仮日本語訳

Guidelines on transparency
透明性に関するガイドライン

本書面は、ARTICLE 29 DATA PROTECTION WORKING PARTY （第29条作業部会）により2017年11月29日に採択後、修正のうえ2018年4月11日に採択された、 “Guidelines on transparency” の英語版の一部を個人情報保護委員会が翻訳したものである。本書面は参考のための仮日本語訳であって、その利用について当委員会は責任を負わないものとし、正確な内容については原文を参照されたい。

TABLE OF CONTENTS

目次

Introduction

序

1. These guidelines provide practical guidance and interpretative assistance from the Article 29 Working Party (WP29) on the new obligation of transparency concerning the processing of personal data under the General Data Protection Regulation[1] (the "GDPR"). Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights[2]. Insofar as compliance with transparency is required in relation to data processing under Directive (EU) 2016/680[3], these guidelines also apply to the interpretation of that principle[4]. These guidelines are, like all WP29 guidelines, intended to be generally applicable and relevant to controllers irrespective of the sectoral, industry or regulatory specifications particular to any given data controller. As such, these guidelines cannot address the nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area. However, these guidelines are intended to enable controllers to understand, at a high level, WP29's interpretation of what the transparency obligations entail in practice and to indicate the approach which WP29 considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures.

1. 本ガイドラインは、一般データ保護規則[1]（以下「GDPR」という）に基づく個人データの取扱いに関し、新たに設けられた透明性の義務について、第 29 条作業部会（WP29）が定めた実践的な指針と解釈を示す。透明性は、GDPR に基づく包括的な義務であって、以下の

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

個人データの取扱いに係る自然人の保護及び当該データの自由な移転並びに指令第 95/46/EC 号の廃止に関する 2016 年 4 月 27 日の欧州議会及び欧州理事会規則（EU）2016/679 号。

[2] These guidelines set out general principles in relation to the exercise of data subjects' rights rather than considering specific modalities for each of the individual data subject rights under the GDPR.

これらのガイドラインでは、GDPR に基づく個々のデータ主体のそれぞれの権利に関する手続を個別に検討するのではなく、データ主体の権利の行使に関する一般原則を定めている。

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

犯罪の防止、捜査、探知、起訴、又は刑事罰を科すために所管官庁が行う個人データの取扱いに関する自然人の保護並びに当該データの自由な移転並びに理事会枠組決定第 2008/977/JHA 号の廃止に関する 2016 年 4 月 27 日の欧州議会及び欧州理事会指令（EU）2016/680 号

[4] While transparency is not one of the principles relating to processing of personal data set out in Article 4 of Directive (EU) 2016/680, Recital 26 states that any processing of personal data must be "lawful, fair and transparent" in relation to the natural persons concerned.

透明性は、指令（EU）2016/680 号 4 条に規定されている個人データの取扱いに関する原則の一つではないものの、前文第 26 項では、個人データの取扱いが、該当する自然人との関係において「適法、公正かつ透明」でなければならないと述べられている。

三つの中心的な分野に適用される。すなわち、(1)データ主体への公正な取扱いに関連する情報の提供、(2)データ管理者が、GDPR に基づくデータ主体の権利についてデータ主体に伝える方法、(3)データ管理者がデータ主体の権利行使をどのように支援するか、の三つである[2]。EU 指令第 2016/680 号[3]に基づくデータの取扱いに関して透明性の遵守が要求される限り、本ガイドラインもその原則の解釈に適用される[4]。本ガイドラインについては、全ての第 29 条作業部会ガイドラインと同様、当該データ管理者のセクター、業界、規制上の仕様にかかわらず、管理者に一般的に適用され、関連づけられるものであることが意図されている。したがって、本ガイドラインは、特定のセクター、業界又は規制分野の透明性の義務に関して問題となりうるような表現の細かな差異及び各種の変動する要素に対処するためのものではない。しかしながら、本ガイドラインは、管理者が、透明性の義務に実際に伴うものが何であるかに関して、第 29 条作業部会の解釈を十分に理解できるようにすること、並びに、管理者による透明性を確保するための措置が公正さ及びアカウンタビリティを伴ったものでありながらも、透明性を備えたものとなるようにするために管理者が採用すべきと W29 が考えるアプローチを示すことを意図している。

2. Transparency is a long established feature of the law of the EU[5]. It is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union. Under the GDPR (Article 5(1)(a) [6]), in addition to the requirements that data must be processed lawfully and fairly, transparency is now included as a fundamental aspect of these principles[7]. Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject[8]. Connected to this, the accountability principle

---

[5] Article 1 of the TEU refers to decisions being taken "*as openly as possible and as close to the citizen as possible*"; Article 11(2) states that "*The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society*"; and Article 15 of the TFEU refers amongst other things to citizens of the Union having a right of access to documents of Union institutions, bodies, offices and agencies and the requirements of those Union institutions, bodies, offices and agencies to ensure that their proceedings are transparent.

リスボン条約第 1 条では、決定は「*可能な限り公開の場で、かつ、可能な限り市民に近いところで*」行われると述べられており、第 11 条(2)では、「*機関は、代表団体及び市民社会との公開され、透明性があり、かつ定期的な対話を維持する*」とされている。また、ローマ条約第 15 条では、とりわけ、EU 市民が、EU 機関、団体、事業体及び行政機関の文書にアクセスする権利を有すること、並びに、その手続が透明性を備えたものとなるように確保する EU 機関、団体、事業体、及び行政機関の義務に言及している。

[6] "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".

「個人データは、データ主体との関係で適法、公正かつ透明性のある方法で取扱われるものとする」。

[7] In Directive 95/46/EC, transparency was only alluded to in Recital 38 by way of a requirement for processing of data to be fair, but not expressly referenced in the equivalent Article 6(1)(a).

指令第 95/46/EC 号では、透明性について、前文第 38 項でデータの公正な取扱いを求める要件として言及するに過ぎず、これに準ずる第 6 条(1)(a)では明記していない。

[8] Article 5.2 of the GDPR obliges a data controller to demonstrate transparency (together with the five other principles relating to data processing set out in Article 5.1) under the principle of accountability.

requires transparency of processing operations in order that data controllers are able to demonstrate compliance with their obligations under the GDPR[9].

2. 透明性は、EU 法において確立されてきた伝統である[5]。それは、市民が自らに影響を及ぼすプロセスについて理解し、必要に応じてこれに異議を唱えられるようにすることで、そうしたプロセスへの信頼を生み出すためのものである。また、これは、欧州連合基本権憲章第 8 条に規定されている個人データの取扱いに関連する公正さの原則の表明でもある。GDPR（第 5 条(1)(a)[6]）の下では、データが適法かつ公正に取扱われなければならないという要件に加え、現在では透明性が、これら公正さの原則の基本的要素として含められている[7]。透明性は、公正さとアカウンタビリティという GDPR に基づく新しい原則に本質的に結びついている。また、第 5 条(2)により管理者は、個人データがデータ主体との関係において透明性のある方法で取扱われていることを常に証明できなければならないことになる[8]。これに関して言えば、データ管理者が GDPR に基づく義務の履行を証明できるためには、アカウンタビリティの原則に基づいて、取扱業務にも透明性が求められることとなる[9]。

3. In accordance with Recital 171 of the GDPR, where processing is already under way prior to 25 May 2018, a data controller should ensure that it is compliant with its transparency obligations as of 25 May 2018 (along with all other obligations under the GDPR). This means that prior to 25 May 2018, data controllers should revisit all information provided to data subjects on processing of their personal data (for example in privacy statements/ notices etc.) to ensure that they adhere to the requirements in relation to transparency which are discussed in these guidelines. Where changes or additions are made to such information, controllers should make it clear to data subjects that these changes have been effected in order to comply with the GDPR. WP29 recommends that such changes or additions be actively brought to the attention of data subjects but at a minimum controllers should make this information publically available (e.g. on their website). However, if the changes or additions are material or substantive, then in line with paragraphs 29 to 32 below, such changes should be actively brought to the attention of the data subject.

3. 2018 年 5 月 25 日までに取扱いを開始している場合、データ管理者は、GDPR の前文第 171 項に従い、2018 年 5 月 25 日の時点で（GDPR に基づく他の義務とともに）透明性の義務に適合するように確保するべきである。これが意味することは、データ管理者が、本ガイドラインで説明している透明性に関する要件に自らが適合するよう確保するため、2018 年 5 月 25 日までに、データ主体の個人データの取扱いに関して各々のデータ主体に提供している全ての情報（例えば、プライバシーステートメント／プライバシーノーティスなど）を

GDPR 第 5 条(2)は、アカウンタビリティの原則に基づき、（第 5 条（1）に規定されたデータの取扱いに関する他の五つの原則とともに）透明性を証明するようデータ管理者に義務付けている。

[9] The obligation upon data controllers to implement technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR is set out in Article 24.1.

第 24 条（1）では、GDPR に従って取扱いが行われるよう確保し、それを証明するための技術的及び組織的措置を実施するデータ管理者の義務を規定している。

再確認するべきだということである。そのような情報が変更又は追加された場合、管理者は、これらの変更が GDPR を遵守する形で実施されたことをデータ主体に明示すべきである。第 29 条作業部会では、そのような変更や追加について積極的にデータ主体に知らせるよう勧告しているものの、管理者は、最低限、こうしたことに関する情報を（例えばウェブサイト上に）公開すべきである。しかしながら、変更又は追加が重大なものである場合、又はかなりの規模に及ぶ場合、以下の第 29 項から第 32 項に則り、そのような変更についてデータ主体に積極的に情報提供を行うべきである。

4. Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights[10]. The concept of transparency in the GDPR is user-centric rather than legalistic and is realized by way of specific practical requirements on data controllers and processors in a number of articles. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR. However, the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects.

4. 透明性がデータ管理者によって遵守されている場合、例えば、事前の情報に基づく同意を提供又は撤回し、データ主体の権利を行使することよって、データ主体は、データの管理者及び処理者に対して説明責任を課すこと及び自らの個人データを管理することができるようになる[10]。GDPR における透明性の概念は、法律的観点からのものであるというよりも、むしろユーザー中心主義的なものであり、データ管理者及び処理者に対する具体的で実用的な要件を多数の条文に盛り込むことで実現されている。実用的な（情報に関する）要件は、GDPR の第 12 条から第 14 条までに規定されている。しかしながら、情報の質、アクセスしやすさ及び理解しやすさは、透明性に関する情報の実際の内容と同程度に重要であり、これらはデータ主体のために確保されなければならない。

5. The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This is clear from Article 12 which provides that transparency applies at the following stages of the data processing cycle:

---

[10] See, for example, the Opinion of Advocate General Cruz Villalon (9 July 2015) in the Bara case (Case C-201/14) at paragraph 74: “the requirement to inform the data subjects about the processing of their personal data, which guarantees transparency of all processing, is all the more important since it affects the exercise by the data subjects of their right of access to the data being processed, referred to in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive”.

例えば、Bara 事件（Case C-201/14）における Cruz Villalon 法務官の意見（2015 年 7 月 9 日 9 日）74 項を参照。「*全ての取扱いの透明性を保証する、それぞれの個人データの取扱いについてデータ主体に通知するという要件は、指令第 95/46 号の第 12 条の規定する、取り扱われているデータへのアクセス権と、同指令の第 14 条の規定する、そうしたデータの取扱いに異議を述べる権利のデータ主体による行使に影響を及ぼすため、さらに重要である*」。

5. GDPR の透明性に関する要件は、取扱いの全サイクルにわたって、取扱いの法的根拠にかかわらず、適用される。このことは、データの取扱いのサイクルのうち、以下の段階のそれぞれに透明性が適用されると規定する第 12 条から明らかである。

- before or at the start of the data processing cycle, i.e. when the personal data is being collected either from the data subject or otherwise obtained;
  データを取扱うサイクルの開始前又は開始時、すなわち、個人データがデータ主体から収集されているか、又は他の方法で収集されているとき、

- throughout the whole processing period, i.e. when communicating with data subjects about their rights; and
  取扱いの期間全体、すなわちデータ主体の権利についてそのデータ主体に連絡する間、及び

- at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing.
  取扱いが進められている特定の時点、例えばデータ侵害が発生した場合や取扱いに対する重大な変更が生じた場合など。

The meaning of transparency
透明性の意味

6. Transparency is not defined in the GDPR. Recital 39 of the GDPR is informative as to the meaning and effect of the principle of transparency in the context of data processing:
6. 透明性は GDPR では定義されていない。GDPR の前文第 39 項は、データの取扱いとの関係における透明性の原則の意味と効果に対する示唆に富んでいる。

"It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…"
「自然人に関する個人データが収集され、利用され、調査され、又は、それら以外の取扱い

をされていること、及び、どの範囲の個人データが取扱われており、又は、取扱われることになるのかが、当該自然人に対して明らかにされなければならない。透明性の原則は、それらの個人データの取扱いと関連する情報及びコミュニケーションに容易にアクセスできること及び容易に理解できること、また、明確かつ平易な文言が用いられることを求める。この基本原則は、特に、データ主体に対する管理者の識別名及び取扱いの目的の情報、並びに、関係する自然人に関する公正かつ透明性のある取扱いを確保し、そして、取扱われている自然人に関する個人データの確認及びコミュニケーションを得る当該自然人の権利を確保するためのさらなる情報と関係している。」。

Elements of transparency under the GDPR
GDPR に基づく透明性の要素

7. The key articles in relation to transparency in the GDPR, as they apply to the rights of the data subject, are found in Chapter III (Rights of the Data Subject). Article 12 sets out the general rules which apply to: the provision of information to data subjects (under Articles 13 - 14); communications with data subjects concerning the exercise of their rights (under Articles 15 - 22); and communications in relation to data breaches (Article 34). In particular Article 12 requires that the information or communication in question must comply with the following rules:
7. GDPR における透明性に関する主要な条文であって、データ主体の権利に適用されるものは、第 III 章（データ主体の権利）に規定されている。第 12 条は、以下に適用される一般的ルールを定めている。すなわち、データ主体への情報提供（第 13 条～第 14 条に基づく）、それぞれの権利行使に関するデータ主体との連絡（第 15 条～第 22 条に基づく）、データ侵害に関する連絡（第 34 条）である。特に第 12 条では、問題となる情報又は通知が以下のルールに従って行われることを要求している。

- it must be concise, transparent, intelligible and easily accessible (Article 12.1);
  簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式でなければならず（第 12 条(1)）、

- clear and plain language must be used (Article 12.1);
  明瞭かつ平易な文言が使われなければならず（第 12 条(1)）、

- the requirement for clear and plain language is of particular importance when providing information to children (Article 12.1);
  子どもに情報を提供する際は、明瞭かつ平易な文言という要件が特に重要であり（第 12 条(1)）、

- it must be in writing“*or by other means, including where appropriate, by electronic means*”(Article 12.1);
  書面で、「*又は適切であるときは電子的な手段を含めその他の方法によら*」なければならず（第 12 条(1)）、

- where requested by the data subject it may be provided orally (Article 12.1) ; and
  データ主体によって要求された場合は、口頭で提供することができ（第 12 条(1)）、

- it generally must be provided free of charge (Article 12.5).
  一般に無償で提供されなければならない（第 12 条(5)）。

“Concise, transparent, intelligible and easily accessible”
「簡潔で、透明性があり、理解しやすく、容易にアクセスできる」

8. The requirement that the provision of information to, and communication with, data subjects is done in a “concise and transparent” manner means that data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues.
8. データ主体への情報提供と連絡が「簡潔かつ透明性がある」方法で行われるという要件は、情報疲労を避けるために情報管理者が情報／通知を効率的かつ簡潔に提示すべきであることを意味する。この情報は、契約条項や一般的な利用規約など、他の非プライバシー関連情報とは明確に区別できるものとすべきである。オンラインの文脈では、階層的なプライバシーステートメント／プライバイシー通知を用いることにより、データ主体が、特定の事項について検索するために大量のテキストをスクロールすることを要せず、プライバシーステートメント／プライバシーノーティスのアクセスしたい箇所を直ちに表示できるようになる。

9. The requirement that information is “intelligible” means that it should be understood by an average member of the intended audience. Intelligibility is closely linked to the requirement to use clear and plain language. An accountable data controller will have knowledge about the people they collect information about and it can use this knowledge to determine what that audience would likely

understand. For example, a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children. If controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/ notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things.

9. 情報が「理解しやすい」という要件は、対象とする情報の受け手のうちの平均的な人々に理解されるものであることを意味する。理解しやすさは、明瞭かつ平易な文言の使用という要件と密接に関連している。アカウンタビリティを満たしているデータ管理者であれば、情報収集の対象者に関する知識があるはずであり、その知識を使って、どのように説明すればその受け手に理解してもらえるかを判断できるはずである。例えば、就労経験者の個人データを収集する管理者であれば、子どもの個人データを取得する管理者よりも、自らの情報の受け手が高い理解力を有すると想定してもよい。管理者が情報の理解しやすさや透明性の度合い、また、ユーザーインターフェイス／通知／ポリシーなどの有効性について確信できない場合、ユーザーによる公開討論、可読性テスト、適切な場合は特に業界団体、消費者擁護団体、規制当局との公式及び非公式のやりとりや対話などの仕組みを通じて試験を行うことができる。

10. A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR and indeed is linked to Recital 39 which states that "*[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data...*" In particular, for complex, technical or unexpected data processing, WP29's position is that, as well as providing the prescribed information under Articles 13 and 14 (dealt with later in these guidelines), controllers should also separately spell out in unambiguous language what the most important *consequences* of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data.

10. 本規定で概説された透明性の原則における中心的な検討事項は、データ主体が、取扱い

の範囲と結果がどのようなものであるかを事前に判断できなければならず、自らの個人データの使途に関し、後の時点で不意をつかれるようなことがあってはならないということである。また、これは、GDPR 第 5 条(1)に基づく公正性の原則の重要な側面であり、実際にも、「*自然人は、個人データの取扱いと関連するリスク、ルール、保護措置及び権利・・・について、知らされなければならない。*」と述べる前文第 39 項と連動している。特に、複雑なデータ、技術的データ、又は予期せぬデータの取扱いの場合、第 29 条作業部会が示している見解は、管理者が、第 13 条及び第 14 条（本ガイドラインの後半で扱う）で指定する情報を提供するだけでなく、取扱いによる最も重大な*結果*としてどのようなものが生じるのかを、明瞭な文言で別途明記すべきだというものである。すなわち、プライバシーステートメント／プライバシーノーティスで具体的に記載した取扱いのために、データ主体が実際に被る影響とはどのようなものなのかについて明記するということである。データ管理者は、アカウンタビリティの原則に従い、また、前文第 39 項に沿って、この種の取扱いに関わる自然人にとってのリスクとなりデータ主体に通知するべきものが存在するかどうかを評価すべきである。これは、データ主体の個人データの保護に関連して、その基本的な権利と自由に最も大きな影響を及ぼす可能性のある取扱いの種類について概要を示すのに資することとなる。

11. The “easily accessible” element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/ notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc. These mechanisms are further considered below, including at paragraphs 33 to 40).

