal data as soon as it is no longer necessary to have directly identifiable personal data, and store identification keys separately.
  仮名化 – 直接識別可能な個人データを持つ必要がなくなり次第、個人データを仮名化し、識別キーは分けて記録保存すること。

- Anonymization and deletion – Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted.
  匿名化及び消去 – 個人データが目的のために不要な場合、又は必要ではなくなった場合、個人データを匿名化又は消去すること。

- Data flow – The data flow should be made efficient enough to not create more copies than necessary.
  データフロー – 必要以上の複製を作成しないよう、データフローを十分に効率化すること。

- "State of the art" – The controller should apply up to date and appropriate technologies for data avoidance and minimisation.
  「先端技術」 – 管理者は、データの回避及び最小化のために、最新かつ適切な技術を適用しなければならない。

Example 1
事例 1
A bookshop wants to add to their revenue by selling their books online. The bookshop owner wants to set up a standardised form for the ordering process. To ensure customers fill out all the wanted information the bookshop owner makes all of the fields in the form mandatory (if you don't fill out all the fields the customer can't place the order). The webshop owner initially uses a standard contact form, which asks information including the customer's date of birth, phone number and home address. However, not all the fields in the form are necessary for the purpose of buying and delivering the books. In this particular case, if the data subject pays for the product up front, the data subject's date of birth and phone number are not necessary for the purchase of the product. This means that these cannot be required fields in the web form to order the product, unless the controller can clearly demonstrate that it is otherwise necessary, and why the fields are necessary. Moreover, there are situations where an address will not be necessary. For example, when ordering an eBook the customer can download the product directly to their device.
ある書店は、書籍をオンラインで販売することにより、収益を増やしたい。書店のオーナーは、このための注文プロセス用に、標準フォームを設定したい。書店のオーナーは、自身が欲しい全ての情報を顧客が入力するよう確保すべく、当該フォームの全てのフィールドを必須入力項目にする（全てのフィールドに入力しない場合、顧客は注文できない)。ウェブショップのオーナーは、最初、標準的な問合わせフォームを使用し、顧客の生年月日、電話番号及び自宅の住所などの情報を求める。一方、書籍を購入し、配送する目的にとって、当該フォームの全てのフィールドの情報が必要なわけではない。この特定のケースでは、データ主体が商品の代金を前払いする場合、データ主体の生年月日及び電話番号は、当該商品の購入のために必要ではない。このことは、それが別途必要であるということ及び当該フィールドが必要な理由を明確に証明できない限り、管理者は、商品を注文するための Web フォームにおいてこれらの項目を必須入力フィールドにできないことを意味する。更に、住所が必要とならない場合もある。例えば、電子書籍を注文する場合、顧客は商品を自身のデバイスに直接ダウンロードすることが可能である。

The webshop owner therefore decides to make two web forms: one for ordering books, with a field for the customer's address and one web form for ordering eBooks without a field for the customer's address.
したがって、ウェブショップのオーナーは、二種類の Web フォームを作成することを決定する。一つは顧客の住所のフィールドがある書籍注文用で、もう一つは顧客の住所のフィールドがない電子書籍の注文用の Web フォームである。

Example 2
事例 2
A public transportation company wishes to gather statistical information based on travellers' routes. This is useful for the purposes of making proper choices on changes in public transport schedules and proper routings of the trains. The passengers have to pass their ticket through a reader every time they enter or exit a means of transport. Having carried out a risk assessment related to the rights and freedoms of passengers' regarding the collection of passengers' travel routes, the controller establishes that it is possible to identify the passengers in circumstances where they live or work in scarcely populated areas, based on single route identification thanks to the ticket identifier. Therefore, since it is not necessary for the purpose of optimizing the public transport schedules and routings of the trains, the controller does not store the ticket identifier. Once the trip is over, the controller only stores the individual travel routes so as to not be able to identify trips connected to a single ticket, but only retains information about separate travel routes.
ある公共交通機関は、旅行者の経路を基にした統計情報を収集することを希望している。これは、公共交通機関のスケジュール変更及び列車の適切な経路変更について、適切な選択をするという目的にとって有用である。乗客は、交通手段に出入りする度に、自身のチケットを読取り機に通す必要がある。乗客の旅行経路の収集に関して、乗客の権利及び自由に関連するリスク評価を実施した結果、管理者は、乗客のチケットの識別子により、単一経路の識別を基に、乗客が人口の少ない地域に居住又は勤務している状況において、その乗客を特定することが可能であることを立証する。乗客の特定は公共交通機関のスケジュール及び列車経路を最適化する目的には必要ないため、結果、管理者は、乗客のチケットの識別子を記録保存しない。移動が終了する時点で、管理者は、個々の旅行経路のみを記録保存し単一のチケットに関連付けられた移動を識別できないようにするが、旅行経路別に関する情報に限り保持する。

In cases where there can still be a risk of identifying a person solely by their public transportation travel route the controller implements statistical measures to reduce the risk, such as cutting the beginning and the end of the route.
乗客の公共交通機関の旅行経路だけで個人が特定されるリスクが依然として存在する可能性がある場合、管理者は、経路の始点と終点をカットするなど、リスクを低減するための統計的措置を講じる。

Example 3
事例 3
A courier aims at assessing the effectiveness of its deliveries in terms of delivery times, workload scheduling and fuel consumption. In order to reach this goal, the courier has to process a number of personal data relating to both employees (drivers) and customers (addresses, items to be delivered, etc.). This processing operation entails risks of both monitoring employees, which requires specific legal safeguards, and tracking customers' habits through the knowledge of the delivered items over time. These risks can be significantly reduced with appropriate pseudonymization of employees and customers. In particular if pseudonymization keys are frequently rotated and macro areas are considered instead of detailed addresses, an effective data minimisation is pursued, and the controller

can solely focus on the delivery process and on the purpose of resource optimization, without crossing the threshold of monitoring individuals' (customers' or employees') behaviours.
ある宅配業者は、配達時間、作業量のスケジュール及び燃料消費量の観点から、配達の効率性について評価したい。この目的を達成するために、宅配業者は、従業員（ドライバー）及び顧客（住所、配達する商品など）の両方に関連する多数の個人データを取り扱う必要がある。この取扱業務には、特定の法的な保護措置が要求される従業員の監視、及び一定期間の配送物の情報の蓄積を通じた顧客の習慣の追跡という、両方のリスクが伴う。これらのリスクは、従業員及び顧客について、適切に匿名化することで大幅に軽減可能である。特に、仮名化の鍵が頻繁に交替され、詳細な住所ではなくマクロ領域が考慮される場合、効果的なデータの最小化が追求され、管理者は、個人（顧客又は従業員）の行動を監視するという閾値を超えることなく、配達手順及びリソースの最適化の目的にのみ集中することが可能となる。