11. 「容易にアクセスできる」要素とは、データ主体が情報を探す必要がないことを意味する。例えば、彼らに直接的に提示したり、それをリンクしたり、それを明示的に告示したり、/自然言語による質問への回答としてなど、その情報にどこでどのようにアクセスできるかが一目瞭然であるべきである（例を挙げるならば、オンラインでの階層的なプライバシーステートメント/プライバシーノーティス、FAQ（よくある質問）、データ主体がオンラインフォームに記入した時に起動するようコンテキストで関連付けられたポップアップ、又はインタラクティブなデジタル環境においてはチャットボット・インターフェースを通じたインタラクティブなデジタル環境においてなど。これらのメカニズムについては、以下 33 項から 40 項においてさらに検討する）。

Example **例**

Every organisation that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as “Privacy”, “Privacy Policy” or “Data Protection Notice”). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.
ウェブサイトを開設している全ての組織が、ウェブサイト上にプライバシーステートメント／プライバシーノーティスを公表するべきである。このプライバシーステートメント／プライバシーノーティスへの直リンクは、（「プライバシー」、「プライバシーポリシー」、「データ保護通知」などの）一般的に使われている用語を使用し、そのウェブサイトの各ページにおいて明瞭に視認できるようにするべきである。テキストやリンクを目立たなくするか、ウェブページ上で見つけ難くするような配置や配色は、容易にアクセスしうるものとはみなされない。

For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than “two taps away” (e.g. by including a “Privacy”/ “Data Protection” option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.
アプリの場合、ダウンロードする前にオンラインストアからも必要な情報を入手できるようにするべきである。アプリがインストールされた後も、アプリ内から情報に容易にアクセスできる必要がある。この要件を満たす一つの方法は、/情報が表示されるまでに確実に「2 タップ」以上必要とされないようにすることである（例えばアプリのメニュー機能に「プライバシー」／「データ保護」オプションを含めるなど）。さらに、当該プライバシー情報は、そのアプリに固有のものでなければならず、アプリを所有する又は公開している企業の単なる包括的なプライバシーポリシーであってはならない。

WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected.
第 29 条作業部会では、個人データをオンラインで収集する時点で、プライバシーステートメント／プライバシーノーティスへのリンクを貼っておくか、又は個人データを収集するのと同じページにその情報を表示することを最も望ましい慣行として勧告している。

"Clear and plain language"
「明瞭かつ平易な文言」

12. With *written* information (and where written information is delivered orally, or by audio/ audiovisual methods, including for vision-impaired data subjects), best practices for clear writing should be followed[11]. A similar language requirement (for "plain, intelligible language") has previously been used by the EU legislator[12] and is also explicitly referred to in the context of consent in Recital 42 of the GDPR[13]. The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.

12. *書面に記載された*情報の場合（及び書面に記載された情報が口頭で又は視覚障害のあるデータ主体向けを含むオーディオ方式／オーディオビジュアル方式によって提供されている場合）、明瞭に記載するうえで最も望ましい慣行に従うべきである[11]。（「平易かつ理解しやすい文言」と）類似の文言に関する要件はこれまでも EU の立法者によって使われており[12]、GDPR の前文第 42 項の同意の文脈で明示的に言及されている[13]。明瞭かつ平易な文言の要件は、複雑な文章や文言の構造を避け、できるだけ単純な方法で情報を提供すべきであることを意味する。情報は具体的かつ明示的なものであるべきであり、抽象的又は相反的な言葉で表現されるべきではなく、異なる解釈の余地を残すものであってはならない。特に、個人データを取扱う目的とその法的根拠を明確にするべきである。

Poor Practice Examples
推奨されない慣行の例

The following phrases are not sufficiently clear as to the purposes of processing:

[11] See How to Write Clearly by the European Commission (2011), to be found at: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.
欧州委員会による How to Write Clearly (2011)（https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5 で閲覧できる）を参照。

[12] Article 5 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts
消費者契約の不公正な条件に関する 1993 年 4 月 5 日の理事会指令第 93/13/EEC 号の第 5 条。

[13] Recital 42 states that a declaration of consent pre-formulated by a data controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.
前文第 42 項では、管理者によって事前に書式化された同意の宣言は、理解しやすく、容易にアクセスできる方式により、明確かつ平易な文言を用いて示されなければならず、かつ、不公正な条件を含むものであってはならないと述べられている。

以下のような表現では、取扱いの目的が十分に明瞭ではない。

- "*We may use your personal data to develop new services*" (as it is unclear what the "services" are or how the data will help develop them);
  「*新しいサービスを開発するためにお客様の個人データを利用する場合があります*」（「サービス」とは何か、データがサービスを開発するのにどう役立つかが不明瞭であるため）、

- "*We may use your personal data for research purposes*" (as it is unclear what kind of "research" this refers to); and
  「*研究目的でお客様の個人データを利用する場合があります*」（どのような「研究」を指しているのかが不明瞭であるため）、及び

- "*We may use your personal data to offer personalized services*" (as it is unclear what the "personalisation" entails).
  「*パーソナライズされたサービスを提供するためにお客様の個人データを利用する場合があります*」（「パーソナライゼーション」が何を意味するのかが不明瞭であるため）。

Good Practice Examples[14]
望ましい慣行の例 [14]

- "*We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in*" (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);
  「*お客様が興味を持つと思われる他の製品を提案するために購買履歴を保管し、過去に購入した製品の詳細な情報を利用します*」（どのような種類のデータが取り扱われるのかということ、データ主体が製品の広告の対象となること、及びそのデータがこれを可能にするために利用されることが明瞭である）、

- "*We will retain and evaluate information on your recent visits to our website and how you*

[14] The requirement for transparency exists entirely independently of the requirement upon data controllers to ensure that there is an appropriate legal basis for the processing under Article 6.
透明性の要件は、取扱いのための適切な法的根拠が存在するよう確保することをデータ管理者に求める第 6 条に基づく要件とは全く独立して存在する。

move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive" (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and
「人々が*当社ウェブサイトをどのように利用しているかを理解し、当社ウェブサイトをより直感的に利用できるものにするという分析を行う目的で、お客様による当社ウェブサイトへの最近のアクセスと、当社ウェブサイトの中のさまざまなページをどのように移動したかに関する情報を保持し、評価します*」（どのようなタイプのデータが取扱われ、どのようなタイプの分析を管理者が今後行うかが明瞭である）、及び

- "*We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read*" (it is clear what the personalization entails and how the interests attributed to the data subject have been identified).
「*お客様がクリックしたウェブサイト上の記事に関する記録を保管し、お客様が読んだ記事に基づいて識別したお客様の関心に沿って、当ウェブサイト上の広告を絞り込むためにその情報を利用します*」（パーソナライゼーションが何を意味し、データ主体の関心をどう識別したかが明瞭である）。

13. Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing. Paragraphs and sentences should be well structured, utilizing bullets and indents to signal hierarchical relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the second language(s) so that the translated text does not have to be deciphered or re-interpreted. (A translation in one or more other languages should be provided where the controller targets[15] data subjects

[15] For example, where the controller operates a website in the language in question and/or offers specific country options and/or facilitates the payment for goods or services in the currency of a particular member state then these may be indicative of a data controller targeting data subjects of a particular member state.
例えば、管理者がウェブサイトを当該言語で運営する、及び／又は特定の加盟国の通貨による商品又はサービスの支払いについて当該国特有の選択肢を提供する、及び／又は特定の加盟国の通貨による支払いを容易にする場合、これは、データ管理者が、当該加盟国のデータ主体を対象としていることを示唆する可能性がある。

speaking those languages.)

13. 「may（可能性がある）」、「might（かもしれない）」、「some（ある程度）」、「often（しばしば）」及び「possible（ありうる）」などの修飾語も避けるべきである。データ管理者が曖昧な表現を利用する場合には、アカウンタビリティの原則に従い、そのような表現を利用せざるを得ない理由とそれによって取扱いの公正さが損なわれない理由を証明できる必要がある。階層関係を示すため、文頭の中黒や字下げを利用し、段落と文章の構成を適切に行うべきである。文体は受動態ではなく能動態にし、余分な名詞の使用は避けるべきである。データ主体に提供される情報には、過度に法律的、技術的又は専門的な表現又は用語を含めるべきではない。情報を他の一つの又は複数の言語に翻訳する場合、データ管理者は確実に、全ての翻訳が正確であること、及び翻訳されたテキストを解読又は再翻訳する必要がないよう、表現及び構文がその言語で意味をなすようにするべきである。（管理者がこれらの他の言語を話すデータ主体を対象としている [15] 場合、その一つの又は複数の言語の翻訳を提供するべきである）。

Providing information to children and other vulnerable people

子どもやその他の弱い立場にいる人々に情報を提供する

14. Where a data controller is targeting children[16] or is, or should be, aware that their goods/ services are particularly utilized by children (including where the controller is relying on the consent of the child) [17], it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognizes that the message/ information is being directed at them[18]. A useful example of child-centred language used as an

[16] The term “child” is not defined under the GDPR, however WP29 recognises that, in accordance with the UN Convention on the Rights of the Child, which all EU Member States have ratified, a child is a person under the age of 18 years. 17

GDPR では「子ども」という用語を定義していないものの、第 29 条作業部会では、全ての EU 加盟国が批准している国連児童の権利に関する条約に従い、18 歳未満の者を子どもであると認識している。

[17] i.e. children of 16 years or older (or, where in accordance with Article 8.1 of the GDPR Member State national law has set the age of consent at a specific age between 13 and 16 years for children to consent to an offer for the provision of information society services, children who meet that national age of consent).

すなわち、16 歳以上の子どもたち（又は、加盟国が、GDPR の第 8 条(1)に従い、子どもたちが情報社会サービスの提供の申し込みに同意できる同意年齢を国内法により 13 歳から 16 歳までの特定の年齢に設定している場合には、その国における同意年齢を満たす子どもたち）。

[18] Recital 38 states that “Children merit special protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data”. Recital 58 states that “Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand”.

前文第 38 項では、「子どもは、個人データの取扱いと関連するリスク、結果及び関係する保護措置、並びに、自らの権利について十分に認識できないかもしれないため、その個人データに関して特別の保護を享受する。」と述べている。前文第 58 項では、「子どもが特別の保護を享受することに鑑み、取扱いが子ども向けのものであるときは、いかなる情報及び連絡も、子どもが容易に理解することのできるような明確かつ平易な文言によるものでなければならない。」と述べている。

alternative to the original legal language can be found in the “UN Convention on the Rights of the Child in Child Friendly Language” [19].

14.子ども [16] を対象としているか、又はその商品／サービスが特に子どもによって利用されていることをデータ管理者が認識している若しくは認識すべき場合（管理者が子ども [17] の同意に依拠している場合を含む）、情報の受け手である子どもが、メッセージ／情報が自らに向けられたものであると認識できるようにするために、適切かつ子どもの心に響く語彙、調子、文体で表現されるようにしなければならない [18]。「国連の児童向けの表現についての児童の権利に関する条約」において、元の法律的な表現の代わりに、子ども向けの表現に関して有用な例が示されている [19]。

15. WP29’s position is that transparency is a free-standing right which applies as much to children as it does to adults. WP29 emphasises in particular that children do not lose their rights as data subjects to transparency simply because consent has been given/ authorized by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies. While such consent will, in many cases, be given or authorized on a once-off basis by the holder of parental responsibility, a child (like any other data subject) has an ongoing right to transparency throughout the continuum of their engagement with a data controller. This is consistent with Article 13 of the UN Convention on the Rights of the Child which states that a child has a right to freedom of expression which includes the right to seek, receive and impart information and ideas of all kinds[20]. It is important to point out that, while providing for consent to be given on behalf of a child when under a particular age, [21] Article 8 *does not provide* for transparency measures to be directed at the holder of parental responsibility who gives such consent.

15. 第 29 条作業部会は、透明性が大人と同様子どもにも適用される独立した権利であるとの見解である。第 29 条作業部会は、特に、GDPR 第 8 条が適用される状況において、子どもに対する保護責任を有する者から同意又は許可を得たことのみを理由に、子どもたちが透明性に対するデータ主体としての権利を失わないことを強調する。子どもに対する保護責任を有する者による同意又は許可というものは、その場限りのものであることが大半ではあるが、子どもには（他のデータ主体の場合と同様）データ管理者と関わる全期間を通して継続的な権利がある。これは、子どもが、表現の自由についての権利を有しており、その

[19] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

[20] Article 13 of the UN Convention on the Rights of the Child states that: “The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child’s choice.”

国連の児童の権利に関する条約第 13 条は以下のように述べる。「児童は、表現の自由についての権利を有する。この権利には、口頭、手書き若しくは印刷、芸術の形態又は自ら選択する他の方法により、国境とのかかわりなく、あらゆる種類の情報及び考えを求め、受け、及び伝える自由を含む」。

[21] See footnote 17 above.

上記の脚注 17 を参照。

権利には、あらゆる種類の情報及び考えを求め、受け、及び伝える自由が含まれていると規定する国連の児童の権利に関する条約第 13 条とも一致している[20]。第 8 条では、一定の年齢未満の子どものために同意を与える場合について規定する[21]一方、そのような同意を与える保護責任を有する者に対しては、透明性に関する措置を講ずるよう*規定していない*点を指摘することは重要である。

Therefore, data controllers have an obligation in accordance with the specific mentions of transparency measures addressed to children in Article 12.1 (supported by Recitals 38 and 58) to ensure that where they target children or are aware that their goods or services are particularly utilized by children of a literate age, that any information and communication should be conveyed in clear and plain language or in a medium that children can easily understand. For the avoidance of doubt however, WP29 recognises that with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency.
したがって、データ管理者には、第 12 条(1)の子どもを対象とする（前文第 38 項及び第 58 項により裏付けられている）透明性に関する措置への具体的な言及に従って、子どもを対象とする場合又は特に読み書きのできる年齢の子どもたちによってその商品／サービスが利用されていることを認識している場合に、あらゆる情報及び連絡が、明瞭かつ平易な文言で、又は子どもが容易に理解しうる媒体で伝達されるよう確保する義務がある。しかしながら、疑問の余地をなくすため、第 29 条作業部会では、極めて幼いか又は読み書きができる年齢に達していない子どもたちの場合、そのような子どもたちは書面又は書面以外の方法による透明性に関する最も基本的なメッセージでさえ理解できない場合が大半である点を考慮し、子どもに対する保護責任を有する者も対象に透明性に関する措置を講じることがありうると認識している。

16. Equally, if a data controller is aware that their goods/ services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects[22]. This relates to the need for a data controller to assess its audience's likely level of understanding, as discussed above at paragraph 9.
16. 同様に、障害を持つ人々又は情報へのアクセスが困難な人々を含む、社会において他の弱い立場にいる人々が商品／サービスを利用していることを認識している（又はこれらの

[22] For example, the UN Convention on the Rights of Persons with Disabilities requires that appropriate forms of assistance and support are provided to persons with disabilities to ensure their access to information.
例えば、国連障害者の権利に関する条約では、障害者が情報を利用する機会を得られるようにするため、障害者に対する他の適当な形態の援助及び支援を促進するよう求めている。

人々を対象としている）場合、データ管理者は、そのようなデータ主体に関連して自らの透明性に関する義務をどのようにして遵守することを確保するかについて評価する際に、そのようなデータ主体の脆弱性を考慮するべきである[22]。これは、9 項で議論したように、データ管理者が自らの閲覧者の理解力を推定し、評価する必要性とも関連している。

“In writing or by other means”

「書面で、又は他の手段によって」

17. Under Article 12.1, the default position for the provision of information to, or communications with, data subjects is that the information is in writing[23]. (Article 12.7 also provides for information to be provided in combination with standardized icons and this issue is considered in the section on visualization tools at paragraphs 49 to 53). However, the GDPR also allows for other, unspecified “means” including electronic means to be used. WP29’s position with regard to written electronic means is that where a data controller maintains (or operates, in part or in full, through) a website, WP29 recommends the use of layered privacy statements/ notices, which allow website visitors to navigate to particular aspects of the relevant privacy statement/ notice that are of most interest to them (see more on layered privacy statements/ notices at paragraph 35 to 37) [24]. However, the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (whether in a digital or paper format) which can be easily accessed by a data subject should they wish to consult the entirety of the information addressed to them. Importantly, the use of a layered approach is not confined only to written electronic means for providing information to data subjects. As discussed at paragraphs 35 to 36 and 38 below, a layered approach to the provision of information to data subjects may also be utilized by employing a combination of *methods* to ensure transparency in relation to processing.

17. 第 12 条(1)に基づきデータ主体に情報を提供する又は連絡を取る場合、その情報は書面で伝えられることが基本である[23]。（また、第 12 条(7)では、標準化された図形記号と組み合わせて情報を提供することを規定しており、この問題は、49 から 53 項の視覚化ツールに関する箇所で考察している）。しかしながら、GDPR では、電子的方法を含む他の不特定の「手段」も利用することを認めている。書面を電子的に提供する方法に関する第 29 条作業部会の見解としては、データ管理者がウェブサイトを開設している（又は活動の一部若しくは全

[23] Article 12.1 refers to “language” and states that the information shall be provided in writing, or by other means, including, where appropriate, by electronic means.
第 12 条第 1 項では「文言」に言及し、情報が書面で提供されるものとし、適切な場合、電子的方法を含め、その他の手段によって提供されると述べる。

[24] The WP29’s recognition of the benefits of layered notices has already been noted in Opinion 10/2004 on More Harmonised Information Provisions and Opinion 02/2013 on apps on smart devices.
第 29 条作業部会では、既に情報規定の追加的調和に関する意見第 10/2004 号及びスマートデバイス上のアプリに関する意見第 02/2013 号において、階層的な通知の利点に関する自らの認識を述べている。

部をウェブサイトで行っている）場合、階層的なプライバシーステートメント／プライバシーノーティスを利用することで、ウェブサイトの訪問者がプライバシーステートメント／プライバシーノーティスのうち、それぞれにとって最も関心のある側面にたどり着ける仕組みにすることを勧告している（階層的なプライバシーステートメント／プライバシーノーティスの詳細については、35 から 37 項を参照）[24]。しかしながら、データ主体が自らに向けられた情報全体を確認したい場合に容易にアクセスできるよう、そうした情報全体を（デジタル形式であろうと紙の形式であろうと）一つの場所又は一つの完全な文書の形式でも提供しなければならない。階層的なアプローチの利用は、データ主体に情報を提供する上で書面を電子的に提供する方法にのみ限定されない点が重要である。以下の 35 から 36 項及び 38 項で論じているように、取扱いの透明性を確保する*方法*を組み合わせる場合にもデータ主体への情報提供に対する階層的なアプローチを利用できる可能性がある。

18. Of course, the use of digital layered privacy statements/ notices is not the only written electronic means that can be deployed by controllers. Other electronic means include “just-in-time” contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Non-written electronic means which may be used *in addition to* a layered privacy statement/ notice might include videos and smartphone or IoT voice alerts[25]. “Other means”, which are not necessarily electronic, might include, for example, cartoons, infographics or flowcharts. Where transparency information is directed at children specifically, controllers should consider what types of measures may be particularly accessible to children (e.g. these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).