Example 4
事例 4
A hospital is collecting data about its patients in a hospital information system (electronic health record). Hospital staff needs to access patient files to inform their decisions regarding care for and treatment of the patients, and for the documentation of all diagnostic, care and treatment actions taken. By default, access is granted to only those members of the medical staff who are assigned to the treatment of the respective patient in the speciality department she or he is assigned to. The group of people with access to a patient's file is enlarged if other departments or diagnostic units are involved in the treatment. After the patient is discharged, and billing is completed, access is reduced to a small group of employees per speciality department who answer requests for medical information or a consultation made or asked for by other medical service providers upon authorization by the respective patient.
ある病院は、患者に関するデータを病院情報システム（電子医療記録）に収集している。 病院のスタッフは、患者のケアと治療に関する決定を通知するため、また行われた全ての診断、ケア、治療行為を文書化するために、患者のファイルにアクセスする必要がある。デフォルトで、アクセスは、専門部門において割り当てられた各患者の治療を担当する医療スタッフのメンバーに限定して、許可されている。他の部門又は診断部門が治療に関与する場合、患者のファイルにアクセスする人々のグループは拡大する。患者が退院し、請求が完了すると、アクセスは専門部門ごとの少人数のスタッフに減らされる。当該スタッフは、各患者の許可に基づいて、他の医療サービス提供者からなされる若しくは求められる医療情報又は相談の要求に応じる。

3.6 Accuracy
正確性

77. Personal data shall be accurate and kept up to date, and every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[38]
個人データは、正確であり、かつ最新の状態に維持されなければならない。また、その個人データが取扱われる目的を考慮した上で、遅滞なく、不正確な個人データが消去又は訂正されることを確保するための全ての手立てが講じられなければならない。[38]

[38] Art. 5(1)(d) GDPR.
GDPR 第 5 条(1)(d)。

78. The requirements should be seen in relation to the risks and consequences of the concrete use of data. Inaccurate personal data could be a risk to the data subjects' rights and freedoms, for example when leading to a faulty diagnosis or wrongful treatment of a health protocol, or an incorrect image of a person can lead to decisions being made on the wrong basis either manually, using automated decision-making, or through artificial intelligence.
当該要件は、データの具体的な使用によるリスク及び結果との関連で捉えられなければならない。不正確な個人データは、データ主体の権利及び自由に対するリスクとなる可能性がある。例えば、誤った診断又は治療計画書に基づく間違った治療につながる場合、又は手動、自動的な決定の使用、若しくは人工知能を通してのいずれかによる、ある人物の誤ったイメージが、誤った根拠に基づく決定を導く可能性がある場合などである。

79. Key design and default accuracy elements may include:
正確性の主要なデザイン及びデフォルトの要素には、以下が含まれうる。

- Data source – Sources of personal data should be reliable in terms of data accuracy.
データの情報源 – 個人データの情報源は、データの正確性の点で信頼できるものでなければならない。

- Degree of accuracy – Each personal data element should be as accurate as necessary for the specified purposes.
正確性の程度 – 各個人データの要素は、特定された目的にとって必要な程度に正確でなければならない。

- Measurably accurate - Reduce the number of false positives/negatives, for example biases in automated decisions and artificial intelligence.
測定可能な程度の正確性 – 自動的な決定及び人工知能におけるバイアスなど、偽陽性／偽陰性の数を減らすこと。

- Verification – Depending on the nature of the data, in relation to how often it may change, the controller should verify the correctness of personal data with the data subject before and at different stages of the processing (e.g. to age requirements).
検証 – データの性質に応じて、データが変わりうる頻度に関連して、管理者は、取扱いの前及び取扱いの異なる段階において、データ主体に関する個人データの正確性を検証しなければならない（年齢要件に対してなど）。

- Erasure/rectification – The controller shall erase or rectify inaccurate data without delay. The controller shall in particular facilitate this where the data subjects are or were children and later want to remove such personal data.[39]
消去／訂正 – 管理者は、不正確なデータについて、遅滞なく消去又は訂正すること。管理者は、データ主体が子どもである又は当時子どもであり、後にそのような不正確な個人データの削除を希望する場合には、特にこのことが容易になされるようにすること。[39]

- Error propagation avoidance – Controllers should mitigate the effect of an accumulated error in the processing chain.
エラーの伝播の回避 – 管理者は、取扱いの連鎖の中で、エラーが蓄積されることによる影響を低減しなければならない。

[39] Cf. Recital 65.
前文第 65 項参照。

- Access – Data subjects should be given information about and effective access to personal data in accordance with the GDPR articles 12 to 15 in order to control accuracy and rectify as needed.
  アクセス – 正確性を管理し、必要に応じて訂正するために、GDPR 第 12 条から第 15 条に従い、データ主体には、個人データに関する情報及び個人データに効果的にアクセスする権利が与えられなければならない。

- Continued accuracy – Personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps.
  継続的な正確性 – 個人データは、取扱いの全ての段階で正確でなければならず、重要な段階では、正確性のテストが実施されなければならない。

- Up to date – Personal data shall be updated if necessary for the purpose.
  最新の – 個人データは、目的のために、必要に応じて更新されること。

- Data design - Use of technological and organisational design features to decrease inaccuracy, for example present concise predetermined choices instead of free text fields.
  データのデザイン – 不正確さを減らすために、例えば、自由記述欄の代わりに、簡潔なあらかじめ決められた選択肢を提示するなど、技術的及び組織的なデザイン機能を使用すること。