18. 当然ではあるが、階層的なデジタル形式のプライバシーステートメント／プライバシーノーティスが、書面を電子的に提供する上で管理者の採用できる唯一の方式ではない。他の電子的な方法には、「ジャストインタイム」の状況に応じたポップアップ通知、3D タッチ又はマウスオーバーによる通知、及びプライバシーダッシュボードなどが含まれる。階層的なプライバシーステートメント／プライバシーノーティス*に加えて*用いることができる、書面によらない電子的方法には、ビデオ、スマートフォン、又は IoT 音声アラートが含まれる可能性がある[25]。必ずしも電子的なものではない「その他の手段」には、例えば、一コマ漫画、インフォグラフィック又はフローチャートが含まれる可能性がある。特に透明性に関する情報を子どもに提供する場合、管理者は、（その他の手段の中でも例えば漫画／一コマ漫画、絵文字、アニメーションなど）特にどの種類の措置が子どもたちにとってアクセスし易いかを考慮するべきである。

[25] These examples of electronic means are indicative only and data controllers may develop new innovative methods to comply with Article 12.
これらの電子的方法の例は、単なる参考例であり、データ管理者は、第 12 条を遵守するための新しい革新的な方法を開発してもよい。

19. It is critical that the method(s) chosen to provide the information is/are appropriate to the particular circumstances, i.e. the manner in which the data controller and data subject interact or the manner in which the data subject's information is collected. For example, only providing the information in electronic written format, such as in an online privacy statement/ notice may not be appropriate/ workable where a device that captures personal data does not have a screen (e.g. IoT devices/ smart devices) to access the website/ display such written information. In such cases, appropriate alternative *additional* means should be considered, for example providing the privacy statement/ notice in hard copy instruction manuals or providing the URL website address (i.e. the specific page on the website) at which the online privacy statement/ notice can be found in the hard copy instructions or in the packaging. Audio (oral) delivery of the information could also be additionally provided if the screenless device has audio capabilities. WP29 has previously made recommendations around transparency and provision of information to data subjects in its Opinion on Recent Developments in the Internet of Things[26] (such as the use of QR codes printed on internet of things objects, so that when scanned, the QR code will display the required transparency information). These recommendations remain applicable under the GDPR.

19. 情報を提供するために選択した 1 つ又は複数の方法が、その状況、すなわちデータ管理者とデータ主体がやりとりをする方法、又はデータ主体の情報を収集する方法に適していることが極めて重要である。例えば、個人データを取得するデバイスに、ウェブサイトにアクセスするための画面／書面による情報を表示するための画面がない（例えば IoT デバイスやスマートデバイスなどの）場合には、オンラインによるプライバシーステートメント／プライバシーノーティスなどの電子文書の形式でのみ情報を提供することが適切ではない／可能ではない場合がある。そのような場合には、例えば、ハードコピーの取扱説明書にプライバシーステートメント／プライバシーノーティスを記載するか、又はプライバシーステートメント／プライバシーノーティスをオンラインで掲示しているウェブサイト（すなわちウェブサイトの当該ページ）の URL を、ハードコピーの取扱説明書又はパッケージに表示するなど、適切な代替的かつ*追加的*手段を考慮するべきである。スクリーンを持たないデバイスに音声機能が存在する場合に、併せて音声（口頭）形式の情報も配信してよい。第 29 条作業部会では、モノのインターネット（IoT）の最近の動向に関する意見 [26] において、（スキャンした際に QR コードにより必要な透明性情報が表示されるよう QR コードを IoT 機器に印刷するなど）透明性とデータ主体への情報提供に関する勧告をこれまでも行ってきた。これらの勧告は、GDPR の下でも引き続き適用される。

[26] WP29 Opinion 8/2014 adopted on 16 September 2014
2014 年 9 月 16 日に採択された第 29 条作業部会意見第 8/2014 号。

"..the information may be provided orally"
「情報は口頭で提供してもよい」

20. Article 12.1 specifically contemplates that information may be provided orally to a data subject on request, provided that their identity is proven by other means. In other words, the means employed should be more than reliance on a mere assertion by the individual that they are a specific named person and the means should enable the controller to verify a data subject's identity with sufficient assurance. The requirement to verify the identity of the data subject before providing information orally only applies to information relating to the exercise by a specific data subject of their rights under Articles 15 to 22 and 34. This precondition to the provision of oral information cannot apply to the provision of general privacy information as outlined in Articles 13 and 14, since information required under Articles 13 and 14 must also be made accessible to *future users*/ customers (whose identity a data controller would not be in a position to verify). Hence, information to be provided under
20. 第 12 条(1)では、特にデータ主体の身元が他の手段によって証明されていれば、その要求に応じてデータ主体に情報を口頭で提供してもよいと考えている。言い換えれば、身元確認手段は、相手が自らの名前を名乗ったのみでは不十分であり、管理者がデータ主体の身元を十分な確証を得られる程度に検証できるものとするべきである。情報を口頭で提供する前にデータ主体の身元を確認するという要件は、そのデータ主体による第 15 条から第 22 条まで及び第 34 条に基づく権利の行使に関連する情報にのみ適用される。この口頭情報を提供するための前提条件は、第 13 条及び第 14 条に概説される一般的なプライバシー情報の提供には適用されない。その理由は、第 13 条及び第 14 条に基づき要求される情報は、（データ管理者がその身元を確認できる立場にない）*将来のユーザー／*顧客もアクセスしうるものでなければならないためである。したがって、

Articles 13 and 14 may be provided by oral means without the controller requiring a data subject's identity to be proven.
第 13 条及び第 14 条に基づき提供される情報は、データ管理者がデータ主体の身元の証明を要求することなく、口頭で提供することができる。

21. The oral provision of information required under Articles 13 and 14 does not necessarily mean oral information provided on a person-to-person basis (i.e. in person or by telephone). Automated oral information may be provided in addition to written means. For example, this may apply in the context of persons who are visually impaired when interacting with information society service providers, or in the context of screenless smart devices, as referred to above at paragraph 19. Where a data controller has chosen to provide information to a data subject orally, or a data subject requests the provision of oral information or communications, WP29's position is that the data controller should allow the data

subject to re-listen to pre-recorded messages. This is imperative where the request for oral information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information in written format. The data controller should also ensure that it has a record of, and can demonstrate (for the purposes of complying with the accountability requirement): (i) the request for the information by oral means, (ii) the method by which the data subject's identity was verified (where applicable – see above at paragraph 20) and (iii) the fact that information was provided to the data subject.

21. 第 13 条及び第 14 条に基づき必要とされる情報の口頭による提供は、必ずしも個人対個人の（すなわち、対面又は電話による）口頭での情報提供を意味するものではない。書面による手段に加えて自動化された方法で口頭情報を提供してもよい。例えば、これは、視覚障害者が情報社会サービス提供者と対話する場合又は上記 19 項で述べたスクリーンを持たないスマートデバイスの場合にあてはまる可能性がある。データ管理者がデータ主体に口頭で情報を提供することを選択した場合、又はデータ主体が口頭による情報提供又は連絡を要求した場合、データ管理者は、データ主体があらかじめ録音されたメッセージを繰り返し聞けるようにするべきだというのが第 29 条作業部会の見解である。特に、視覚障害のあるデータ主体又は書面形式での情報にアクセスすること若しくはそれを理解するのが困難な他のデータ主体が口頭による情報提供を要求している場合にはそれが必須である。また、データ管理者は、（アカウンタビリティの要件を遵守するために）次の内容を記録し、それを証明できるよう確保すべきである。すなわち、(i) 口頭の手段による情報の要求、(ii) データ主体の身元を確認した方法（該当する場合には、上記の 20 項を参照）及び(iii) データ主体に情報を提供したという事実の三点である。

"Free of charge"

「無償で」

22. Under Article 12.5, [27] data controllers cannot generally charge data subjects for the provision of information under Articles 13 and 14, or for communications and actions taken under Articles 15 - 22 (on the rights of data subjects) and Article 34 (communication of personal data breaches to data subjects) [28]. This aspect of transparency also means that any information provided under the

[27] This states that "Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge."

ここでは、「第 13 条及び第 14 条に基づき提供される情報及び第 15 条から第 22 条まで及び第 34 条に基づき行われるあらゆる連絡及び措置は無償で提供されるものとする」と述べられている。

[28] However, under Article 12.5 the controller may charge a reasonable fee where, for example, a request by a data subject in relation to the information under Article 13 and 14 or the rights under Articles 15 - 22 or Article 34 is excessive or manifestly unfounded. (Separately, in relation to the right of access under Article 15.3 a controller may charge a reasonable fee based on administrative costs for any further copy of the personal data which is requested by a data subject).

しかしながら、管理者は、第 12 条第 5 項に基づき、例えば、第 13 条及び第 14 条に基づく情報又は第 15 条から第 22 条まで若しくは第 34 条に基づく権利に関係するデータ主体の請求が過度であるか、又は

transparency requirements cannot be made conditional upon financial transactions, for example the payment for, or purchase of, services or goods[29].

22. データ管理者は、第 12 条(5)に基づき [27]、一般にデータ主体に対し、第 13 条及び第 14 条に基づく情報の提供、又は（データ主体の権利に関する）第 15 条から第 22 条及び（データ主体への個人データ侵害の伝達に関する）第 34 条に基づく連絡又は行為についてその料金を請求することができない [28]。透明性のこの側面は、透明性の要件に基づき提供される情報が、サービスや商品への支払いやその購入など、金銭的取引をそのための条件とできないことも意味する [29]。

Information to be provided to the data subject – Articles 13 & 14
データ主体に提供される情報 - 第 13 条及び第 14 条

Content

内容

23. The GDPR lists the categories of information that must be provided to a data subject in relation to the processing of their personal data where it is collected from the data subject (Article 13) or obtained from another source (Article 14). The table in the Annex to these guidelines summarises the categories of information that must be provided under Articles 13 and 14. It also considers the nature, scope and content of these requirements. For clarity, WP29's position is that there is no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively. All of the information across these sub-articles is of equal importance and must be provided to the data subject.

23. GDPR では、データ主体から情報を収集する場合（第 13 条）又は別の情報源から取得される場合（第 14 条）に個人データの取扱いに関連してデータ主体に提供しなければならない種類の情報を列挙している。本ガイドラインの附属書にある表は、第 13 条及び第 14 条に基づき提供しなければならない種類の情報をまとめたものである。また、この表では、こ

明らかに根拠がない場合には、これに合理的な料金を請求することができる。（これとは別に、第 15 条第 3 項に基づくアクセス権に関連して、管理者は、データ主体から要求された個人データの追加的な複製について、管理コストに基づいた合理的な料金を請求することができる）。

[29] By way of illustration, if a data subject's personal data is being collected in connection with a purchase, the information which is required to be provided under Article 13 should be provided prior to payment being made and at the point at which the information is being collected, rather than after the transaction has been concluded. Equally though, where free services are being provided to the data subject, the Article 13 information must be provided prior to, rather than after, sign-up given that Article 13.1 requires the provision of the information "at the time when the personal data are obtained".

一例として、購入に関連してデータ主体の個人データを収集している場合、第 13 条に基づき提供されるべき情報は、取引が終了した後ではなく、支払いが行われる前及び情報が収集される時点で提供されるべきである。同様に、データ主体に無償サービスを提供している場合も、第 13 条第 1 項において「個人データを取得する際」に情報を提供するよう求めている点を考慮すると、登録後ではなく登録前に第 13 条の情報を提供しなければならない。

れらの要件の性質、範囲及び内容も検討している。ここで明確にしておくために述べておくならば、第 13 条と第 14 条のそれぞれ第 1 項に基づき提供されなければならない情報と第 2 項に基づき提供されなければならない情報との間に差異がないというのが第 29 条作業部会の見解である。これらの各項の情報はいずれも同程度の重要性を備え、これをデータ主体に提供しなければならない。

“Appropriate measures”
「適切な措置」

24. As well as content, the form and manner in which the information required under Articles 13 and 14 should be provided to the data subject is also important. The notice containing such information is frequently referred to as a data protection notice, privacy notice, privacy policy, privacy statement or fair processing notice. The GDPR does not prescribe the format or modality by which such information should be provided to the data subject but does make it clear that it is the data controller’s responsibility to take “appropriate measures” in relation to the provision of the required information for transparency purposes. This means that the data controller should take into account all of the circumstances of the data collection and processing when deciding upon the appropriate modality and format of the information provision. In particular, appropriate measures will need to be assessed in light of the product/ service user experience. This means taking account of the device used (if applicable), the nature of the user interfaces/ interactions with the data controller (the user “journey”) and the limitations that those factors entail. As noted above at paragraph 17, WP29 recommends that where a data controller has an online presence, an online layered privacy statement/ notice should be provided.
24. 第 13 条及び第 14 条に基づけば、データ主体に提供するべき情報の内容だけでなく、その形式及び方法も重要である。このような情報を含む通知は、データ保護通知、プライバシーノーティス、プライバシーポリシー、プライバシーステートメント又は公正取扱通知と呼ばれる場合が多い。GDPR では、そのような情報をデータ主体に提供すべき形式又は手続を規定していないものの、透明性を確保する目的で、必要な情報の提供に関して「適切な措置」を講ずる責任がデータ管理者にある点については明確にされている。これは、データ管理者が、情報提供の適切な手続とフォーマットを決定する際に、データの収集及び取扱いを取り巻く一切の状況を考慮に入れるべきであることを意味する。特に、製品/サービスのユーザーの経験値を考慮して、適切な措置を評価する必要がある。これは、使われるデバイス（該当する場合）、ユーザーインターフェイス／データ管理者との相互作用の性質（ユーザー「遍歴」）、及びこれらの要因に伴う制限を考慮に入れることを意味する。上記 17 項で述べたように、第 29 条作業部会では、データ管理者がオンラインで活動している場合、オンラインの階層的なプライバシーステートメント／プライバシーノーティスを提供すべきことを勧告している。

25. In order to help identify the most appropriate modality for providing the information, in advance of “going live”, data controllers may wish to trial different modalities by way of user testing (e.g. hall tests, or other standardized tests of readability or accessibility) to seek feedback on how accessible, understandable and easy to use the proposed measure is for users. (See also further comments above on other mechanisms for carrying out user testing at paragraph 9). Documenting this approach should also assist data controllers with their accountability obligations by demonstrating how the tool/ approach chosen to convey the information is the most appropriate in the circumstances.
25. 「正式なサービスの開始」前の段階で、情報を提供するための最も適切な手続の特定に資するために、データ管理者は、さまざまな方式を試みて、ユーザーテスト（例えば会場テストや、又は読みやすさやアクセスしやすさに関係する他の標準化されたテストなど）を行い、自らが提案する手段がユーザーにとってどの程度アクセスしやすいか、どの程度理解しやすく、使いやすいかといったことに関してフィードバックを収集することを考えるかもしれない（ユーザーテストを実施するための他の仕組みに関する上記 9 項のコメントも参照）。また、このアプローチの文書化は、データ管理者が、情報を伝達するうえで自らが選択したツール／アプローチがその状況において最も適切なものであることを証明することで、アカウンタビリティに関する義務の履行を助けるものである。

Timing for provision of information
情報提供のタイミング

26. Articles 13 and 14 set out information which must be provided to the data subject at the commencement phase of the processing cycle[30]. Article 13 applies to the scenario where the data is collected from the data subject. This includes personal data that:
26. 第 13 条及び第 14 条は、取扱いのサイクルが開始される段階でデータ主体に提供しなければならない情報を規定している [30]。第 13 条は、データ主体からデータが収集される場合に適用される。これには、以下の個人データが含まれる。

· a data subject consciously provides to a data controller (e.g. when completing an online form); or

[30] Pursuant to the principles of fairness and purpose limitation, the organisation which collects the personal data from the data subject should always specify the purposes of the processing at the time of collection. If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data, as well as the categories of the inferred data processed, must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose in compliance with Article 13.3 or Article 14.4.
公正性及び目的限定の原則に従い、データ主体から個人データを収集する組織は、常に収集時に取扱いの目的を明示するべきである。その目的に個人の推定データの作成が含まれる場合には、そのような個人の推定データを作成し、さらに取扱いをめぐって、意図している目的、並びに取扱う推定データの種類を、常に収集時、又は第 13 条（3）又は第 14 条（4）に従って、新たな目的のための追加的取扱いの前に、データ主体に連絡しなければならない。

データ主体がデータ管理者に意識的に提供するもの（例えば、オンラインフォームに記入した場合）、又は

- a data controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors).
  データ管理者が、（例えば、カメラ、ネットワーク機器、Wi-Fi トラッキング、RFID 又は他の種類のセンサなどの自動的にデータをキャプチャするデバイス又はデータキャプチャソフトウェアを使って）データ主体を観察することによって収集したもの。

Article 14 applies in the scenario where the data have not been obtained from the data subject. This includes personal data which a data controller has obtained from sources such as:
第 14 条は、データをデータ主体から得ていない場合に適用される。これには、データ管理者が個人データを以下の情報源から取得する場合が含まれる。

- third party data controllers;
  第三者のデータ管理者、

- publicly available sources;
  公開された情報源、

- data brokers; or
  データブローカー、又は

- other data subjects.
  他のデータ主体。

27. As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided "*at the time when personal data are obtained*". In the case of indirectly obtained personal data under Article 14, the timeframes within which the required information must be provided to the data subject are set out in Article 14.3 (a) to (c) as follows:
27. この情報の提供時期については、これを適時に提供することが、透明性の義務及び公正にデータを取扱う義務との関係で不可欠な要素である。第 13 条が適用される場合、第 13 条(1)に基づき、情報を「*個人データを取得する際*」に提供しなければならない。第 14 条に基

づき間接的に取得された個人データの場合、14 条(3)(a)～(c)では、必要な情報をデータ主体に提供しなければならない時期を次のように定めている。

- The general requirement is that the information must be provided within a "reasonable period" after obtaining the personal data and no later than one month, "*having regard to the specific circumstances in which the personal data are processed*" (Article 14.3(a)).
  一般的な要件として、「*個人データが取扱われる具体的状況を考慮に入れ*」、個人データの取得後の「合理的期間」内、ただし、遅くとも 1 か月以内に情報を提供しなければならない（第 14 条(3)(a)）。