Example 1
事例 1
An insurance company wishes to use artificial intelligence (AI) to profile customers buying insurance as a basis for their decision making when calculating the insurance risk. When determining how their AI solutions should be developed, they are determining the means of processing and shall consider data protection by design when choosing an AI application from a vendor and when deciding on how to train the AI.
ある保険会社は、保険リスクを算出する際の判断材料として、保険を購入する顧客のプロファイリングを行うために、人工知能 (AI) を使用したい。自社の AI ソリューションをどのように開発すべきかを決定するにあたり、保険会社は、取扱いの手段を決定しているところであり、ベンダーから AI アプリケーションを選択する際及び AI のトレーニング方法を決定する際に、データ保護バイデザインを考慮する予定である。

When determining how to train the AI, the controller should have accurate data to achieve precise results. Therefore, the controller should ensure that the data used to train the AI is accurate.
AI のトレーニング方法を決定するにあたり、管理者は、正確な結果を得るために、正確なデータを保持しなければならない。したがって、管理者は、AI のトレーニングに使用されるデータが正確であることを確保しなければならない。

Granted that they have a valid legal basis to train the AI using personal data from a large subset of their existing customers, the controller chooses a pool of customers that is representative of the population to also avoid bias.
自社の既存の顧客の大規模な部分集合からの個人データを使用して AI をトレーニングするために、当社が有効な法的根拠を保持していることを前提として、管理者は、バイアスを避けるためにも、母集団を代表する顧客の集団を選ぶ。

The customer data is then collected from the respective data handling system, including data on the type of insurance, for example health insurance, home insurance, travel insurance, etc. as well as data

from public registries they have lawful access to. All data are pseudonymized prior to transfer to the system dedicated to the training of the AI model.
次に、顧客データは、健康保険、住宅保険、旅行保険などの保険の種類に関するデータや、当社が適法にアクセスできるパブリックレジストリからのデータなど、それぞれのデータ処理システムから収集される。全てのデータは、AI モデルのトレーニング専用のシステムに転送される前に仮名化される。

To ensure that the data used for AI training is as accurate as possible, the controller only collects data from data sources with correct and up-to date information.
AI トレーニングに使用されるデータが可能な限り正確であることを確保するため、管理者は、正確かつ最新情報のデータ情報源からのみデータを収集する。

The insurance company tests whether the AI is reliable and provides non-discriminatory results both during its development and finally before the product is released. When the AI is fully trained and operative, the insurance company uses the results to support the insurance risk assessments, yet without solely relying on the AI to decide whether to grant insurance, unless the decision is made in accordance with the exceptions in Article 22 (2) GDPR.
当該保険会社は、開発中及び当該製品を稼働させる前の最終段階の両方において、当該 AI が信頼できるものかどうか、また、統計的無差別な結果を提供するかどうかについて、テストする。AI が完全に訓練され、機能する場合、保険会社は、保険リスク評価を支援するために当該結果を使用するが、GDPR 第 22 条(2)の例外に従って決定される場合を除き、保険を付与するかどうかの決定を AI だけに依存することはない。

The insurance company will also regularly review the results from the AI, to maintain the reliability and when necessary adjust the algorithm.
保険会社はまた、AI から得られる結果を定期的に見直し、信頼性を維持し、また必要に応じてアルゴリズムを調整する。

Example 2
事例 2
The controller is a health institution looking to find methods to ensure the integrity and accuracy of personal data in their client registers.
管理者は、患者名簿内の個人データの完全性及び正確性を確保する方法を模索している医療機関である。

In situations where two persons arrive at the institution at the same time and receive the same treatment, there is a risk of mistaking them if the only parameter to distinguish them is by name. To ensure accuracy, the controller needs a unique identifier for each person, and therefore more information than just the name of the client.
2 名の人物が同時に同施設に到着し、同じ治療を受ける状況において、彼らを区別する唯一のパラメータが名前である場合、彼らを取り違えるリスクがある。正確性を確保するために、管理者は、各個人の一意の識別子が必要であり、したがって患者の名前だけでなく追加的な情報が必要である。

The institution uses several systems containing personal information of clients, and needs to ensure that the information related to the client is correct, accurate and consistent in all the systems at any point in time. The institution has identified several risks that may arise if information is changed in one system but not in the others.
当該医療機関は、複数のシステムを使用し患者の個人情報を記録しており、患者に関連する情報が、どの時点においても、全てのシステムにおいて正しく、的確で、一貫していること

を確保する必要がある。当該医療機関は、情報が一つのシステムで変更され、他のシステムでは変更されない場合に発生する可能性のある、いくつかのリスクを特定している。

The controller decides to mitigate the risk by using a hashing technique that can be used to ensure integrity of data in the treatment journal. Immutable cryptographic time stamps are created for treatment journal records and the client associated with them so that any changes can be recognized, correlated and traced if required.
管理者は、治療日誌内のデータの完全性を確保するために利用可能なハッシュ化技術を使用することにより、このリスクを低減することを決定する。治療日誌記録とそれに関連付けられた患者に対して、イミュータブル暗号タイムスタンプが生成されることで、如何なる変更も認識され、関連付けられ、かつ必要な場合、変更を追跡することが可能となる。

3.7 Storage limitation
記録保存の制限

80. The controller must ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.[40]It is vital that the controller knows exactly what personal data the company processes and why. The purpose of the processing shall be the main criterion to decide in how long personal data shall be stored.
管理者は、個人データが、その個人データが取扱われる目的のために必要な期間だけ、データ主体の識別を許容する方式で維持されるよう、確保しなければならない。[40] 会社がどのような個人データを取り扱うのか、また、何故取り扱うのかについて、管理者が正確に把握することが肝要である。取扱いの目的は、個人データを記録保存する期間を決定する主要な基準となる。

81. Measures and safeguards that implement the principle of storage limitation shall complement the rights and freedoms of the data subjects, specifically, the right to erasure and the right to object.
記録保存の制限の原則を実装する措置及び保護措置は、データ主体の権利及び自由、特に、消去の権利及び異議を述べる権利を補完するものとする。

82. Key design and default storage limitation elements may include:
記録保存の制限の主要なデザイン及びデフォルトの要素には、以下が含まれうる。

- Deletion and anonymization – The controller should have clear internal procedures and functionalities for deletion and/or anonymization.
  消去及び匿名化 – 管理者は、消去及び／又は匿名化のための明確な内部手順及び機能を保持しなければならない。

- Effectiveness of anonymization/deletion – The controller shall make sure that it is not possible to re-identify anonymized data or recover deleted data, and should test whether this is possible.
  匿名化／消去の実効性 – 管理者は、匿名化されたデータを再識別すること、又は消去されたデータを回復することが不可能であることを確認するものとし、このことが可能かどうかをテストしなければならない。

- Automation – Deletion of certain personal data should be automated

[40] Art. 5(1)(c) GDPR.※
GDPR 第 5 条(1)(c)。※
※仮訳者注：記録保存の制限の規定は、GDPR 第 5 条(1)(e)。

自動化 – 特定の個人データの消去は自動化されなければならない。

- Storage criteria – The controller shall determine what data and length of storage is necessary for the purpose.
  記録保存の基準 – 管理者は、取扱いの目的にとって、どのようなデータ及び期間の記録保存が必要かについて判断すること。

- Justification – The controller shall be able to justify why the period of storage is necessary for the purpose and the personal data in question, and be able to disclose the rationale behind, and legal grounds for the retention period.
  正当性 – 管理者は、記録保存の期間が、取扱いの目的及び該当の個人データにとって、必要である理由を正当化できるものとし、その背後にある理論的根拠、及び保持期間の法的根拠を開示できること。

- Enforcement of retention policies – The controller should enforce internal retention policies and conduct tests of whether the organization practices its policies.
  保持方針の実施 – 管理者は、内部の保持方針を実施させ、また組織がその方針を実践しているかどうかのテストを実施しなければならない。

- Backups/logs – Controllers shall determine what personal data and length of storage is necessary for back-ups and logs.
  バックアップ／ログ – 管理者は、バックアップ及びログのために、どのような個人データ及び期間の記録保存が必要かについて判断すること。

- Data flow – Controllers should beware of the flow of personal data, and the storage of any copies thereof, and seek to limit their "temporary" storage.
  データフロー – 管理者は、個人データの流れ、及びその複生物の記録保存に注意し、「一時的な」記録保存を制限するよう努めなければならない。

Example
事例

The controller collects personal data where the purpose of the processing is to administer a membership of the data subject. The personal data shall be deleted when the membership is terminated and there is no legal basis for further storage of the data.
管理者は、データ主体のメンバーシップを管理するという取扱い目的で、個人データを収集する。メンバーシップが終了し、データを追加的に記録保存する法的根拠がなくなった時点で、個人データは消去される。

The controller first draws up an internal procedure for data retention and deletion. According to this, employees shall manually delete personal data after the retention period ends. The employee follows the procedure to regularly delete and correct data from any devices, from backups, logs, e-mails and other relevant storage media.
管理者はまず、データの保持及び消去のための内部手順を作成する。これによると、従業員は、保持期間終了後、個人データを手動で消去することになる。従業員は当該内部手順に従い、あらゆるデバイス、並びにバックアップ、ログ、電子メール、及びその他の関連する記憶媒体から、データを定期的に消去及び修正する。

To make deletion more effective, and less error-prone, the controller then implements an automatic system instead, in order to delete data automatically, reliably and more regularly. The system is configured to follow the given procedure for data deletion which then occurs at a predefined regular

interval to remove personal data from all of the company's storage media. The controller reviews and tests the retention procedure regularly and ensures that it concurs with the up-to-date retention policy.
消去をより効果的にし、かつエラーの発生を少なくするために、管理者は代わりに、データを自動的に、確実に、より頻繁に消去するための、自動システムを実装する。このシステムは、所定のデータ消去手順に従うように設定されており、データ消去は事前に定義された定期的な間隔で実行され、会社の全ての記憶媒体から個人データが消去される。管理者は定期的に保持手順を見直し、テストし、また、それが最新の保持方針と一致していることを確保する。

3.8 Integrity and confidentiality
完全性及び機密性

83. The principle of integrity and confidentiality includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The security of personal data requires appropriate measures designed to prevent and manage data breach incidents; to guarantee the proper execution of data processing tasks, and compliance with the other principles; and to facilitate the effective exercise of individuals' rights.
完全性及び機密性の原則には、無権限の又は違法な取扱いに対して、及び、偶発的な喪失、破壊又は損壊に対して、適切な技術上又は組織上の措置を用いて行われる保護が含まれる。個人データの安全性には、データ侵害インシデントを防止及び管理するために、データ取扱い任務の適切な遂行及び他の基本原則の遵守を保証するために、また、個人の権利の効果的な行使を促進するために設計された、適切な措置が要求される。

84. Recital 78 states that one of the DPbDD measures could consist of enabling the controller to *"create and improve security features"*. Along with other DPbDD measures, Recital 78 suggests a responsibility on the controllers to continually assess whether it is using the appropriate means of processing at all times and to assess whether the chosen measures actually counter the existing vulnerabilities. Furthermore, controllers should conduct regular reviews of the information security measures that surround and protect personal data, and the procedure for handling data breaches.
前文第 78 項は、そのような DPbDD 措置を構成しうる一つとして、管理者が *「安全機能を開発し、向上」* させることを可能とすることと規定している。他の DPbDD 措置を実装することと共に、前文第 78 項は、常に適切な取扱いの手段を使用しているかどうかについて継続的に評価し、また、自身が選択した措置が実際に現存の脆弱性に対応しているかを評価するという責任が管理者にあることを示唆している。さらに、管理者は、個人データを取り囲み保護する情報セキュリティ措置、及びデータ侵害対応の手順書について、定期的な見直しを実施しなければならない。

85. Key design and default integrity and confidentiality elements may include:
完全性及び機密性の主要なデザイン及びデフォルトの要素には、以下が含まれうる。

- Information security management system (ISMS) – Have an operative means of managing policies and procedures for information security.
  情報セキュリティ管理システム (ISMS) – 情報セキュリティに関する方針及び手順を管理する運用上の手段を備えること。

- Risk analysis – Assess the risks against the security of personal data by considering the impact on individuals' rights and counter identified risks. For use in risk assessment; develop and maintain a comprehensive, systematic and realistic "threat modelling" and an attack surface analysis of the designed software to reduce attack vectors and opportunities to exploit weak points and vulnerabilities.