- The general one-month time limit in Article 14.3(a) may be further curtailed under Article 14.3(b), [31] which provides for a situation where the data are being used for communication with the data subject. In such a case, the information must be provided *at the latest* at the time of the first communication with the data subject. If the first communication occurs prior to the one-month time limit after obtaining the personal data, then the information must be provided *at the latest* at the time of the first communication with the data subject notwithstanding that one month from the point of obtaining the data has not expired. If the first communication with a data subject occurs more than one month after obtaining the personal data then Article 14.3(a) continues to apply, so that the Article 14 information must be provided to the data subject *at the latest* within one month after it was obtained.
- 第 14 条(3)(a)の一般的な 1 か月の期間は、個人データがデータ主体との連絡を取るために使われるような状況について規定する第 14 条(3)(b)[31] によりさらに短縮される場合がある。そのような場合、遅くとも最初にデータ主体に連絡した時点で情報を提供しなければならない。最初の連絡が、個人データの取得後 1 か月という期限内に行われる場合、データを取得した時点から 1 か月という期限に達していない場合でも、遅くともデータ主体と初めて連絡を取った時にこの情報を提供しなければならない。個人データを取得してから 1 か月以上経過した後にデータ主体と初めて連絡する場合、引き続き第 14 条(3)(a)が適用されるため、第 14 条情報の取得後遅くとも 1 か月以内にその情報をデータ主体に提供しなければならない。

- The general one-month time limit in Article 14.3(a) can also be curtailed under Article 14.3(c) [32]

[31] The use of the words "*if the personal data are to be used for..*" in Article 14.3(b) indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.
第 14 条(3)(b)における「*個人データが（中略）使われるならば*」という表現の使用は、第 14 条(3)(a)に規定する最大の期限を考慮した一般的な記述であるものの、それを置き換えるものではないことを示唆している。
[32] The use of the words "*if a disclosure to anther recipient is envisaged...*" in Article 14.3(c) likewise indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not

which provides for a situation where the data are being disclosed to another recipient (whether a third party or not) [33]. In such a case, the information must be provided at the latest at the time of the first disclosure. In this scenario, if the disclosure occurs prior to the one-month time limit, then the information must be provided at the latest at the time of that first disclosure, notwithstanding that one month from the point of obtaining the data has not expired. Similar to the position with Article 14.3(b), if any disclosure of the personal data occurs more than one month after obtaining the personal data, then Article 14.3(a) again continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

また、（第三者であるかどうかにかかわらず）他の取得者へのデータの開示が予測される状況について規定する第 14 条(3)(c)[32] に基づき、第 14 条(3)(a)の一般的な 1 か月の期限が短縮される場合もある [33]。そのような場合には、遅くとも初めて開示される時点で情報を提供しなければならない。この状況では、開示が 1 か月の期限の前に行われる場合、データを取得した時点から 1 か月という期限に達していない場合でも、遅くとも初めて開示した時にこの情報を提供しなければならない。第 14 条(3)(b)に関する見解の場合と同様、個人データを入手してから 1 か月以上経過した後に個人データが開示された場合にも、やはり引き続き第 14 条(3)(a)が適用されるため、第 14 条の情報の取得後遅くとも 1 か月以内にその情報をデータ主体に提供しなければならない。

28. Therefore, in any case, the maximum time limit within which Article 14 information must be provided to a data subject is one month. However, the principles of fairness and accountability under the GDPR require data controllers to always consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing, when deciding at what point to provide the Article 14 information. Accountability requires controllers to demonstrate the rationale for their decision and justify why the information was provided at the time it was. In practice, it may be difficult to meet these requirements when providing information at the 'last moment'. In this regard, Recital 39 stipulates, amongst other things, that data subjects should be "*made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing*". Recital 60 also refers to the requirement that the data subject be informed of the existence of the processing operation and its purposes in the context of the principles of fair and transparent processing. For all of these reasons,

---

replace it.

同様に第 14 条(3)(c)の「*他の取得者への開示が予測されるならば*」という表現の使用も、第 14 条(3)(a)に規定する最大の期限を考慮した一般的な記述であるものの、それを置き換えるものではないことを示唆している。

[33] Article 4.9 defines "recipient" and clarifies that a recipient to whom personal data are disclosed does not have to be a third party. Therefore, a recipient may be a data controller, joint controller or processor.

第 4 条(9)では、「取得者」を定義し、個人データの開示を受ける取得者が第三者である必要はないことを明確にしている。したがって、取得者は、データ管理者、共同管理者、又は処理者であってもよい。

WP29's position is that, wherever possible, data controllers should, in accordance with the principle of fairness, provide the information to data subjects well in advance of the stipulated time limits. Further comments on the appropriateness of the timeframe between notifying data subjects of the processing operations and such processing operations actually taking effect are set out in paragraphs 30 to 31 and 48.

28. したがって、いかなる場合も、第 14 条の情報をデータ主体に提供しなければならない期間の上限は 1 か月である。しかしながら、GDPR に基づく公正さとアカウンタビリティの原則により、データ管理者は、第 14 条の情報をどの時点で提供するかを決定する際に、データ主体の合理的な期待、取扱いがその主体に及ぼす影響、及びその取扱いに関連して自らの権利を行使する主体の能力を常に考慮する必要がある。アカウンタビリティの原則のために、管理者は、自分たちの決定の根拠を示し、その情報をその時点で提供したことの正当性を証明する必要がある。情報を「期限間際」に提供する場合など、これらの要件を満たすことが実際には難しい場合もある。この点に関して、前文第 39 項では、とりわけ、データの主体が、「*個人データの取扱いと関連するリスク、ルール、保護措置及び権利、並びに、その取扱いと関連する自身の権利をどのように行使するかについて、知らされる。*」べきであると規定している。また、前文第 60 項も、公正かつ透明性のある取扱いの原則との関連において、その取扱業務の存在及びその目的についてデータ主体が情報の提供を受けるという要件に言及している。以上の理由全てから、データ管理者が、公正さの原則に従い、可能な限り規定された期限より十分前に情報をデータ主体に提供すべきであるというのが第 29 条作業部会の見解である。取扱業務に関するデータ主体への通知からその取扱業務が実際に行われるまで期間の妥当性について、30 項から 31 項まで及び 48 項でさらにコメントしている。

Changes to Article 13 and Article 14 information

第 13 条及び第 14 条の情報の変更

29. Being accountable as regards transparency applies not only at the point of collection of personal data but throughout the processing life cycle, irrespective of the information or communication being conveyed. This is the case, for example, when changing the contents of existing privacy statements/ notices. The controller should adhere to the same principles when communicating both the initial privacy statement/ notice and any subsequent substantive or material changes to this statement/ notice. Factors which controllers should consider in assessing what is a substantive or material change include the impact on data subjects (including their ability to exercise their rights), and how unexpected/ surprising the change would be to data subjects. Changes to a privacy statement/ notice that should always be communicated to data subjects include inter alia: a change in processing purpose; a change to the identity of the controller; or a change as to how data subjects can exercise their rights in relation

to the processing. Conversely, an example of changes to a privacy statement/ notice which are not considered by WP29 to be substantive or material include corrections of misspellings, or stylistic/ grammatical flaws. Since most existing customers or users will only glance over communications of changes to privacy statements/ notices, the controller should take all measures necessary to ensure that these changes are communicated in such a way that ensures that most recipients will actually notice them. This means, for example, that a notification of changes should always be communicated by way of an appropriate modality (e.g. email, hard copy letter, pop-up on a webpage or other modality which will effectively bring the changes to the attention of the data subject) specifically devoted to those changes (e.g. not together with direct marketing content), with such a communication meeting the Article 12 requirements of being concise, transparent, intelligible, easily accessible and using clear and plain language. References in the privacy statement/ notice to the effect that the data subject should regularly check the privacy statement/notice for changes or updates are considered not only insufficient but also unfair in the context of Article 5.1(a). Further guidance in relation to the timing for notification of changes to data subjects is considered below at paragraph 30 to 31.

29. 透明性に関する説明責任を負う必要性は、伝達される情報や通信にかかわらず、個人データの収集時点だけでなく、取扱いの全サイクルにわたって適用される。例えば、既存のプライバシーステートメント／プライバシーノーティスの内容を変更する場合がその一例である。管理者は、当初のプライバシーステートメント／プライバシーノーティス、そしてこのステートメント／プライバシーノーティスのその後の実質的又は重大な変更のいずれについても、これを伝える際に、同じ原則を遵守するべきである。何が実質的又は重大な変化であるかを評価する際に管理者が考慮すべき要因には、データ主体（の権利を行使するその能力を含むデータ主体）への影響や、その変化がデータ主体にとってどの程度不測のもの／想定外のものとなるかが含まれる。データ主体に必ず伝達されるべきプライバシーステートメント／プライバシーノーティスの変更には、とりわけ以下が含まれる。すなわち、取扱目的の変更、管理者の身元の変更、又はデータ主体が取扱いに関連して権利を行使できる方法に関する変更、である。逆に、第 29 条作業部会が実質的又は重要であるとみなしていないプライバシーステートメント／プライバシーノーティスへの変更の例には、誤字、又は文体／文法上の欠陥の訂正が含まれる。既存の顧客やユーザーの大半は、プライバシーステートメント／プライバシーノーティスの変更に関する連絡を一瞥するにとどまるため、管理者は、取得者の大半がこれらの変更に確実に気づくような方法によってこれが伝わるようにするために、あらゆる必要な措置を講じるべきである。これは、例えば、変更の通知が、常にこれに特化した（例えば、ダイレクトマーケティング用メッセージとは分けて）、適切な手続（例えば電子メール、ハードコピーされたレター、Web ページ上のポップアップ、又は変更についてデータ主体に効果的に伝えることができる他の手続など）により連絡されるべきであり、また、そのような連絡が、簡潔で、透明性があり、理解しやすくかつ容易にアクセスしうるものであり、これに明瞭かつ平易な文言を使うという第 12 条の要件を満た

すものであることを意味する。変更又は更新が行われていないかプライバシーステートメント／プライバシーノーティスを定期的にチェックするようプライバシーステートメント／プライバシーノーティスにおける記載でデータ主体に知らせるのみでは、第 5 条(1)(a)との関連において不十分なだけでなく不公正であるとみなされる。変更についてデータ主体に通知するタイミングに関する指針について以下の 30 項から 31 項までにおいて追加的検討を加えている。

Timing of notification of changes to Article 13 and Article 14 information
第 13 条及び第 14 条の情報の変更を通知するタイミング

30. The GDPR is silent on the timing requirements (and indeed the methods) that apply for notifications of changes to information that has previously been provided to a data subject under Article 13 or 14 (excluding an intended further purpose for processing, in which case information on that further purpose must be notified prior to the commencement of that further processing as per Articles 13.3 and 14.4 – see below at paragraph 45). However, as noted above in the context of the timing for the provision of Article 14 information, the data controller must again have regard to the fairness and accountability principles in terms of any reasonable expectations of the data subject, or the potential impact of those changes upon the data subject. If the change to the information is indicative of a fundamental change to the nature of the processing (e.g. enlargement of the categories of recipients or introduction of transfers to a third country) or a change which may not be fundamental in terms of the processing operation but which may be relevant to and impact upon the data subject, then that information should be provided to the data subject well in advance of the change actually taking effect and the method used to bring the changes to the data subject's attention should be explicit and effective. This is to ensure the data subject does not "miss" the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDPR in relation to the change (e.g. to withdraw consent or to object to the processing).
30. GDPR では、第 13 条又は第 14 条に基づきデータ主体に以前に提供された情報の変更の通知に適用されるタイミングに関する要件（さらにその方法）について規定していない（そのデータをさらに他の目的で取扱うことが想定されている場合を除く。その場合には、第 13 条 3 項及び第 14 条(4)に従い（下記の 45 項を参照）、当該他の目的での取扱いを開始する前にその目的を通知しなければならない）。しかしながら、上記において第 14 条に関する情報を提供するタイミングとの関連において述べたように、データ管理者は、やはり、データ主体の合理的な期待又はこれらの変更がデータ主体に及ぼす潜在的な影響に関して、公正性及びアカウンタビリティの原則に留意しなければならない。情報の変更が、取扱いの性質の根本的な変更（例えば取得者の区分の拡大又は第三国への移転の拡大など）又は取扱業務の

点では根本的なものではない可能性があるものの、データ主体に関連するものであり、これに影響を及ぼす可能性がある場合には、変更が実際に効力を及ぼす時点よりも十分前の段階で、その情報をデータ主体に提供すべきであり、また、変更についてデータ主体の注意を喚起するために明示的かつ効果的な方法を用いるべきである。これは、データ主体が変更を「見過ご」さないことを確保し、また、(a)変更の性質と影響を考慮し、(b)変更に関連して GDPR に基づく自ら権利を行使する（例えば、同意を撤回する又は取扱いに異議を述べる）ための合理的な期間をデータ主体に与えるためである。

31. Data controllers should carefully consider the circumstances and context of each situation where an update to transparency information is required, including the potential impact of the changes upon the data subject and the modality used to communicate the changes, and be able to demonstrate how the timeframe between notification of the changes and the change taking effect satisfies the principle of fairness to the data subject. Further, WP29's position is that, consistent with the principle of fairness, when notifying such changes to data subjects, a data controller should also explain what will be the likely impact of those changes on data subjects. However, compliance with transparency requirements does not "whitewash" a situation where the changes to the processing are so significant that the processing becomes completely different in nature to what it was before. WP29 emphasises that all of the other rules in the GDPR, including those relating to incompatible further processing, continue to apply irrespective of compliance with the transparency obligations.
31. データ管理者は、変更がデータ主体に及ぼす潜在的な影響や変更の連絡に利用される手続など、透明性に関する情報の更新が必要となる、それぞれの状況を取り巻く事情及び文脈を慎重に検討し、データ主体に対する公正性の原則を満たすように、変更の通知から変更が効力を及ぼすまでの期間を設定したことを証明できるようにすべきである。さらに、そのような変更をデータ主体に通知する際は、データ管理者が、公正性の原則に従い、その変更によりデータ主体に及ぶ可能性のある影響についても説明するべきだというのが第 29 条作業部会の見解である。しかしながら、透明性に関する要件を遵守したとしても、取扱いの変更が極めて重大であり、取扱いの性質がそれまでとは全く変わってしまうような状況を「取り繕う」ことはできない。第 29 条作業部会では、相容れないような追加的取扱いに関する規則を含む GDPR の他の全ての規則が、引き続き、透明性の義務の遵守に関係なく適用される点を強調する。

32. Additionally, even when transparency information (e.g. contained in a privacy statement/ notice) does not materially change, it is likely that data subjects who have been using a service for a significant period of time will not recall the information provided to them at the outset under Articles 13 and/or 14. WP29 recommends that controllers facilitate data subjects to have continuing easy access to the information to re-acquaint themselves with the scope of the data processing. In accordance with the

accountability principle, controllers should also consider whether, and at what intervals, it is appropriate for them to provide express reminders to data subjects as to the fact of the privacy statement/ notice and where they can find it.

32. さらに、(例えば、プライバシーステートメント／プライバシーノーティスに含まれる) 透明性に関する情報が大きくは変化しない場合であっても、サービスを長期間利用してきたデータ主体は、第 13 条及び又は第 14 条に基づき最初に提供を受けた情報を思い出せない可能性が高い。第 29 条作業部会では、データ主体が、データの取扱いの範囲を再確認するための情報に継続して容易にアクセスできるよう管理者がデータ主体を支援することを勧告する。また、管理者は、アカウンタビリティの原則に従い、プライバシーステートメント／通知の内容及びこれをどこで閲覧できるかについて、データ主体に説明を提供し伝えることが適切であるかどうか、またその間隔の期間について考慮するべきである。

Modalities - format of information provision

手続 - 情報提供の形式

33. Both Articles 13 and 14 refer to the obligation on the data controller to "*provide the data subject with all of the following information...*" The operative word here is "provide". This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.). The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app. The example at paragraph 11 illustrates this point. As noted above at paragraph 17, WP29 recommends that the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (e.g. whether in a digital form on a website or in paper format) which can be easily accessed should they wish to consult the entirety of the information.

33. 第 13 条と第 14 条のいずれも、「*データ主体に対し、以下の全ての情報を提供する*」データ管理者の義務に言及している。この場合の「提供する」は能動的な言葉である。これは、データ管理者が積極的な措置を講じ、当該情報をデータ主体に提供しなければならない、又はデータ主体を（例えば、直接リンク、QR コードの使用などを通じて）データのある場所に積極的に誘導しなければならないということを意味する。データ主体に対し、ウェブサイトやアプリの使用条件など、他の情報の中からこれらの条文の対象とする情報を自ら進んで検索するように強いるものであってはならない。11 項の例は、この点をはっきりと示している。上記 17 項で述べたように、第 29 条作業部会は、データ主体が情報全体を確認したい場合に容易にアクセスできるよう、そうした情報全体を（デジタル又は紙形式であろうと）一つの場所又は一つの完全な文書の形式でも提供すべきであると勧告する。

34. There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible. As such, and bearing in mind the fundamental principles of accountability and fairness, controllers must undertake their own analysis of the nature, circumstances, scope and context of the processing of personal data which they carry out and decide, within the legal requirements of the GDPR and taking account of the recommendations in these Guidelines particularly at paragraph 36 below, how to prioritise information which must be provided to data subjects and what are the appropriate levels of detail and methods for conveying the information.
34. GDPR においては、一方には、GDPR の下で必要とされる包括的な情報をデータ主体に提供するという要件があり、もう一方には、その情報を簡潔で、透明性があり、理解しやすくかつ容易にアクセスしうる形式でデータ主体に提供するという要件があるため、当然のことながら両者の間に緊張関係が生じている。したがって、アカウンタビリティと公正性の基本原則を念頭に置きつつ、管理者は、自らの実施する個人データの取扱いの性質、状況、範囲及び文脈を独自に分析しなければならず、GDPR の法的要件の範囲内で、また、本ガイドラインの勧告、特に下記の 36 項を踏まえ、データ主体に提供しなければならない情報にどのように優先順位を設定するか、情報を伝達する上でどの程度詳細に伝えることが適切であるか及びどのように伝達するかを決定する。

Layered approach in a digital environment and layered privacy statements/ notices
デジタル環境における階層的なアプローチと階層的なプライバシーステートメント／プライバシーノーティス

35. In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/ notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read. It should be noted that layered privacy statements/ notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/ notice. It is also important that the information contained within the different layers of a layered notice is

consistent and that the layers do not provide conflicting information.