リスク分析 – 個人の権利への影響を考慮することにより個人データの安全性に対するリスクを評価し、特定されたリスクに対応すること。リスク評価の際に使用するものとして、設計したソフトウェアの弱点及び脆弱性を悪用する攻撃ベクトル並びに攻撃機会を減らすことを目的とした、包括的で体系的かつ現実的な「脅威モデリング」及び攻撃対象領域分析を開発し、維持管理すること。

- Security by design – Consider security requirements as early as possible in the system design and development and continuously integrate and perform relevant tests.
  セキュリティ設計 – システムの設計及び開発のできるだけ早い段階でセキュリティ要件を検討し、継続的に関連するテストを統合し、実行すること。

- Maintenance – Regular review and test software, hardware, systems and services, etc. to uncover vulnerabilities of the systems supporting the processing.
  維持管理　– ソフトウェア、ハードウェア、システム及びサービスなどを定期的に見直し、また、テストし、取扱いを支援するシステムの脆弱性を発見すること。 ·

- Access control management – Only the authorized personnel who need to should have access to the personal data necessary for their processing tasks, and the controller should differentiate between access privileges of authorized personnel.
  アクセス制御管理　–　アクセスする必要のある、権限を付与された担当者のみが、その取扱い任務に必要な個人データに対するアクセス権を持つ必要があり、管理者は、権限を付与される担当者のアクセス権限について差別化しなければならない。

    - Access limitation (agents) – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.
      アクセスの制限（従業員）– 自身の職務を遂行するために個人データへのアクセスを必要とする従業員の数が最小限となるようにデータの取扱いを形成し、それに応じてアクセスを制限すること。

    - Access limitation (content) – In the context of each processing operation, limit access to only those attributes per data set that are needed to perform that operation. Moreover, limit access to data pertaining to those data subjects who are in the remit of the respective employee.
      アクセスの制限（内容）– 各取扱業務の過程において、該当の業務を実行するために必要となるデータセットごとの属性のみへのアクセスに限定すること。加えて、アクセスを、従業員ごとの職務権限内にあるデータ主体に関連するデータに限定すること。

    - Access segregation – Shape the data processing in a way that no individual needs comprehensive access to all data collected about a data subject, much less all personal data of a particular category of data subjects.
      アクセスの分離 – あるデータ主体に関して収集された全てのデータに、特に特定の類型のデータ主体に関する全ての個人データに、何人も包括的にアクセスする必要がないように、データの取扱いを形成すること。

- Secure transfers – Transfers shall be secured against unauthorized and accidental access and changes.
  安全な移転 – 移転は、無権限及び偶発的なアクセス並びに変更に対して保護されること。

- Secure storage – Data storage shall be secure from unauthorized access and changes. There should be procedures to assess the risk of centralized or decentralized storage, and what categories of personal data this applies to. Some data may need additional security measures than others or isolation from others.
  安全な記録保存 – データは、無権限なアクセス及び変更から安全に記録保存されること。集中型又は分散型の保存リスクについて、またこのことがどの種類の個人データに当てはまるかについて評価するための手順を設けること。一部のデータには、他のデータに比べ追加的な安全管理措置が必要な場合、又は他のデータからの分離が必要な場合がありうる。

- Pseudonymization – Personal data and back-ups/logs should be pseudonymized as a security measure to minimise risks of potential data breaches, for example using hashing or encryption.
  仮名化 – 潜在的なデータ侵害のリスクを最小限に抑えるための安全管理措置として、個人データ及びバックアップ／ログは、例えば、ハッシュ化又は暗号化を用いて、仮名化しなければならない。

- Backups/logs – Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control. These shall be protected from unauthorised and accidental access and change and reviewed regularly and incidents should be handled promptly.
  バックアップ／ログ – 情報セキュリティに必要な範囲でバックアップ及びログを維持し、日常的なセキュリティ管理として監査証跡及びイベント監視を使用すること。バックアップ及びログを無権限及び偶発的なアクセス並びに変更から保護し、定期的に見直すこと。また、インシデントは迅速に対処されなければならない。

- Disaster recovery/ business continuity – Address information system disaster recovery and business continuity requirements to restore the availability of personal data following up major incidents.
  災害復旧/事業継続 – 重大なインシデントに続く個人データの可用性を回復するため、情報システムの災害復旧及び事業継続の要件に対応しておくこと。

- Protection according to risk – All categories of personal data should be protected with measures adequate with respect to the risk of a security breach. Data presenting special risks should, when possible, be kept separated from the rest of the personal data.
  リスクに応じた保護 – 全ての種類の個人データは、セキュリティ侵害のリスクに関して適切な措置で保護されなければならない。特別なリスクを伴うデータは、可能な場合、他の個人データから切り離して保管されなければならない。

- Security incident response management – Have in place routines, procedures and resources to detect, contain, handle, report and learn from data breaches.
  セキュリティインシデント対応管理 – データ侵害を検知し、封じ込め、対処し、報告し、またそこから学ぶための一定の行動、手順、及びリソースを整備しておくこと。

- Incident management – Controller should have processes in place to handle breaches and incidents, in order to make the processing system more robust. This includes notification procedures, such as management of notification (to the supervisory authority) and information (to data subjects).
  インシデント管理 – 管理者は、処理システムをより強固なものにするために、侵害及びインシデントに対応するための工程を整備しておかなければならない。これには、

（監督機関に対する）通知及び（データ主体に対する）連絡の管理など、通知の手順が含まれる。

Example
事例
A controller wants to extract large quantities of personal data from a medical database containing electronic (patient) health records to a dedicated database server in the company in order to process the extracted data for quality assurance purposes. The company has assessed the risk for routing the extracts to a server that is accessible to all of the company's employees as likely to be high for data subjects' rights and freedoms. Since there is only one department in the company who needs to process the patient data extracts, the controller decides to restrict access to the dedicated server to employees in that department. Moreover, to further reduce risk, the data will be pseudonymized before they are transferred.
ある管理者は、電子的な（患者の）健康記録が入っている医療データベースから大量の個人データを社内の専用データベースサーバーに抽出し、品質保証の目的のためにその抽出したデータを取り扱いたい。同社は、全従業員がアクセス可能なサーバーに当該抽出物を移すリスクは、データ主体の権利及び自由にとって高いおそれがあると評価している。当該患者データの抽出物を取り扱う必要があるのは、社内で 1 部署に限られるため、管理者は、当該専用サーバーへのアクセスを、該当する部署の従業員に限定することを決定する。さらに、リスクを追加的に低減するため、データを移転前に仮名化する。