35. デジタル環境では、データ管理者が透明性を確保するために複数の方法の組合せを利用することを選択した場合には、データ主体に提供する必要のある情報の量に照らして、階層的なアプローチを採用してもよい。第 29 条作業部会では、特に、情報疲労を避けるため、データ主体に提供しなければならない全ての情報を画面上に単一の通知として表示するよりむしろ、そのようなさまざまな種類の情報にリンクするために階層的なプライバシーステートメント／プライバシーノーティスを利用すべきと勧告する。階層的なプライバシーステートメント／プライバシーノーティスを利用すれば、特に、ステートメント／通知のユーザーの読みたい箇所を直接誘導することを可能にし、網羅性と理解しやすさとの緊張関係を解決することができる場合がある。階層的なプライバシーステートメント／プライバシーノーティスとは、単にページが入れ子構造になっており、該当する情報に到達するために数回クリックすれば足りるというものではない点に注意したい。プライバシーステートメント／プライバシーノーティスの第 1 層の設計と配置は、データ主体が、自らの個人データの取扱いをめぐって自らに利用可能な情報と、そうした詳細な情報をプライバシーステートメント／プライバシーノーティスの階層内のどこで／どのように見つけることができるかを明瞭に概観できるようなものとするべきである。また、階層的な通知のさまざまな階層内に含まれる情報に一貫性があり、階層間で矛盾する情報が提供されないことも重要である。

36. As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/ notice, WP29 recommends that the first layer/ modality should include the details of the purposes of processing, the identity of controller and a description of the data subject's rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.) The importance of providing this information upfront arises in particular from Recital 39[34]. While controllers must be able to demonstrate accountability as to what further information they decide to prioritise, WP29's position is that, in line with the fairness principle, in addition to the information detailed above in this paragraph, the first layer/ modality should also contain information on the processing which has the most impact on the data subject and processing

[34] Recital 39 states, on the principle of transparency, that "That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed."
前文第 39 項では、透明性の原則について、「この基本原則は、特に、データ主体に対する管理者の識別名及び取扱いの目的の情報、並びに、関係する自然人に関する公正かつ透明性のある取扱いを確保し、そして、取扱われている自然人に関する個人データの確認及びコミュニケーションを得る当該自然人の権利を確保するためのさらなる情報と関係している。」と述べている。

which could surprise them. Therefore, the data subject should be able to understand from information contained in the first layer/ modality what the consequences of the processing in question will be for the data subject (see also above at paragraph 10).

36. 階層的なアプローチでデータ主体に通知するために管理者が利用した第一の手続の内容（すなわち、管理者がデータ主体に最初に接触する主な方法）、又は階層的なプライバシーステートメント／通知の第 1 層の内容について、第 29 条作業部会では、第一の階層／手続に、取扱い目的の詳細、管理者の身元、データ主体の権利の説明を含めることを勧告する。（さらに、この情報については、例えば、データ主体がオンラインフォームに記入する際に表示されるなど、個人データの収集時にデータ主体の注意を直接喚起すべきである）。特に前文第 39 項から、この情報を前もって提供することが重要である [34]。管理者は、自らがさらにどの情報を優先することに決めたかについてもアカウンタビリティを証明できなければならないものの、公正性の原則に基づき、第一の階層／手続には、本項で詳細に説明した上記の情報に加え、データ主体への影響が最も大きな取扱いと、データ主体にとって不意打ちとなりかねない取扱いに関する情報も含めるべきであるというのが第 29 条作業部会の見解である。したがって、データ主体が、第 1 層／手続に含まれる情報をもとに当該取扱いの結果がデータ主体にとってどのようなものであるについて理解できるようにするべきである（上記 10 項参照）。

37. In a digital context, aside from providing an online layered privacy statement/ notice, data controllers may also choose to use *additional* transparency tools (see further examples considered below) which provide tailored information to the individual data subject which is specific to the position of the individual data subject concerned and the goods/ services which that data subject is availing of. It should be noted however that while WP29 recommends the use of online layered privacy statements/ notices, this recommendation does not exclude the development and use of other innovative methods of compliance with transparency requirements.

37. データ管理者は、デジタル環境において、階層的なプライバシーステートメント／プライバシーノーティスをオンラインで提供する以外にも、対象となる個々のデータ主体のポジション及びそのデータ主体が利用できる商品／サービスに応じ、個々のデータ主体のニーズに合わせた情報を提供するような*追加的な*透明性を確保するためのツール（以下で検討する他の事例も参照）の利用を選択することもできる。ただし、第 29 条作業部会ではオンラインの階層的なプライバシーステートメント／プライバシーノーティスを利用することを勧告しているものの、この勧告により、透明性の要件を遵守するための他の革新的な方法の開発及び使用が妨げられているわけではない点に留意すべきである。

Layered approach in a non-digital environment

非デジタル環境における階層的なアプローチ

38. A layered approach to the provision of transparency information to data subjects can also be deployed in an offline/ non-digital context (i.e. a real-world environment such as person-to-person engagement or telephone communications) where multiple modalities may be deployed by data controllers to facilitate the provision of information. (See also paragraphs 33 to 37 and 39 to 40 in relation to different modalities for providing the information.) This approach should not be confused with the separate issue of layered privacy statements/ notices. Whatever the formats that are used in this layered approach, WP29 recommends that the first "layer" (in other words the primary way in which the controller first engages with the data subject) should generally convey the most important information (as referred to at paragraph 36 above), namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject. For example, where the first point of contact with a data subject is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13/ 14 by way of further, different means, such as by sending a copy of the privacy policy by email and/ or sending the data subject a link to the controller's layered online privacy statement/ notice.

38. データ主体への透明性情報の提供に対する階層的なアプローチはオフライン／非デジタル環境（すなわち、個人対個人の接触や電話での会話などの現実における環境）でも採用でき、その場合には、データ管理者が、情報の提供を容易にするために複数の手続を採用してもよい。（情報を提供するためのさまざまな手続に関しては 33 項から 37 項まで、また 39 項から 40 項までも参照）。このアプローチは、階層的なプライバシーステートメント／プライバシーノーティスの別個の問題と混同してはならない。第 29 条作業部会では、この階層的なアプローチで使われている形式が何であれ、最初の「階層」（つまり、管理者がデータ主体に最初に接触する主要な方法）で、一般に（上記の 36 項でいう）最も重要な情報、すなわち取扱目的の詳細、管理者の身元、データ主体の権利の存在、これに併せて取扱いによる影響が最も大きいか又はデータ主体にとって不意打ちとなりかねない取扱いに関する情報を伝えることを勧告する。例えば、データ主体との最初の接触が電話によるものである場合、この情報をデータ主体との通話時に提供し、また、第 13 条／第 14 条に基づいて提供する必要のあるその他の情報は、プライバシーポリシーのコピーを電子メールで送信する及び又は管理者のオンラインによる階層的なプライバシーステートメント／プライバシーノーティスへのリンクをデータ主体に送信するなど、他の追加的な手段を利用して提供してもよい。

“Push” and “pull” notices
「プッシュ」及び「プル」通知

39. Another possible way of providing transparency information is through the use of “push” and “pull” notices. Push notices involve the provision of “just-in-time” transparency information notices while “pull” notices facilitate access to information by methods such as permission management, privacy dashboards and “learn more” tutorials. These allow for a more user-centric transparency experience for the data subject.
39. 透明性に関する情報を提供するもう一つの方法として、「プッシュ」及び「プル」通知の利用が考えられる。プッシュ通知は、透明性に関する情報の「ジャストインタイム」の通知の提供を含む一方、「プル」通知は、権限管理、プライバシーダッシュボード、及び「詳細な学習（learn more）」が可能なチュートリアルなどの方法による情報へのアクセスを容易にする。これにより、データ主体にとって、よりユーザー中心の透明性が得られる。

- A privacy dashboard is a single point from which data subjects can view ‘privacy information’ and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the service in question. This is particularly useful when the same service is used by data subjects on a variety of different devices as it gives them access to and control over their personal data no matter how they use the service. Allowing data subjects to manually adjust their privacy settings via a privacy dashboard can also make it easier for a privacy statement/ notice to be personalized by reflecting only the types of processing occurring for that particular data subject. Incorporating a privacy dashboard into the existing architecture of a service (e.g. by using the same design and branding as the rest of the service) is preferable because it will ensure that access and use of it will be intuitive and may help to encourage users to engage with this information, in the same way that they would with other aspects of the service. This can be an effective way of demonstrating that ‘privacy information’ is a necessary and integral part of a service rather than a lengthy list of legalese.
  プライバシーダッシュボードは、データ主体が「プライバシー情報」を表示し、問題のサービスが自分たちのデータを特定の方法で利用することを許可又は禁止することによって自分たちのプライバシー設定を管理できる方法の１つである。この機能により、データ主体がそのサービスをどのように使っているかにかかわらず、データ主体による自らの個人データへのアクセスとその管理が可能になるため、データ主体が複数のデバイスで同じサービスを利用する場合に特に便利である。データ主体がプライバシーダッシュボードを通じて自分のプライバシー設定を手動で調整できるようにすれば、その特定のデータ主体について発生する取扱いのみを反映させることでプライバシーステートメント／プライバシーノーティスをパーソナライズしやすくなる。（例えば、他のサ

ービスと同じデザインとブランドを利用するなどにより）サービスの既存のアーキテクチャーにプライバシーダッシュボードを組み込めば、この機能へのアクセスとその利用が直感的なものとなるようにして、サービスの他の側面と同じ方法でこの情報に接するようユーザーに促す上で役立つ可能性があるため、そうすることが望ましい。これは、「プライバシー情報」が、法律用語の長いリストというよりむしろ、サービスの必要不可欠な部分であることを示すのに効果的な方法である。

- A just-in-time notice is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read. This method is useful for providing information at various points throughout the process of data collection; it helps to spread the provision of information into easily digestible chunks and reduces the reliance on a single privacy statement/ notice containing information that is difficult to understand out of context. For example, if a data subject purchases a product online, brief explanatory information can be provided in pop-ups accompanying relevant fields of text. The information next to a field requesting the data subject's telephone number could explain for example that this data is only being collected for the purposes of contact regarding the purchase and that it will only be disclosed to the delivery service.
ジャストインタイムの通知は、データ主体に最も関連があり読むべきである場合に、その場限りで特定の「プライバシー情報」を提供するために利用される。この方法は、データの収集プロセス全体のさまざまな時点で情報を提供するのに適する。すなわち、情報を理解しやすいまとまりに分けて提供し、文脈から切り離されると理解しがたい情報を含む単一のプライバシーステートメント／プライバシーノーティスへの依存度を減らす。例えば、データ主体が製品をオンラインで購入する場合、該当するテキストフィールドに付随するポップアップで、簡単な情報説明を提供することができる。例えば、データ主体の電話番号を要求するフィールドの隣に情報を示し、このデータの購入に関係する連絡の目的でのみデータを収集し、収集されたデータは配送サービスにのみ開示されるということを説明する方法もある。

Other types of "appropriate measures"
他のタイプの「適切な措置」

40. Given the very high level of internet access in the EU and the fact that data subjects can go online at any time, from multiple locations and different devices, as stated above, WP29's position is that an "appropriate measure" for providing transparency information in the case of data controllers who maintain a digital/ online presence, is to do so through an electronic privacy statement/ notice. However, based on the circumstances of the data collection and processing, a data controller may need to additionally (or alternatively where the data controller does not have any digital/online presence)

use other modalities and formats to provide the information. Other possible ways to convey the information to the data subject arising from the following different personal data environments may include the following modes applicable to the relevant environment which are listed below. As noted previously, a layered approach may be followed by controllers where they opt to use a combination of such methods while ensuring that the most important information (see paragraph 36 and 38) is always conveyed in the first modality used to communicate with the data subject.

40. EU におけるインターネットの普及率が極めて高い水準にあり、また、上述のようにデータ主体が複数の場所や異なるデバイスからいつでもオンラインにアクセスできるという事実を考慮すると、デジタル環境／オンラインで活動するデータ管理者の場合には、電子的なプライバシーステートメント／プライバシーノーティスを用いることが透明性に関する情報を提供するための「適切な措置」であるというのが第 29 条作業部会の見解である。しかしながら、データ管理者は、データの収集及び取扱状況に基づき、情報を提供するために前記のものに追加して（又は、データ管理者がデジタル環境／オンラインで活動していない場合には、これに代える形で）他の手続及びフォーマットを利用する必要が生じうる。以下の異なる個人データの環境から生じる情報をデータ主体に伝達するための他の方法としては、該当する環境（以下に列挙する）に適用可能な以下の手続が挙げられる。前述のように、管理者が、データ主体と初めて絡連を取る際に常に最も重要な情報（36 及び 38 項を参照）が伝達されるよう確保しつつ、上記の方法の組み合わせを利用することを選択した場合には、階層的なアプローチを採用してもよい。

a. Hard copy/ paper environment, for example when entering into contracts by postal means: written explanations, leaflets, information in contractual documentation, cartoons, infographics or flowcharts;

a. 例えば、郵送で契約を結んだ場合におけるハードコピー／紙の環境： 書面による説明、リーフレット、契約文書の情報、1 コマ漫画、インフォグラフィック又はフローチャート、

b. Telephonic environment: oral explanations by a real person to allow interaction and questions to be answered or automated or pre-recorded information with options to hear further more detailed information;

b. 電話を利用する環境： 対話や質問への回答が可能な生身の人間による口頭の説明又はさらに詳細な情報を聞けるという選択肢を用意した上での自動音声若しくは録音音声による情報の提供、

c. Screenless smart technology/ IoT environment such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written details incorporated into paper set-up instructions, videos incorporated into digital set-up instructions, written information on the smart device, messages sent by SMS or email, visible boards containing the information, public signage or public information campaigns;

c. スクリーンを持たないスマートテクノロジー／Wi-Fi トラッキング分析などの IoT 環境：アイコン、QR コード、音声アラート、紙媒体でのセットアップ手順説明書に記載されている詳細な情報、デジタル環境でのセットアップ手順説明書に取り込まれた映像、スマートデバイス上に表示される書面による情報、SMS 又は電子メールによって送信されるメッセージ、情報を表示する目に見えるボード、公共の標識又は公開情報キャンペーン、

d. Person to person environment, such as responding to opinion polls, registering in person for a service: oral explanations or written explanations provided in hard or soft copy format;
d. 世論調査への回答、本人によるサービスの直接登録などの個人対個人の環境： 口頭での説明又はハードコピー又はソフトコピーによる説明書、

e. “Real-life” environment with CCTV/ drone recording: visible boards containing the information, public signage, public information campaigns or newspaper/ media notices.
e. CCTV／ドローンの録画による「実写」環境：情報を表示する目に見えるボード、公共の標識、公開情報キャンペーン、新聞／メディアによる公告。

Information on profiling and automated decision-making
プロファイリングと自動化された意思決定に関する情報

41. Information on the existence of automated decision-making, including profiling, as referred to in Articles 22.1 and 22.4, together with meaningful information about the logic involved and the significant and envisaged consequences of the processing for the data subject, forms part of the obligatory information which must be provided to a data subject under Articles 13.2(f) and 14.2(g). WP29 has produced guidelines on automated individual decision-making and profiling[35] which should be referred to for further guidance on how transparency should be given effect in the particular circumstances of profiling. It should be noted that, aside from the specific transparency requirements applicable to automated decision-making under Articles 13.2(f) and 14.2(g), the comments in these guidelines relating to the importance of informing data subjects as to the consequences of processing of their personal data, and the general principle that data subjects should not be taken by surprise by the processing of their personal data, equally apply to profiling generally (not just profiling which is

[35] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251
2016/679 規則の目的のためのプロファイリングを含む自動化された個人の意思決定に関するガイドライン, WP 251

captured by Article 22[36]), as a type of processing[37].

41. 第 22 条(1)及び第 22 条(4)で言及しているように、プロファイリングを含む自動化された意思決定の存在に関する情報、並びに、それに関連する論理についての有意な情報、及びデータ主体に関する当該取扱いによって得られる予測される重大な結果は、第 13 条(2)(f)及び第 14 条(2)(g)に基づいてデータ主体に提供されなければならないことを義務づけられた情報となる。第 29 条作業部会では、プロファイリングを含む自動化された個人の意思決定に関するガイドラインを作成しており[35]、プロファイリングをめぐる特定の状況において透明性をどのように確保するべきかの判断における詳細な指針については、これを参照するべきである。第 13 条(2)(f)及び第 14 条(2)(g)に基づいて、自動化された意思決定に適用される特有の透明性の要件とは別に、これらの指針において、データ主体が自らの個人データの取扱いの結果について情報の提供を受けることの重要性に関するコメントと、データ主体にとって自らの個人データが想定外の取扱いをされることがあってはならないという一般原則が、取扱いの一形態である（第 22 条の対象とするプロファイリングだけでなく[36]）プロファイリング全般にも同様に適用される点に留意すべきである[37]。

Other issues – risks, rules and safeguards

その他の問題 - リスク、規則、保護措置

42. Recital 39 of the GDPR also refers to the provision of certain information which is not explicitly covered by Articles 13 and Article 14 (see recital text above at paragraph 28). The reference in this recital to making data subjects aware of the risks, rules and safeguards in relation to the processing of personal data is connected to a number of other issues. These include data protection impact assessments (DPIAs). As set out in the WP29 Guidelines on DPIAs, [38] data controllers may consider publication of the DPIA (or part of it), as a way of fostering trust in the processing operations and demonstrating transparency and accountability, although such publication is not obligatory. Furthermore, adherence to a code of conduct (provided for under Article 40) may go towards demonstrating transparency, as codes of conduct may be drawn up for the purpose of specifying the

[36] This applies to decision-making based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her.
これは、プロファイリングを含む自動化された取扱いのみに基づく意思決定であって、データ主体に関する法的効果又はデータ主体に類似の重要な効果を及ぼすものに適用される。

[37] Recital 60, which is relevant here, states that “Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling”.
これに関連する前文第 60 項では、「さらに、データ主体は、プロファイリングの存在及びそのようなプロファイリングから生ずる結果についても情報の提供を受けるものとしなければならない。」と述べられている。

[38] 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.1
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.1

application of the GDPR with regard to: fair and transparent processing; information provided to the public and to data subjects; and information provided to, and the protection of, children, amongst other issues.

42. また、GDPR の前文第 39 項では、第 13 条及び第 14 条において明示的には対象とされていない一定の情報の提供にも言及している（前文第 28 項の文言を参照）。個人データの取扱いに関連するリスク、規則、保護措置に関してデータ主体に情報を提供しなければならないという本前文の記載は、他の問題とも関連している。この問題に含まれているのが、データ保護影響評価（DPIA）である。DPIA に関する第 29 条作業部会ガイドライン[38]に規定されているように、公開義務はないものの、データ管理者は、取扱業務への信頼を構築し、透明性とアカウンタビリティを証明する方法として DPIA（又はその一部）の公開を検討しうる。さらに、行動規範は以下の点に関連する GDPR の適用方法を明記する目的で策定することもできるため、行動規範（第 40 条に規定されている）を遵守すれば、透明性を証明する上で有利に働く可能性がある。すなわち、公正で透明性のある取扱い、公衆とデータ主体に提供される情報、また特に、子どもたちに提供される情報、及び子どもたちの保護、である。

43. Another relevant issue relating to transparency is data protection by design and by default (as required under Article 25). These principles require data controllers to build data protection considerations into their processing operations and systems from the ground up, rather than taking account of data protection as a last-minute compliance issue. Recital 78 refers to data controllers implementing measures that meet the requirements of data protection by design and by default including measures consisting of transparency with regard to the functions and processing of personal data.

43. 透明性に関してもう一つ問題となってくるものは、（第 25 条により要求される）データ保護バイデザインとデータ保護バイデフォルトである。これらの原則によって、データ管理者は、データ保護を、最終段階で法令を遵守するために調整を加えるような問題として捉えるよりむしろ、取扱業務及びシステムの初期段階からデータ保護に対する配慮を組み込まねばならなくなる。前文第 78 項は、データ管理者が、個人データの機能及び取扱いに関して、透明性を確保する措置を含めた、データ保護バイデザインとデータ保護バイデフォルトの要件を満たすための措置を実施することに言及している。

44. Separately, the issue of joint controllers is also related to making data subjects aware of the risks, rules and safeguards. Article 26.1 requires joint controllers to determine their respective responsibilities for complying with obligations under the GDPR in a transparent manner, in particular with regard to the exercise by data subjects of their rights and the duties to provide the information under Articles 13 and 14. Article 26.2 requires that the essence of the arrangement between the data

controllers must be made available to the data subject. In other words, it must be completely clear to a data a subject as to which data controller he or she can approach where they intend to exercise one or more of their rights under the GDPR[39].

44. 上記とは別に、共同管理者の問題が、リスク、規則、保護措置に関してデータ主体に情報提供を行うことに関係してくる。第 26 条(1)では、共同管理者に対し、特にデータ主体によるその権利の行使及び第 13 条及び第 14 条に基づく情報提供の義務との関連で、GDPR に基づく義務を遵守する上でのそれぞれの責任について透明性のある方法で決定することを要求している。第 26 条(2)では、データ管理者間の取決めの要点がデータ主体にとって利用可能なものでなければならないと求めている。言い換えれば、GDPR に基づく自らの権利を一つ、若しくは複数行使したい場合にどのデータ管理者にアプローチすればよいのかが、データ主体にとって完全に明瞭でなければならない[39]。

Information related to further processing
追加的取扱いに関連する情報

45. Both Articles 13 and Article 14 contain a provision[40] that requires a data controller to inform a data subject if it intends to further process their personal data for a purpose other than that for which it was collected/ obtained. If so, "*the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2*". These provisions specifically give effect to the principle in Article 5.1(b) that personal data shall be collected for specified, explicit and legitimate purposes, and further processing in a manner that is incompatible with these purposes is prohibited[41]. The second part of Article 5.1(b) states that further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes, shall, in accordance with Article 89.1, not be considered to be *incompatible* with the initial purposes. Where personal data are further processed for purposes that are *compatible* with the original purposes (Article 6.4 informs this issue[42]), Articles 13.3

[39] Under Article 26.3, irrespective of the terms of the arrangement between joint data controllers under Article 26.1, a data subject may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.
第 26 条(3)に基づき、第 26 条(1)に基づく共同データ管理者間の取り決めの条件にかかわらず、データ主体は、各共同データ管理者について、また、これに対抗して、GDPR に基づく自らの権利を行使することができる。

[40] At Articles 13.3 and 14.4, which are expressed in identical terms, apart from the word "collected", which is used in Article 13, and which is replaced with the word "obtained" in Article 14.
第 13 条(3)及び第 14 条(4)は、第 13 条では「収集される」という言葉が使われ、第 14 条ではこれが「取得される」という言葉に置き換えられている以外、同一の用語で表現されている。

[41] See, for example on this principle, Recitals 47, 50, 61, 156, 158; Articles 6.4 and 89
この原則については、例えば、前文第 47 項、50 項、61 項、156 項、158 項、また、第 6 条(4)及び第 89 条を参照。

[42] Article 6.4 sets out, in non-exhaustive fashion, the factors which are to be taken into account in ascertaining whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, namely: the link between the purposes; the context in which the personal data have been collected; the nature of the personal data (in particular whether special categories of personal data or personal data relating to

and 14.4 apply. The requirements in these articles to inform a data subject about further processing promotes the position in the GDPR that a data subject should reasonably expect that at the time and in the context of the collection of personal data that processing for a particular purpose may take place[43]. In other words, a data subject should not be taken by surprise at the purpose of processing of their personal data.

45. 当初収集／取得した目的以外の目的で個人データを追加的に取り扱う予定がある場合、データ主体に通知するようデータ管理者に要求する規定[40]が第 13 条にも第 14 条にも含まれている。そのような場合、「*管理者は、データ主体に対し、当該追加的取扱いの開始前に、当該別の目的に関する情報及び第 2 項に定める関連する付加的情報を提供する。*」。これらの規定は、個人データは特定され、明確であり、かつ、正当な目的のために収集されるものとし、かつ、その目的に適合しない様態で追加的取扱いをしてはならないという第 5 条(1)(b)の原則で具体的に述べられている[41]。第 5 条(1)(b)の後半では、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために行われる追加的取扱いは、第 89 条(1)に従い、当初の目的と*適合しない*ものとはみなされないと述べている。個人データが当初の目的と*適合する*目的で追加的に取り扱われる場合（第 6 条(4)がこの問題について述べている[42]）、第 13 条(3)及び第 14 条(4)が適用される。追加的取扱いについてデータ主体に通知するというこれらの条項の要件は、個人データの収集時及びそれとの関連において当該目的での取扱いがなされることをデータ主体が合理的に予期できなければならないという GDPR の立場を裏付けるものである[43]。言い換えれば、自らの個人データの取扱目的をめぐってデータ主体の想定外であるようなことがあってはならない。

46. Articles 13.3 and 14.4, insofar as they refer to the provision of "*any relevant further information as referred to in paragraph 2*", may be interpreted at first glance as leaving some element of appreciation to the data controller as to the extent of and the particular categories of information from the relevant sub-paragraph 2 (i.e. Article 13.2 or 14.2 as applicable) that should be provided to the data subject. (Recital 61 refers to this as "*other necessary information*".) However the default position is that all such information set out in that subarticle should be provided to the data subject unless one or more categories of the information does not exist or is not applicable.

46. 第 13 条(3)及び第 14 条(4)は、「*第 2 項で定めるようなあらゆる関連性のある追加的情報*」という規定に言及する限りにおいて、一見すると、データ主体に提供すべき該当する第

criminal offences and convictions are included); the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards.

第 6 条(4)では、目的外の取扱いが、個人データを当初収集した際の目的と合致するかどうかを確認するために考慮に入れるべき要素を非網羅的に規定している。すなわち、目的間の関連性、個人データが収集された文脈、個人データの性質（特に、特別な種類の個人データが含まれるか否か、又は有罪判決又は犯罪に係る個人データが含まれるか否か）、予定されている追加的取扱いにおいて、データ主体に生じうる結果、適切な保護措置の存在といったものである。

[43] Recitals 47 and 50

前文第 47 項及び 50 項

2 項（すなわち適用される場合に応じて第 13 条(2)又は第 14 条(2)）の情報の程度及び特別な種類についてデータ管理者が判断する余地を残していると解釈できる可能性がある。（前文第 61 項では、これを「*その他の必要な情報*」と呼んでいる）。しかしながら、その項で規定する一つ、若しくは複数の種類の情報が存在しないか、又は適用できない場合を除き、当該全ての情報をデータ主体に提供するべきであるというのが基本的な見解である。

47. WP29 recommends that, in order to be transparent, fair and accountable, controllers should consider making information available to data subjects in their privacy statement/ notice on the compatibility analysis carried out under Article 6.4[44] where a legal basis other than consent or national/ EU law is relied on for the new processing purpose. (In other words, an explanation as to how the processing for the other purpose(s) is compatible with the original purpose). This is to allow data subjects the opportunity to consider the compatibility of the further processing and the safeguards provided and to decide whether to exercise their rights e.g. the right to restriction of processing or the right to object to processing, amongst others[45]. Where controllers choose not to include such information in a privacy notice/ statement, WP29 recommends that they make it clear to data subjects that they can obtain the information on request.

47. 第 29 条作業部会は、新しい取扱いの目的が同意又は国内／EU 法以外の法的根拠に立脚している場合に、透明性、公正さ及びアカウンタビリティを備えるためには、管理者が、プライバシーステートメント／プライバシーノーティスの中で第 6 条(4)[44] に基づき行われる適合性分析に関する情報（言い換えれば、他の目的での取扱いが当初の目的とどのように適合するかの説明）をデータ主体に提供するよう考慮することを勧告する。これは、追加的取扱いと提供される保護措置との適合性を検討し、また、例えば特に取扱いを制限する権利や取扱いに異議を述べる権利など自分たちの権利を行使するかどうかを決定する機会をデータ主体に与えるためである[45]。管理者がプライバシーステートメント／プライバシーノーティスにそのような情報を含めないことを選択した場合、第 29 条作業部会は、要求すればその情報を入手できることをデータ主体に明確に伝えることを勧告する。

48. Connected to the exercise of data subject rights is the issue of timing. As emphasized above, the provision of information in a timely manner is a vital element of the transparency requirements under Articles 13 and 14 and is inherently linked to the concept of fair processing. Information in relation to *further processing* must be provided “prior to that further processing”. WP29’s position is that a reasonable period should occur between the notification and the processing commencing rather than

[44] Also referenced in Recital 50
前文第 50 項でも言及している。

[45] As referenced in Recital 63, this will enable a data subject to exercise the right of access in order to be aware of and to verify the lawfulness of the processing.
前文第 63 項で言及しているように、これにより、データ主体が、取扱いの適法性を認識し、検証するためにアクセス権を行使することが可能になる。

an immediate start to the processing upon notification being received by the data subject. This gives data subjects the practical benefits of the principle of transparency, allowing them a meaningful opportunity to consider (and potentially exercise their rights in relation to) the further processing. What is a reasonable period will depend on the particular circumstances. The principle of fairness requires that the more intrusive (or less expected) the further processing, the longer the period should be. Equally, the principle of accountability requires that data controllers be able to demonstrate how the determinations they have made as regards the timing for the provision of this information are justified in the circumstances and how the timing overall is fair to data subjects. (See also the previous comments in relation to ascertaining reasonable timeframes above at paragraphs 30 to 32.)

48. データ主体の権利行使に関連してタイミングの問題が存在する。上記で強調したように、適時に情報を提供することは、第 13 条及び第 14 条に基づく透明性要件の極めて重要な要素であり、公正な取扱いの概念に本質的に結びついている。*追加的取扱い*に関連する情報は、「追加的取扱いがなされる前に」提供されなければならない。データ主体が通知を受け取り次第ただちに取扱いを開始するのではなく、通知から取扱いの開始までに合理的な期間を設けるべきだというのが第 29 条作業部会の見解である。これにより、データ主体は、透明性の原則から得られる実益を取得し、追加的取扱いについて考慮（し、潜在的にはこれに関連する自らの権利を行使）する意味のある機会を手に入れることができる。合理的な期間は、それぞれの状況に応じて決まる。公正さの原則に基づき、追加的取扱いがより侵害的である（又は予期されていない）ほど、この期間も長く取る必要がある。同様に、アカウンタビリティの原則により、データ管理者は、この情報を提供したタイミングに関する自分たちの行った決定がその状況において正当であり、そのタイミングが全体としてデータ主体に対して公正であるという根拠を示すことができる必要がある。（上記 30 から 32 項における合理的な期間の確定に関するこれまでのコメントも参照）。

Visualisation tools
視覚化ツール

49. Importantly, the principle of transparency in the GDPR is not limited to being effected simply through language communications (whether written or oral). The GDPR provides for visualization tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks) where appropriate. Recital 58[46] indicates that the accessibility of information addressed to the public

[46] "Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."
「そのような情報は、例えば、ウェブサイトを介して公衆に伝達される場合には、電子的な方式で提供されうる。この点は、オンライン広告の場合など、関係者の急増や慣行の技術的複雑さから、自らに関連する個人データが収集されているのか否か、また、誰により、どのような目的で収集されているかについ

or to data subjects is especially important in the online environment[47].
49. 重要な点として、GDPR における透明性の原則を実現する方法は、（書面又は口頭にかかわらず）単なる言語的なコミュニケーションに限定されない。GDPR では、必要に応じて、視覚化ツール（特に、図形記号、認証メカニズム並びにデータ保護シール及びマークに言及している）について規定している。前文第 58 項[46]では、公衆又はデータ主体を対象とする情報のアクセス可能性がオンライン環境において特に重要であることを示している[47]。

Icons

アイコン

50. Recital 60 makes provision for information to be provided to a data subject "in combination" with standardized icons, thus allowing for a multi-layered approach. However, the use of icons should not simply replace information necessary for the exercise of a data subject's rights nor should they be used as a substitute to compliance with the data controller's obligations under Articles 13 and 14. Article 12.7 provides for the use of such icons stating that:
50. 前文第 60 項は、標準化されたアイコンと「組み合わせて」データ主体に情報を提供する場合について規定し、多階層的なアプローチを認めている。しかしながら、アイコンの使用は、あくまでもデータ主体の権利の行使に必要な情報に単に代わりうるものではなく、第 13 条及び第 14 条に基づくデータ管理者の義務を遵守する代わりとしても使うべきではない。第 12 条(7)は、次のように述べ、アイコンを利用することを規定している。

"The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where icons are presented electronically they shall be machine-readable".
「第 13 条及び第 14 条によりデータ主体に対して提供される情報は、用意に視認でき、分かりやすく、明確に理解できる様態で、予定されている取扱いの意味のある概要を提供するための標準的なアイコンと組み合わせて提供できる。アイコンが電子的に表示される場合、それらは、機械によって読み取り可能なものとする。

51. As Article 12.7 states that "*Where the icons are presented electronically, they shall be machinereadable*", this suggests that there may be situations where icons are not presented

---

て知り、理解することが困難な状況において特に重要である」。
[47] In this context, controllers should take into account visually impaired data subjects (e.g. red-green colour blindness).
これに関連して、管理者は、視覚障害のあるデータ主体（例えば赤緑色盲など）を考慮に入れるべきである。

electronically, [48] for example icons on physical paperwork, IoT devices or IoT device packaging, notices in public places about Wi-Fi tracking, QR codes and CCTV notices.

51. 第 12 条(7)では「*アイコンが電子的に表示される場合、それらは、機械によって読み取り可能なものとする*」と述べているため、これは、例えば、物理的書類、IoT デバイス又は IoT デバイスパッケージ、公共の場における Wi-Fi トラッキング、QR コード及び CCTV 通知にアイコンが表示される場合など、アイコンが電子的に表示されていない場合があることを示唆している [48]。

52. Clearly, the purpose of using icons is to enhance transparency for data subjects by potentially reducing the need for vast amounts of written information to be presented to a data subject. However, the utility of icons to effectively convey information required under Articles 13 and 14 to data subjects is dependent upon the standardization of symbols/ images to be universally used and recognized across the EU as shorthand for that information. In this regard, the GDPR assigns responsibility for the development of a code of icons to the Commission but ultimately the European Data Protection Board may, either at the request of the Commission or of its own accord, provide the Commission with an opinion on such icons[49]. WP29 recognises that, in line with Recital 166, the development of a code of

---

[48] There is no definition of "machine-readable" in the GDPR but Recital 21 of Directive 2013/37/EU17 defines "machine-readable" as:

"*a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats.*"

GDPR では「機械可読性」について定義していないものの、指令第 2013/37/EU17 号の前文第 21 項では「機械可読性」を次のように定義している。

「ソフトウェアアプリケーションが個人の事実記載を含む特定のデータ及びその内部構造を容易に特定、認識及び抽出できるよう構造化されているファイルフォーマットである。機械可読性のある形式で構造化されているファイルの符号化されたデータは、機械可読性のあるデータである。機械可読性のある形式は、公開又は独占的な形式でもよく、公式な標準形式である場合とそうでない場合がある。自動処理を制限するファイル形式で符号化されている文書については、文書からのデータ抽出が不可能又は容易でないため、機械可読な形式でないとみなされる。加盟国は、適切な場合、公開されている、機械可読な形式の利用を促進すべきである」。

[49] Article 12.8 provides that the Commission is empowered to adopt delegated acts under Article 92 for the purpose of determining the information to be presented by the icons and the information for providing standardised icons. Recital 166 (which deals with delegated acts of the Commission in general) is instructive, providing that the Commission must carry out appropriate consultations during its preparatory work, including at expert level. However, the European Data Protection Board (EDPB) also has an important consultative role to play in relation to the standardisation of icons as Article 70.1(r) states that the EDPB shall on its own initiative or, where relevant, at the request of the Commission, provide the Commission with an opinion on icons.