To regulate access and mitigate possible damage from malware, the company decides to segregate the network, and establish access controls to the server. In addition, they put up security monitoring and an intrusion detection and prevention system and isolates it from routine use. An automated auditing system is put in place to monitor access and changes. Reporting and automated alerts are generated from this when certain events related to usage are configured. The controller will ensure that users only have access on a need to know basis and with the appropriate access level. Inappropriate use can be quickly and easily detected.
アクセスを規制し、かつマルウェアによる被害の可能性を低減するため、同社は、ネットワークを分離し、当該サーバーへのアクセス制御を設けることを決定する。さらに、セキュリティ監視及び侵入検知・防止システムを設置し、当該サーバーを日常業務使用から隔離する。アクセス及び変更を監視するため、自動監査システムを導入する。使用状況に関連する特定のイベントが形成されると、レポート及び自動アラートがここから生成される。管理者は、ユーザーのアクセス権が、知る必要性の基準及び適切なアクセス基準に従って限定されるよう確保する予定である。不適切な使用は、迅速かつ容易に検出可能である。

Some of the extracts have to be compared with new extracts, and therefore are required to be stored for three months. The controller decides to put them into separate databases on the same server, and use both transparent and column-level encryption to store them. Keys for column data decryption are stored in dedicated security modules that can only be used by authorized personnel, but not extracted. Handling upcoming incidents makes the system more robust, and reliable. The data controller understands that preventative and effective measures and safeguards should be built into all personal data processing it undertakes now and in the future, and that doing so may help prevent future such data breach incidents.
一部の抽出物については、新しい抽出物と比較する必要があり、結果、3 か月間保存する必要がある。管理者は、それらを同じサーバー上の別のデータベースに配置し、透過的データ暗号化及び列レベル暗号化の両方を使用してそれらを保存することを決定する。列データの復号化用の鍵は、専用のセキュリティ モジュールに保存される。当該モジュールは、権限のある担当者のみが使用可能であり、抽出することはできない。今後のインシデントに対応しておくことで、システムがより強固になり、信頼性が高まる。データ管理者は、現在及び将

来的に実施する全ての個人データの取扱いの中に、予防的かつ効果的な措置及び保護措置を組み込んでおく必要があり、そうすることが将来のデータ侵害インシデントの防止に役立ちうることを理解している。

The controller establishes these security measures both to ensure accuracy, integrity and confidentiality, but also to prevent malware spread by cyber-attacks and to make the solution robust. Having robust security measures contributes to build trust with the data subjects.
管理者は、正確性、完全性及び機密性を確保するためだけでなく、サイバー攻撃によるマルウェアの拡散を防止し、当該ソリューションを強固なものにするために、これらのセキュリティ措置を設ける。強固なセキュリティ措置を講じることは、データ主体との信頼関係の構築に寄与する。

3.9 Accountability[41]
アカウンタビリティ [41]

86. The principle of accountability states that the controller shall be responsible for, and be able to demonstrate compliance with all of the abovementioned principles.
アカウンタビリティの原則は、管理者は、上記の全ての基本原則について責任を負い、かつ、その遵守を証明できるようにしなければならないものとすると規定している。

87. The controller needs to be able to demonstrate compliance with the principles. In doing so, the controller may demonstrate the effects of the measures taken to protect the data subjects' rights, and why the measures are considered to be appropriate and effective. For example, demonstrating why a measure is appropriate to ensure the principle of storage limitation in an effective manner.
管理者は、基本原則の遵守を証明できる必要がある。その際、管理者は、データ主体の権利を保護するために講じられている措置の効果と、その措置が適切かつ効果的であると考えられる理由を立証してもよい。例えば、ある措置が、効果的な方法で記録保存の制限の原則を確保するために適切であるという理由を立証するなどである。

88. To be able to process personal data responsibly, the controller should have both the knowledge of and the ability to implement data protection. This entails that the controller should understand their data protection obligations of the GDPR and be able to comply with these obligations.
責任を持って個人データを取り扱うことができるよう、管理者は、データ保護に関する知識及びデータ保護の実装能力の両方を備えていなければならない。このことは、管理者がGDPR のデータ保護義務を理解し、これらの義務を遵守可能でなければならないことを意味する。

4 ARTICLE 25(3) CERTIFICATION
第 25 条(3) 認証

89. According to Article 25(3), certification pursuant to Article 42 may be used as an element to demonstrate compliance with DPbDD. Conversely, documents demonstrating compliance with DPbDD may also be useful in a certification process. This means that where a processing operation by a controller or a processor has been certified as per Article 42, supervisory authorities shall take this into account in their assessment of compliance with the GDPR, specifically with regards to DPbDD.

[41] See Recital 74, where controllers are required to demonstrate the effectiveness of their measures.
前文第 74 項参照。そこでは管理者が、自身の措置の実効性を証明できるようにすることが要求されている。

第 25 条(3)によれば、第 42 条による認証は、DPbDD への遵守を証明する要素として使用されうる。 逆に、DPbDD への遵守を証明する文書が、認証プロセスにおいて有用でもありうる。このことは、管理者又は処理者による取扱業務が第 42 条に従って認証されている場合、監督機関は、GDPR への遵守の評価の際、特に DPbDD に関して、このことを考慮することを意味する。

90. When a processing operation by a controller or processor is certified according to Article 42, the elements that contribute to demonstrating compliance with Article 25(1) and (2) are the design processes, i.e. the process of determining the means of processing, the governance and the technical and organizational measures to implement the data protection principles[.] The data protection certification criteria are determined by the certification bodies or certification scheme owners and then approved by the competent supervisory authority or by the EDPB. For further information about certification mechanisms, we refer the reader to the EDPB Guideline on Certification[42] and other relevant guidance, as published on the EDPB website.
管理者又は処理者による取扱業務が第 42 条に従って認証される場合、第 25 条 (1)及び (2) への遵守の証明に寄与する要素は、設計プロセス、すなわち、データ保護の原則を実装するために、取扱いの手段、ガバナンス並びに技術的及び組織的措置を決定するプロセスである。データ保護の認証基準は、認証機関又は認証スキーム保有者により決定され、次に所轄監督機関又は EDPB により承認される。認証メカニズムの詳細については、EDPB の Web サイト上で公開されている EDPB の認証に関するガイドライン [42] 及びその他の関連ガイダンスを参照されたい。

91. Even where a processing operation is awarded a certification in accordance with Article 42, the controller still has the responsibility to continuously monitor and improve compliance with the DPbDDcriteria of Article 25.
取扱業務が第 42 条に従って認証を得ている場合でも、管理者には依然、第 25 条の DPbDD 基準への遵守を継続的に監視し、改善する責任がある。

5 ENFORCEMENT OF ARTICLE 25 AND CONSEQUENCES
第 25 条の執行及び結果

92. Supervisory authorities may assess compliance with Article 25 according to the procedures listed in Article 58. The corrective powers are specified in Article 58(2) and include the issuance of warnings, reprimands, orders to comply with data subjects' rights, limitations on or ban of processing, administrative fines, etc.
監督機関は、第 58 条に列挙された手順に従い、第 25 条の遵守を評価しうる。是正権限は第 58 条 (2) に規定されており、警告を発すること、懲戒を発すること、データ主体の権利を遵守するよう命令ずること、取扱いを制限又は禁止すること、制裁金を科すことなどが含まれる。

[42] EDPB. "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation". Version 3.0, 4 June 2019.
edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf
EDPB、「規則の第 42 条及び第 43 条に基づく認証及び認証基準の特定に関するガイドライン 1/2018」、バージョン 3.0、2019 年 6 月 4 日。
edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

94. DPbDD is further a factor in determining the level of monetary sanctions for breaches of the GDPR, see Article 83(4).[43] [44]
DPbDD はさらに、GDPR 違反に対する金銭的制裁の水準を決定する要因となる。第 83 条(4)参照。[43] [44]

6 RECOMMENDATIONS
勧告

95. Although not directly addressed in Article 25, processors and producers are also recognized as key enablers for DPbDD, they should be aware that controllers are required to only process personal data with systems and technologies that have built-in data protection.
第 25 条において直接対応されていないが、処理者及び開発者もまた、 DPbDD の主要な実現者として認識されており、両者は、管理者がデータ保護の組み込まれたシステム及び技術でのみ個人データを取り扱うよう要求されていることに留意しなければならない。

96. When processing on behalf of controllers, or providing solutions to controllers, processors and producers should use their expertise to build trust and guide their customers, including SMEs, in designing /procuring solutions that embed data protection into the processing. This means in turn that the design of products and services should facilitate controllers' needs.
管理者に代わって取扱いを行う場合、又は管理者に対しソリューションを提供する場合、処理者及び開発者は、取扱いにデータ保護が組み込まれたソリューションの設計／調達をするよう、自身の専門知識を駆使して信頼を構築し、SMEs を含む顧客を先導しなければならない。このことは、つまり、その製品及びサービスの設計が管理者のニーズを満たすものでなければならないことを意味する。

97. It should be kept in mind when implementing Article 25 that the main design objective is the *effective implementation* of the principles and *protection* of the rights of data subjects into the appropriate measures of the processing. In order to facilitate and enhance the adoption of DPbDD, we make the following recommendations to controllers as well as producers and processors:
第 25 条を実装する際には、主な設計の目的が、適切な取扱いの措置の中に、*効果的な*基本原則の*実装*及びデータ主体の権利の*保護*を導入することであることに留意しなければならない。 DPbDD の導入を促進し、強化するために、EDPB は、管理者並びに開発者及び処理者に対し、次の勧告を行う。

- Controllers should think of data protection from the *initial stages* of planning a processing operation, even before the time of determination of the means of processing.

---

[43] Article 83(2)(d) GDPR stipulates that in determining the imposition of fines for breach of the GDPR *"due regard" shall be taken of "the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32".*
GDPR 第 83 条(2)(d) は、GDPR 違反に対し制裁金を科すか否かについて判断する際には、*「第 25 条及び第 32 条により管理者又は処理者によって実装された技術上及び組織上の措置を考慮に入れた上で、管理者又は処理者の責任の程度」を「適正に考慮」に入れる*と規定している。

[44] More information on fines can be found in Article 29 Working Party. "Guidelines on application and setting of administrative fines for the purposes of the Regulation 2016/679". WP 253, 3 October 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 - endorsed by the EDPB.
制裁金の詳細については、次を参照されたい。第 29 条作業部会 、「規則 2016/679 の目的のための制裁金の適用及び設定に関するガイドライン」、 WP 253、2017 年 10 月 3 日。ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 - EDPB 承認版。

管理者は、取扱業務を計画する*初期の段階*から、取扱いの手段を決定する時点の前であっても、データ保護について考えなければならない。

- Where the controller has a Data Protection Officer (DPO), the EDPB encourages the active involvement of the DPO to integrate DPbDD in the procurement and development procedures, as well as in the whole processing life-cycle.
管理者にデータ保護オフィサー（DPO）がいる場合、EDPB は、調達及び開発手順において、また、取扱いのライフサイクル全体において DPbDD を組み込むべく、DPO が積極的に関与していくよう奨励する。

- A processing operation may be *certified*. The ability to get a processing operation certified provides an added value to a controller when choosing between different processing software, hardware, services and/or systems from producers or processors. Therefore, producers should strive to demonstrate DPbDD in the life-cycle of their development of a processing solution. A certification seal may also guide data subjects in their choice between different goods and services. Having the ability to get a processing certified can serve as a competitive advantage for producers, processors and controllers, and even enhances data subjects' trust in the processing of their personal data. If no certification is offered, controllers should seek to have other *guarantees* that producers or processors comply with the requirements of DPbDD.
取扱業務は、*認証*されうる。取扱業務の認証を得る能力は、開発者又は処理者が提供する様々な処理ソフトウェア、ハードウェア、サービス、及び／又はシステムの中から選択する際、管理者に付加価値を提供する。したがって、開発者は、取扱いのソリューション開発のライフサイクル全体において、 DPbDD を証明するよう努めなければならない。認証シールは、データ主体が様々な商品及びサービスの中からの選択する際の手引きにもなりうる。取扱業務の認証を得る能力を保持することは、開発者、処理者及び管理者に対し競争上の優位性をもたらす可能性があるだけでなく、個人データを取り扱う中でデータ主体からの信頼も高める。認証が提供されない場合、管理者は、開発者又は処理者が DPbDD の要件を遵守しているという他の*保証*を得られるよう努めなければならない。