第 12 条(8)では、欧州委員会が、アイコンによって表示される情報及び標準化されたアイコンを提供するため情報を決定する目的で、第 92 条による委任行為を採択するための権限が与えられると規定する。（欧州委員会に委任される行為全般を扱う）前文第 166 項は有益であり、欧州委員会が、専門家レベルのものを含め、作業を準備する間に適切な協議を行わなければならないと規定している。しかしながら、第 70 条(1)(r)では、欧州データ保護会議（EDPB）が、自身の主導又は、関係があるならば、欧州委員会の要求によりアイコンに関する意見を欧州委員会に提出すると述べているため、EDPB も、アイコンの標準化に関して重要な諮問的役割を果たしている。

icons should be centred upon an evidence-based approach and in advance of any such standardization it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context.
52. 明らかに、アイコンを利用する目的は、膨大な量の書面による情報をデータ主体に提示するわずらわしさを潜在的に軽減することで、データ主体にとっての透明性を高めることである。しかしながら、第 13 条及び第 14 条に基づいて必要とされる情報をデータ主体に効果的に伝える手段としてのアイコンの有用性は、記号／画像が標準化され、その情報の略語として EU 全域で普遍的に使われ、認識されている度合いに左右される。この点に関して、GDPR では、アイコンコードの開発責任を欧州委員会に負わせているものの、欧州データ保護会議は、最終的には委員会の要請又は自らの発意により、そのような図形記号に関する意見を委員会に提出することができる [49]。第 29 条作業部会では、前文第 166 項に従い、証拠に基づいたアプローチを軸にアイコンコードの開発を進めるべきであること、及び、そのような標準化に先立って、産業界及びより広範な公衆と協力し、以上の点との関連におけるアイコンの有効性に関する幅広い研究を行うべきであることを認識している。

Certification mechanisms, seals and marks
認証メカニズム、シール及びマーク

53. Aside from the use of standardized icons, the GDPR (Article 42) also provides for the use of data protection certification mechanisms, data protection seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by data controllers and processors and enhancing transparency for data subjects[50]. WP29 will be issuing guidelines on certification mechanisms in due course.
53. 標準化されたアイコンの使用以外にも、GDPR（第 42 条）では、データ管理者や処理者による取扱業務が GDPR に適合していることを証明し、データ主体にとっての透明性を向上させる目的での、データ保護認証メカニズム、データ保護シール及びマークの使用についても規定している [50]。第 29 条作業部会は、認証メカニズムに関するガイドラインをいずれ発行する予定である。

Exercise of data subjects' rights
データ主体の権利行使

54. Transparency places a triple obligation upon data controllers insofar as the rights of data subjects

[50] See the reference in Recital 100
前文第 100 項の言及を参照。

under the GDPR are concerned, as they must[51]:

54. データ管理者は、透明性の原則により、GDPR に基づくデータ主体の権利が関係する限り、次の三つの義務を負う[51]。

- provide information to data subjects on their rights[52] (as required under Articles 13.2(b) and 14.2(c));
  （第 13 条(2)(b)及び第 14 条(2)(c)に基づき要求されているように）自らの権利に関する情報をデータ主体に提供しなければならない[52]、

- comply with the principle of transparency (i.e. relating to the quality of the communications as set out in Article 12.1) when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34; and
  第 15 条から第 22 条まで及び第 34 条に基づく権利についてデータ主体に連絡する際に（第 12 条(1)に規定する連絡の質に関連して）透明性の原則に従わなければならない、及び

- facilitate the exercise of data subjects' rights under Articles 15 to 22.
  第 15 条から第 22 条までに基づくデータ主体の権利の行使を促進しなければならない。

55. The GDPR requirements in relation to the exercise of these rights and the nature of the information required are designed to *meaningfully position* data subjects so that they can vindicate their rights and hold data controllers accountable for the processing of their personal data. Recital 59 emphasises that "*modalities should be provided for facilitating the exercise of the data subject's rights*" and that the data controller should "*also provide means for requests to be made electronically, especially where personal data are processed by electronic means*". The modality provided by a data controller for data subjects to exercise their rights should be appropriate to the context and the nature of the relationship and interactions between the controller and a data subject. To this end, a data controller may wish to provide one or more different modalities for the exercise of rights that are reflective of the different ways in which data subjects interact with that data controller.

55. これらの権利の行使及び必要とされる情報の性質に関する GDPR の要件は、データ主体を実質的にも、自らの権利を確立し、自分たちの個人データの取扱いについてデータ管理者に説明責任を負わせられる*有利な立場に立たせる*ためのものである。前文第 59 項では、「デ

[51] Under the Transparency and Modalities section of the GDPR on Data Subject Rights (Section 1, Chapter III, namely Article 12)
データ主体の権利に関係する GDPR の透明性及び手続の節（第 3 章 1 節、すなわち第 12 条）に基づく。

[52] Access, rectification, erasure, restriction on processing, object to processing, portability
アクセス、訂正、消去、取扱いの制限、取扱いへの異議、ポータビリティ

ータ主体の権利の行使を容易なものとするため、様式が定められなければならない」こと、また「*特に電子的な方法で個人データが取扱われる場合*」管理者は「*電子的に要求するための方法も提供しなければならない*」ことを強調している。データ主体が自らの権利を行使するためにデータ管理者が提供する手続は、管理者とデータ主体との関係、やり取りの内容や性質に適したものとするべきである。こうした目的のため、データ管理者は、データ主体がそのデータ管理者と互いに連絡を取り合うための様々な方法を反映した権利行使のための一つ若しくは複数の手続を提供したいと考える場合もある。

Example
例

A health service provider uses an electronic form on its website, and paper forms in the receptions of its health clinics, to facilitate the submission of access requests for personal data both online and in person. While it provides these modalities, the health service still accepts access requests submitted in other ways (such as by letter and by email) and provides a dedicated point of contact (which can be accessed by email and by telephone) to help data subjects with the exercise of their rights.
ある医療サービス提供者は、オンラインでのものと対面によるものの両方による個人データのアクセス要求の提出を促進するため、ウェブサイト上での電子フォームと診療所の受付での用紙の両方を利用している。医療サービスは、これらの手続を提供しつつ、他の方法（例えば手紙や電子メール）で提出されたアクセス要求を引き続き受け入れ、データ主体の権利の行使を助けるために（電子メールと電話でアクセスできる）専用の連絡窓口を提供している。

Exceptions to the obligation to provide information
情報提供の義務に対する例外

Article 13 exceptions
第13条の例外

56. The only exception to a data controller's Article 13 obligations where it has collected personal data directly from a data subject occurs "*where and insofar as, the data subject already has the information*" [53]. The principle of accountability requires that data controllers demonstrate (and document) what

[53] Article 13.4

information the data subject already has, how and when they received it and that no changes have since occurred to that information that would render it out of date. Further, the use of the phrase "insofar as" in Article 13.4 makes it clear that even if the data subject has previously been provided with certain categories from the inventory of information set out in Article 13, there is still an obligation on the data controller to supplement that information in order to ensure that the data subject now has a complete set of the information listed in Articles 13.1 and 13.2. The following is a best practice example concerning the limited manner in which the Article 13.4 exception should be construed.

56. データ管理者がデータ主体から個人データを直接収集した場合についてデータ管理者の負う第 13 条に基づく義務に対する唯一の例外が「*データ主体が既にその情報をもっている場合*」である[53]。アカウンタビリティの原則により、データ管理者は、データ主体が既にどのような情報をもち、それをいつどのように受け取り、そのデータ主体の持っている情報が最新のものではなくなってしまうような変化がその後生じていないことを証明（し、文書化）する必要がある。さらに、第 13 条(4)の「している場合に限り」という言葉の使用は、第 13 条に定める情報の目録から一定の種類の情報がデータ主体に過去に提供されていたとしても、データ管理者には、そのデータ主体が第 13 条(1)及び第 13 条(2)に列挙された完全な情報一式を入手できるように確保するためにその情報を補足する義務が依然として存在することを明確にしている。以下は、限定して解釈するべき第 13 条(4)の例外の解釈方法の最も望ましい慣行の例である。

Example
例

An individual signs up to an online email service and receives all of the required Article 13.1 and 13.2 information at the point of sign-up. Six months later the data subject activates a connected instant message functionality through the email service provider and provides their mobile telephone number to do so. The service provider gives the data subject certain Article 13.1 and 13.2 information about the processing of the telephone number (e.g. purposes and legal basis for processing, recipients, retention period) but does not provide other information that the individual already has from 6 months ago and which has not since changed (e.g. the identity and contact details of the controller and the data protection officer, information on data subject rights and the right to complain to the relevant supervisory authority). As a matter of best practice however, the complete suite of information should be provided to the data subject again but the data subject also should be able to easily tell what information amongst it is new. The new processing for the purposes of the instant messaging service may affect the data subject in a way which would prompt them to seek to

[53] 第 13 条（4）

exercise a right they may have forgotten about, having been informed six months prior. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and their rights.
ある個人がオンラインの電子メールサービスに登録し、必要とされる第 13 条(1)及び第 13 条(2)の情報を全て登録時に受け取った。それから 6 か月後に、データ主体が、電子メールサービスプロバイダを通じ、接続されたインスタントメッセージ機能を起動し、そのために携帯電話番号を提供した。サービス提供者は、（例えば取扱目的及び法的根拠、取得者、保存期間など）電話番号の取扱いに関する第 13 条(1)及び第 13 条(2)に基づく一定の情報をデータ主体に提供するものの、（例えば管理者及びデータ保護オフィサーの身元及び連絡先の詳細、データ主体の権利に関する情報及び関連する監督機関に不服を申立てる権利など）その個人が 6 か月前から保有し、それ以降変更されていないその他の情報は提供しない。しかしながら、最良の慣行としては、データ主体に一連の完全な情報を再度提供するべきであるものの、その中のどの情報が新しくなったのかがデータ主体に容易に分かるようにするべきである。インスタントメッセージサービスの目的での新たな取扱いについて、6 か月前に知らされていてデータ主体が忘れていたかもしれない権利を行使することをデータ主体に促すという方法でデータ主体に影響を与えるかもしれない。全ての情報を再度提供すれば、データ主体がデータの使用方法や自らの権利について引き続き十分な情報を得られるようにする上で役に立つ。

Article 14 exceptions
第 14 条の例外

57. Article 14 carves out a much broader set of exceptions to the information obligation on a data controller where personal data has not been obtained from the data subject. These exceptions should, as a general rule, be interpreted and applied narrowly. In addition to the circumstances where the data subject already has the information in question (Article 14.5(a)), Article 14.5 also allows for the following exceptions:
57. 第 14 条は、データ主体から個人データを得ていない場合について、データ管理者の情報義務の例外を大幅に広げている。これらの例外は、原則として狭義に解釈し、適用されるべきである。データ主体が既に問題の情報を保有する状況（第 14 条(5)(a)）に加え、第 14 条(5)も次の例外を認めている。

- The provision of such information is impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical

research purposes or statistical purposes, or where it would make the achievement of the objectives of the processing impossible or seriously impair them;
そのような情報の提供が不可能であるか、又は、過大な負担を要する場合。特に公共の利益のための保管目的、科学的研究若しくは歴史的研究目的又は統計目的のための取扱い、又はそれにより当該取扱いの目的の達成ができない若しくはその達成が損なわれる場合、

· The data controller is subject to a national law or EU law requirement to obtain or disclose the personal data and that the law provides appropriate protections for the data subject's legitimate interests ; or
データ管理者が、個人データを取得又は開示するために規定される国内法又は EU 法の要件に服し、その法律がデータ主体の正当な利益を適切に保護している場合、又は、

· An obligation of professional secrecy (including a statutory obligation of secrecy) which is regulated by national or EU law means the personal data must remain confidential.
（法令の守秘義務を含め）EU 法又は国内法によって規定されている職務上の守秘義務に服するため、個人データが機密のものとして維持しなければならない場合。

Proves impossible, disproportionate effort and serious impairment of objectives
不可能であり、過度の負担を要し、及び目的の達成が深刻に損なわれることが判明する

58. Article 14.5(b) allows for 3 separate situations where the obligation to provide the information set out in Articles 14.1, 14.2 and 14.4 is lifted:
58. 第 14 条(5)(b)では、以下の三つ状況において第 14 条(1)、第 14 条(2)及び第 14 条(4)に定める情報提供義務の適用を除外することを認めている。

(i) Where it proves impossible (in particular for archiving, scientific/ historical research or statistical purposes);
(i) （特に保管目的、科学的若しくは歴史的研究目的又は統計目的のために）それが不可能であることが判明する場合、

(ii) Where it would involve a disproportionate effort (in particular for archiving, scientific/ historical research or statistical purposes); or
(ii) （特に保管目的、科学的若しくは歴史的研究目的又は統計目的のために）それが過度の困難を伴う場合、又は

(iii) Where providing the information required under Article 14.1 would make the achievement of the objectives of the processing impossible or seriously impair them.
(iii) 第 14 条(1)に基づき必要とされる情報を提供した場合、当該取扱いの目的の達成ができないか又は損なわれる場合。

"Proves impossible"
「不可能であることが判明する」

59. The situation where it "proves impossible" under Article 14.5(b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually *prevent it* from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects. The following example demonstrates this.
59. 第 14 条(5)(b)に基づき情報を提供することが「不可能であることが証明されている」状況とは、ある事情には不可能であるか、不可能ではないかの二通りしかないため、全か無か、すなわち不可能の程度という概念は存在しない。このため、データ管理者がこの適用除外を根拠とするのであれば、問題の情報をデータ主体に提供するのを実際に*妨げた*要因を証明しなければならない。一定期間が経過した後、「不可能」にしていた要因がもはや解消され、データ主体に情報を提供することが可能になった場合、データ管理者は直ちにそうするべきである。実務上、情報をデータ主体に提供することが実際に不可能であることをデータ管理者が証明できるような状況はほとんど存在しない。次の例はこのことを示している。

Example
例

A data subject registers for a post-paid online subscription service. After registration, the data controller collects credit data from a credit-reporting agency on the data subject in order to decide whether to provide the service. The controller's protocol is to inform data subjects of the collection of this credit data within three days of collection, pursuant to Article 14.3(a). However, the data subject's address and phone number is not registered in public registries (the data subject is in fact living abroad). The data subject did not leave an email address when registering for the service or the email address is invalid. The controller finds that it has no means to directly contact the data subject. In this case, however, the controller may give information about collection of credit

reporting data on its website, prior to registration. In this case, it would not be impossible to provide information pursuant to Article 14.
データ主体が、後払いのオンライン・購読サービスに登録する。登録後、データ管理者が、サービスを提供するかどうかを決定するために、データ主体の信用データを信用報告機関から収集する。管理者の通常の手順では、第 14 条(3)(a)に従い、収集した日から 3 日以内にこの信用データの収集についてデータ主体に通知しなければならない。しかしながら、データ主体の住所と電話番号がパブリックレジストリに登録されていない（データ主体が実際には海外で生活していた）。データ主体は、サービスに登録する時に電子メールアドレスを残さなかったか、電子メールアドレスが無効である。管理者には、データ主体に直接連絡をとる手段がないことが判明する。しかしながら、管理者は、そのような場合でも、データ主体を登録する前に、信用報告データの収集に関する情報をウェブサイトに表示しうる。このケースでは、第 14 条に従って情報を提供することが不可能ではない。

Impossibility of providing the source of the data
データの情報源を示すことができない場合

60. Recital 61 states that "*where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided*". The lifting of the requirement to provide data subjects with information on the source of their personal data applies only where this is not possible because different pieces of personal data relating to the same data subject cannot be attributed to a particular source. For example, the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by design and by default, [54] transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organization can be tracked and traced back to their source at any point in the data processing life cycle (see paragraph 43 above).
60. 前文第 61 項では、「*様々な情報源が用いられたために、データ主体に対してその個人データの入手元を示すことができない場合には、一般的な情報が提供されなければならない。*」と述べている。同じデータ主体に関するさまざまな個人データの情報源を識別できないため、個人データの情報源に関する情報をデータ主体に提供することができない場合にのみ、そうした情報を提供する要件の適用が除外される。例えば、データ管理者が複数の情報源を

[54] Article 25
第 25 条

利用して複数のデータ主体の個人データを含むデータベースを構築しているという事実のみでは、（時間がかかり、煩わしいにしても）個々のデータ主体の個人データの情報源を識別することが可能な場合、この要件の適用が除外されるには足りない。データ保護バイデザインとデータ保護バイデフォルトの要件 [54] を考慮すると、組織が受け取った個人データの全ての情報源を追跡し、データの取扱いのサイクルの任意の時点で情報源に遡って追跡できるよう、透明性に関する仕組みを初めから取扱システムに組み込むべきである（上記 43 項を参照）。

"Disproportionate effort"
「過度の負担」

61. Under Article 14.5(b), as with the "proves impossible" situation, "disproportionate effort" may also apply, in particular, for processing "*for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the safeguards referred to in Article 89(1)*". Recital 62 also references these objectives as cases where the provision of information to the data subject would involve a disproportionate effort and states that in this regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration. Given the emphasis in Recital 62 and Article 14.5(b) on archiving, research and statistical purposes with regard to the application of this exemption, WP29's position is that this exception should not be *routinely* relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes. WP29 emphasises the fact that where these are the purposes pursued, the conditions set out in Article 89.1 must still be complied with and the provision of the information must constitute a disproportionate effort.

61. 第 14 条(5)(b)のもとでは、「不可能であることが判明する」場合と同様、「過度の負担を要する」場合が、特に、「*第 89 条(1)に定める保護措置による公共の利益における保管目的、科学的若しくは歴史的研究目的又は統計目的*」のための取扱いに適用される場合がある。また、前文第 62 項でも、これらの目的について、データ主体への情報提供に過度な負担を伴う場合であると言及し、このことに関して、データ主体の人数、データの経過年数及び導入されている適切な保護措置を考慮に入れるべきだと述べている。前文第 62 項及び第 14 条(5)(b)においてこの除外が適用される場合として保管、研究及び統計目的が強調されている点を考慮すると、公共の利益のための保管目的、科学的又は歴史的研究目的又は統計目的のために個人データを取扱っていないデータ管理者が、この例外を*規定どおりに*主張することはできないというのが第 29 条作業部会の見解である。第 29 条作業部会は、これらの目的を追求している場合でも、第 89 条(1)に定める条件を依然として遵守しなければならず、情報の提供が過度な負担を構成するものでなければならないという事実を強調する。

62. In determining what may constitute either impossibility or disproportionate effort under Article 14.5(b), it is relevant that there are no comparable exemptions under Article 13 (where personal data is collected from a data subject). The only difference between an Article 13 and an Article 14 situation is that in the latter, the personal data is not collected from the data subject. It therefore follows that impossibility or disproportionate effort typically arises by virtue of circumstances which do not apply if the personal data is collected from the data subject. In other words, the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject.

62. 何が第 14 条(5)(b)にいう不可能又は過度な負担を構成するかを判断する際、第 13 条（個人データをデータ主体から収集する場合）には、これに相当するような、適用除外が存在しない点が重要である。第 13 条の状況と第 14 条の状況との違いは唯一、後者の場合、個人データをデータ主体から収集していない点である。したがって、不可能又は過度な負担が通常、個人データをデータ主体から収集している場合にはあてはまらないような状況から生じることが分かる。換言すれば、不可能又は過度な負担は、個人データをデータ主体以外の者から取得したという事実に直接関連するものでなければならない。

Example
例

A large metropolitan hospital requires all patients for day procedures, longer-term admissions and appointments to fill in a Patient Information Form which seeks the details of two next-of-kin (data subjects). Given the very large volume of patients passing through the hospital on a daily basis, it would involve disproportionate effort on the part of the hospital to provide all persons who have been listed as next-of-kin on forms filled in by patients each day with the information required under Article 14.