- Controllers, processors and producers, should consider their obligations to provide children under 18 and other vulnerable groups with specific protection in complying with DPbDD.
管理者、処理者及び開発者は、DPbDD を遵守する際、18 歳未満の子供ども及びその他の脆弱性のあるグループに対し、特別な保護を提供する自身の義務を考慮しなければならない。

- Producers and processors should seek to facilitate DPbDD implementation in order to support the controller's ability to comply with Article 25 obligations. Controllers, on the other hand, should not choose producers or processors who do not offer systems enabling or supporting the controller to comply with Article 25, because controllers will be held accountable for the lack of implementation thereof.
開発者及び処理者は、管理者の第 25 条の義務を遵守する能力を支援するするために、DPbDD の実装を促進するよう努めなければならない。一方、管理者は、管理者が第 25 条を遵守することを可能にする、又は支援するようなシステムを提供しない開発者又は処理者を選択すべきではない。管理者が、その実装の欠如に対する責任を負うことになるからである。

- Producers and processors should play an active role in ensuring that the criteria for the "state of the art" are met, and notify controllers of any changes to the "state of the art" that may

affect the effectiveness of the measures they have in place. Controllers should include this requirement as a contractual clause to make sure they are kept up to date.
開発者及び処理者は、「先端技術」の基準が満たされていることを確保するなかで積極的な役割を果たし、管理者が講じた措置の実効性に影響がありうる「先端技術」に対する変更について、管理者に通知しなければならない。管理者は、自身の講じた措置が常に最新の状態に保たれるよう確認すべく、この要件を契約条項として盛り込まなければならない。

- The EDPB recommends controllers to require that producers and processors demonstrate how their hardware, software, services or systems enable the controller to comply with the requirements to accountability in accordance with DPbDD, for example by using key performance indicators to demonstrate the effectiveness of the measures and safeguards at implementing the principles and rights.
EDPB は、管理者が開発者及び処理者に対し、次のことを要求するよう勧告する。基本原則及び権利を実装している措置及び保護措置の実効性を実証するために、例えば重要業績評価指数を使用して、開発者及び処理者が、自社のハードウェア、ソフトウェア、サービス、又はシステムにより、管理者がどのように DPbDD に従ったアカウンタビリティに対する要件を遵守することが可能となるかについて実証すること。

- The EDPB emphasizes the need for a harmonized approach to implement principles and rights in an effective manner and encourages associations or bodies preparing codes of conduct in accordance with Article 40 to also incorporate sector-specific guidance on DPbDD.
EDPB は、効果的な態様で基本原則及び権利を実装するための、調和のとれたアプローチの必要性を強調する。EDPB はまた、第 40 条に従い行動規範を用意する団体又は組織に対し、DPbDD に関するセクター固有のガイダンスを組み込むよう奨励する。

- Controllers should be fair to data subjects and transparent on how they assess and demonstrate effective DPbDD implementation, in the same manner as controllers demonstrate compliance with the GDPR under the principle of accountability.
管理者は、アカウンタビリティの原則に基づいて GDPR への遵守を証明するのと同様な態様で、データ主体に対して公正でなければならず、また、効果的な DPbDD の実装を評価及び証明する方法について透明性を確保しなければならない。

- Privacy-enhancing technologies (PETs) that have reached the state-of-the-art maturity can be employed as a measure in accordance with the DPbDD requirements if appropriate in a risk based approach. PETs in themselves do not necessarily cover the obligations of Article 25. Controllers shall assess whether the measure is appropriate and effective in implementing the data protection principles and the rights of data subjects.
最先端の成熟度に達したプライバシー強化技術 (PETs) は、リスクベースのアプローチで適切な場合、DPbDD 要件に従った措置として採用されうる。PETs は、それ自体で、第 25 条の義務を満たすとは限らない。管理者は、その措置がデータ保護の基本原則及びデータ主体の権利を実装する上で適切かつ効果的であるかどうかを評価するものとする。

- Existing legacy systems are under the same DPbDD-obligations as new systems. If legacy systems do not already comply with DPbDD, and changes cannot be made to comply with the obligations, then the legacy system simply does not meet GDPR-obligations and cannot be used to process personal data.
既存のレガシーシステムには、新規のシステムと同じ DPbDD 義務が課される。レガシーシステムが未だ DPbDD を遵守しておらず、かつ当該義務を遵守するための変更

を加えることができない場合、そのレガシーシステムは GDPR の義務を満たしておらず、個人データの取扱いに使用できない。

- Article 25 does not lower the threshold of requirements for SMEs. The following points may facilitate SMEs' compliance with Article 25:
  第 25 条は、SMEs に対して、その要件の閾値を下げていない。次の点は、SMEs が第 25 条を遵守するのを促進しうる。

    - Do early risk assessments
      早期にリスク評価を行うこと
    - Start with small processing – then scale its scope and sophistication later
      小規模な取扱いから開始し、後にその範囲及び高度さを拡大すること
    - Look for producer and processor guarantees of DPbDD, such as certification and adherence to code of conducts
      認証及び行動規範の遵守など、DPbDD に関する開発者及び処理者による保証を求めること
    - Use partners with a good track record
      良好な実績のあるパートナーを使用すること
    - Talk with DPAs
      データ保護機関(DPAs)と協議すること
    - Read guidance from DPAs and the EDPB
      DPAs 及び EDPB からのガイダンスを読むこと
    - Adhere to codes of conduct where available
      利用可能な場合、行動規範を遵守すること
    - Get professional help and advice
      専門家の助け及び助言を得ること

For the European Data Protection Board
The Chair
(Andrea Jelinek)