首都圏の大病院では、2 人の近親者（データ主体）の詳細な情報を得る患者情報用紙に記入することを、通院、長期入院、及び予約する全ての患者に求めている。極めて大勢の患者が病院を日々やって来ては出て行く点を考えると、患者が毎日記入する用紙において近親者として記入された全ての人々に第 14 条に基づき必要とされる情報を提供することは病院にとって過度な負担を伴う。

63. The factors referred to above in Recital 62 (number of data subjects, the age of the data and any appropriate safeguards adopted) may be indicative of the types of issues that contribute to a data controller having to use disproportionate effort to notify a data subject of the relevant Article 14

information.

63. 上記の前文第 62 項（データ主体の人数、データの経過年数及び導入されている適切な保護措置）に定められる要素は、データ管理者が関連する第 14 条の情報をデータ主体に通知するために過度な負担をしなければならない原因となるような問題のタイプを示唆している可能性がある。

Example
例

Historical researchers seeking to trace lineage based on surnames indirectly obtain a large dataset relating to 20,000 data subjects. However, the dataset was collected 50 years ago, has not been updated since, and does not contain any contact details. Given the size of the database and more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually in order to provide them with Article 14 information.
姓に基づいて家系を追跡しようとする歴史研究者が、2 万人のデータ主体に関する大きなデータセットを間接的に取得した。しかしながら、このデータセットは 50 年前に収集され、以来更新されておらず、連絡先に関する詳細な情報も含まれていない。データベースの規模、それ以上にデータの古さを考慮すると、研究者が、第 14 条の情報をデータ主体に提供するためにデータ主体を個別に追跡することは過度な負担を伴う。

64. Where a data controller seeks to rely on the exception in Article 14.5(b) on the basis that provision of the information would involve a disproportionate effort, it should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations. In such a case, Article 14.5(b) specifies that the controller must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests. This applies equally where a controller determines that the provision of the information proves impossible, or would likely render impossible or seriously impair the achievement of the objectives of the processing. One appropriate measure, as specified in Article 14.5(b), that controllers must always take is to make the information publicly available. A controller can do this in a number of ways, for instance by putting the information on its website, or by proactively advertising the information in a newspaper or on posters on its premises. Other appropriate measures, in addition to making the information publicly available, will depend on the circumstances of the processing, but may include: undertaking a data protection impact assessment; applying pseudonymisation techniques to the data; minimizing the data collected and the

storage period; and implementing technical and organizational measures to ensure a high level of security. Furthermore, there may be situations where a data controller is processing personal data which does not require the identification of a data subject (for example with pseudonymised data). In such cases, Article 11.1 may also be relevant as it states that a data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR.

64. 情報の提供に過度な負担が伴うことを理由にデータ管理者が第 14 条(5)(b)の例外を根拠とした場合、データ管理者は、情報提供を受けなかった場合のデータ主体への影響及び効果に対して、データ主体に情報を提供するのに伴う困難についてバランスをとる方法で評価するべきである。データ管理者は、自らのアカウンタビリティに関する義務に従い、この評価を文書化するべきである。そのような場合について、第 14 条(5)(b)では、データ主体の権利、自由及び正当な利益を保護するための適切な措置を講じなければならないと規定している。これは、同様に情報の提供が、不可能であることが証明されているか又は取扱う目的の達成を不可能にする若しくは深刻に損なう可能性が高いと管理者が判断した場合にも適用される。第 14 条(5)(b)に規定されているように、管理者は、適切な措置として、常に情報を公に利用できるようにする措置を講じなければならない。管理者がそうするには、例えばウェブサイトに情報を載せたり、新聞や敷地内のポスターに積極的に広告を出したりなど、幾つかの方法がある。情報を一般に公開することに加え、その他の適切な措置としては、取扱いの状況にもよるものの、次のものが考えられる。すなわち、データ保護影響評価を実施すること、データに仮名化の技法を適用すること、収集するデータの最小化と保存期間の最短化、高いレベルのセキュリティを確保するための技術的及び組織的措置を実施すること、といったものである。さらに、データ管理者が（例えば、仮名化されたデータなど）データ主体の識別を必要としない個人データを取り扱っている場合もある。第 11 条(1)では、そのような場合について、管理者が、単に GDPR を遵守するという目的のために、データ主体を識別するため、追加の情報を維持、取得又は取扱いしなければならないという義務を負わないと述べているので、第 11 条(1)が関わってくる可能性がある。

Serious impairment of objectives

目的が深刻に損なわれる場合

65. The final situation covered by Article 14.5(b) is where a data controller's provision of the information to a data subject under Article 14.1 is likely to make impossible or seriously impair the achievement of the processing objectives. To rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14.1 alone would nullify the objectives of the processing. Notably, reliance on this aspect of Article 14.5(b) presupposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances,

the processing of the personal data is fair and that it has a legal basis.

65. 第 14 条(5)(b)で扱っている最後の状況は、第 14 条(1)に基づくデータ管理者によるデータ主体への情報提供が当該取扱いの目的を不可能にする若しくは深刻に損なう場合である。データ管理者が、この例外を根拠とするためには、第 14 条(1)に定められた情報の提供だけで、取扱いの目的を台無しにすることを証明しなければならない。特に、第 14 条(5)(b)のこの側面を根拠とするには、データの取扱いが第 5 条に定める全ての原則を満たし、かつ最も重要な点として、全ての状況において、個人データの取扱いが公正であり、法的根拠を備えていることが前提になる。

Example
例

Bank A is subject to a mandatory requirement under anti-money laundering legislation to report suspicious activity relating to accounts held with it to the relevant financial law enforcement authority. Bank A receives information from Bank B (in another Member State) that an account holder has instructed it to transfer money to another account held with Bank A which appears suspicious. Bank A passes this data concerning its account holder and the suspicious activities to the relevant financial law enforcement authority. The anti-money laundering legislation in question makes it a criminal offence for a reporting bank to "tip off" the account holder that they may be subject to regulatory investigations. In this situation, Article 14.5(b) applies because providing the data subject (the account holder with Bank A) with Article 14 information on the processing of account holder's personal data received from Bank B would seriously impair the objectives of the legislation, which includes the prevention of "tip-offs". However, general information should be provided to all account holders with Bank A when an account is opened that their personal data may be processed for anti-money laundering purposes.

銀行 A には、マネーロンダリング防止法の下で、自行が保有する口座に関係する不審な活動について、関連する金融法執行当局に報告するという義務的な要件に従わねばならない。銀行 A は（他の加盟国にある）銀行 B から、銀行 B がある口座の名義人より、銀行 A に保有されている疑わしいと思われる別の口座に資金を送金するよう指示を受けたという情報を受け取る。銀行 A は、この口座名義人と疑わしい活動に関するデータを関連する金融法執行当局に渡す。問題のマネーロンダリング防止法では、口座名義人が規制当局の調査の対象となる可能性があることについて報告銀行が名義人に「情報を与える」場合に犯罪になるとしている。この状況では、銀行 B から受け取った口座名義人の個人データの取扱いに関する第 14 条の情報をデータ主体（銀行 A の口座名義人）に提供することが「情報を与えること」の防止を含む法律の目的を著しく損なうため、第 14 条(5)(b)が適用される。しかしながら、個人データがマネーロンダリング防止法目的で取り扱われ

る可能性があるという一般的情報を口座開設時に銀行 A の全ての口座名義人に提供するべきである。

Obtaining or disclosing is expressly laid down in law
取得又は開示が法律に明記されている場合

66. Article 14.5(c) allows for a lifting of the information requirements in Articles 14.1, 14.2 and 14.4 insofar as the obtaining or disclosure of personal data "*is expressly laid down by Union or Member State law to which the controller is subject*". This exemption is conditional upon the law in question providing "*appropriate measures to protect the data subject's legitimate interests*". Such a law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. Accordingly, the data controller must be able to demonstrate how the law in question applies to them and requires them to either obtain or disclose the personal data in question. While it is for Union or Member State law to frame the law such that it provides "*appropriate measures to protect the data subject's legitimate interests*", the data controller should ensure (and be able to demonstrate) that its obtaining or disclosure of personal data complies with those measures. Furthermore, the data controller should make it clear to data subjects that it obtains or discloses personal data in accordance with the law in question, unless there is a legal prohibition preventing the data controller from doing so. This is in line with Recital 41 of the GDPR, which states that a legal basis or legislative measure should be clear and precise, and its application should be foreseeable to persons subject to it, in accordance with the case law of the Court of Justice of the EU and the European Court of Human Rights. However, Article 14.5(c) will not apply where the data controller is under an obligation to obtain data *directly from a data subject*, in which case Article 13 will apply. In that case, the only exemption under the GDPR exempting the controller from providing the data subject with information on the processing will be that under Article 13.4 (i.e. where and insofar as the data subject already has the information). However, as referred to below at paragraph 68, at a national level, Member States may also legislate, in accordance with Article 23, for further specific restrictions to the right to transparency under Article 12 and to information under Articles 13 and 14.
66. 第 14 条(5) (c)では、個人データの取得又は開示が「*管理者が服する EU 法又は加盟国の国内法によって明確に規定されている*」限り、第 14 条(1)、第 14 条(2)及び第 14 条(4)の情報に関する要件の適用除外を認めている。この適用除外は、当該法律が「*データ主体の正当な利益を保護するための適切な措置*」を定めていることが条件となる。そのような法律はデータ管理者に直接適用されるものでなければならず、また、当該の取得又は開示は、データ管理者に義務的なものでなければならない。したがって、データ管理者は、当該法律が自分たちにどのように適用され、それにより当該個人データを取得又は開示するよう自分たちが

どう求められているかを証明できなければならない。「*データ主体の正当な利益を保護するための適切な措置*」を規定するのは連合又は加盟国の法律の問題であるものの、データ管理者は、自らによる個人データの取得又は開示がそうした措置に適合するように（し、これを証明）する必要がある。さらに、データ管理者は、データ管理者が当該法律に従って個人データを取得又は開示することをデータ主体に明らかにするのを禁止する法規定が存在しない限り、この点を明らかにするべきである。これは、そのような法的根拠又は立法上の措置は、欧州連合司法裁判所及び欧州人権裁判所の判例法に従い、明確かつ適正なものであることを要し、また、その適用は、それが適用される者にとって予見可能なものでなければならないと述べる GDPR の前文第 41 項と一致する。しかしながら、データ管理者が*データ主体から直接*データを取得する義務を負っている場合には第 14 条（5）(c)が適用されず、第 13 条が適用される。その場合、取扱いに関する情報をデータ主体に提供するデータ管理者の義務を免除する GDPR の規定は、第 13 条（4）のみである（すなわち、データ主体が既に情報を所持している場合に限られる）。しかしながら、以下の 68 項で言及するように、加盟国は、第 23 条に従い、第 12 条に基づく透明性に対する権利と第 13 条及び第 14 条に基づく情報に対する権利の追加的具体的な制限を国内法で定めることができる。

Example
例

A tax authority is subject to a mandatory requirement under national law to obtain the details of employees' salaries from their employers. The personal data is not obtained from the data subjects and therefore the tax authority is subject to the requirements of Article 14. As the obtaining of the personal data by the tax authority from employers is expressly laid down by law, the information requirements in Article 14 do not apply to the tax authority in this instance.
税務当局は、国内法に基づき従業員の給与の詳細を雇用主から取得する義務的要件に服する。個人データをデータ主体から取得してないため、税務当局には第 14 条の要件が適用される。税務当局による雇用主からの個人データの取得については法律で明示されているため、第 14 条の情報に関する要件はこの場合における税務当局には適用されない。

Confidentiality by virtue of a secrecy obligation
秘密保持義務による秘密保持

67. Article 14.5(d) provides for an exemption to the information requirement upon data controllers where the personal data "*must remain confidential subject to an obligation of professional secrecy*

regulated by Union or Member State law, including a statutory obligation of secrecy". Where a data controller seeks to rely on this exemption, it must be able to demonstrate that it has appropriately identified such an exemption and to show how the professional secrecy obligation directly addresses the data controller such that it prohibits the data controller from providing all of the information set out in Articles 14.1, 14.2 and 14.4 to the data subject.

67. 第 14 条(5)(d)では、個人データを「*制定法上の守秘義務の場合を含め、EU 法又は加盟国の国内法によって規律される職務上の守秘義務によって、機密のものとして維持しなければならない場合*」について、データ管理者に対する情報に関する要件の適用除外を規定している。データ管理者がこの適用除外を根拠としたい場合、そのような適用除外を適切に識別したこと、また、職務上の守秘義務がデータ管理者に直接適用されるため、第 14 条(1)、第 14 条(2)及び第 14 条(4)に定められたすべての情報をデータ管理者がデータ主体に提供することを禁止していることを証明できなければならない。

Example
例

A medical practitioner (data controller) is under a professional obligation of secrecy in relation to his patients' medical information. A patient (in respect of whom the obligation of professional secrecy applies) provides the medical practitioner with information about her health relating to a genetic condition, which a number of her close relatives also have. The patient also provides the medical practitioner with certain personal data of her relatives (data subjects) who have the same condition. The medical practitioner is not required to provide those relatives with Article 14 information as the exemption in Article 14.5(d) applies. If the medical practitioner were to provide the Article 14 information to the relatives, the obligation of professional secrecy, which he owes to his patient, would be violated.

医師（データ管理者）が、患者の医療情報に関して職務上の守秘義務を負っている。（職務上の守秘義務が適用される対象である）患者は、多くの近親者に存在する遺伝的状態に関係する自らの健康情報を医師に提供する。また、患者は、同じ状態にある親戚（データ主体）に関する一定の個人データも医師に提供する。第 14 条(5)(d)の適用除外に該当するため、医師が、これらの親族に第 14 条の情報を提供する必要はない。医師が第 14 条の情報を親族に提供する場合、患者に負う職務上の守秘義務違反となる。

Restrictions on data subject rights
データ主体の権利に関する制限

68. Article 23 provides for Member States (or the EU) to legislate for further restrictions on the scope of the data subject rights in relation to transparency and the substantive data subject rights[55] where such measures respect the essence of the fundamental rights and freedoms and are necessary and proportionate to safeguard one or more of the ten objectives set out in Article 23.1(a) to (j). Where such national measures lessen either the specific data subject rights or the general transparency obligations, which would otherwise apply to data controllers under the GDPR, the data controller should be able to demonstrate how the national provision applies to them. As set out in Article 23.2(h), the legislative measure must contain a provision as to the right of the data subject to be informed about a restriction on their rights, unless so informing them may be prejudicial to the purpose of the restriction. Consistent with this, and in line with principle of fairness, the data controller should also inform data subjects that they are relying on (or will rely on, in the event of a particular data subject right being exercised) such *a national legislative restriction* to the exercise of data subject rights, or to the transparency obligation, unless doing so would be prejudicial to the purpose of the legislative restriction. As such, transparency requires data controllers to provide adequate upfront information to data subjects about their rights and any particular caveats to those rights which the controller may seek to rely on, so that the data subject is not taken by surprise at a purported restriction of a particular right when they later attempt to exercise it against the controller. In relation to pseudonymisation and data minimisation, and insofar as data controllers may purport to rely on Article 11 of the GDPR, WP29 has previously confirmed in Opinion 3/ 2017[56] that Article 11 of the GDPR should be interpreted as a way of enforcing genuine data minimization without hindering the exercise of data subject rights, and that the exercise of data subject rights must be made possible with the help of additional information provided by the data subject.

68. 第 23 条では、措置が、基本的権利及び自由の本質を尊重し、第 23 条(1)(a)から(j)に定められた 10 の目的のうち一つ、若しくは複数を守るために必要かつ相応である場合に、透明性とデータ主体の実体的権利との関連で、データ主体の権利の範囲をさらに制限する規定を加盟国（又は EU）が設けることを認めている[55]。そのような国内措置によって GDPR の下でデータ管理者に本来適用されるデータ主体の特定の権利又は一般的な透明性に関する

[55] As set out in Articles 12 to 22 and 34, and in Article 5 insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.
その提供が第 12 条から第 22 条までに規定されている権利及び義務に適合する限り、第 12 条から第 22 条まで及び第 34 条並びに第 5 条に定めるとおり。

[56] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) – see paragraph 4.2
協調高度道路交通システム（C-ITS）との関係における個人データの取扱いに関する意見第 03/2017 号 - 4.2 項を参照。

義務が軽減される場合、データ管理者は、国内規定が自らにどう適用されるかを証明できる必要がある。第 23 条（2）(h)に規定されているように、制限の目的に妨げうるものでないならば、制限に関する通知を受けるデータ主体の権利に関する規定を立法措置に含めなければならない。また、これと一致し、公正さの原則に沿って、データ管理者は、データ主体の特定の権利の行使又は透明性の義務を国内法により制限することが当該制限を設ける国内法の目的を妨げうるものでない限り、*国内法を根拠としてそのような制限*を加えている（又は、データ主体の特定の権利が行使された際に加える）こともデータ主体に通知するべきである。したがって、データ管理者は、透明性に基づき、データ主体が後に管理者に対して自らの権利を行使しようと試みた際に、自らの主張する特定の権利の制限がデータ主体にとって不意打ちとなることのないよう、データ主体の権利と、管理者自らが根拠にする可能性のある権利への制限事項に関する十分な情報をデータ主体に提供する必要がある。仮名化とデータの最小化に関連して、また、データ管理者が GDPR 第 11 条を根拠にしていると主張できる限りにおいて、第 29 条作業部会が意見第 3/2017 号 [56] において以前確認したように、GDPR 第 11 条は、データ主体の権利の行使を妨げることなくデータの純粋な最小化を実施する方法であると解釈すべきであること、またデータ主体の権利の行使はデータ主体によって提供される追加情報を利用して可能にしなければならない。

69. Additionally, Article 85 requires Member States, by law, to reconcile data protection with the right to freedom of expression and information. This requires, amongst other things, that Member States provide for appropriate exemptions or derogations from certain provisions of the GDPR (including from the transparency requirements under Articles 12 - 14) for processing carried out for journalistic, academic, artistic or literary expression purposes, if they are necessary to reconcile the two rights.
69. さらに、第 85 条では、個人データの保護と表現及び情報の自由に関する権利とを法律によって調和させるよう加盟国に求めている。これには、とりわけ、二つの権利を調和させる必要がある場合、加盟国が、報道の目的及び学術的、美術的又は文学的表現の目的での取扱いについて、GDPR の（第 12 条から 14 条までの透明性に関する要件の規定を含む）一定の規定の適切な適用除外又は例外を定める必要がある。

Transparency and data breaches
透明性及びデータ侵害

70. WP29 has produced separate Guidelines on Data Breaches[57] but for the purposes of these guidelines, a data controller's obligations in relation to communication of data breaches to a data

[57] Guidelines on Personal data breach notification under Regulation 2016/679, WP 250
2016/679 規則に基づく個人データ侵害の通知に関するガイドライン、WP 250

subject must take full account of the transparency requirements set out in Article 12[58]. The communication of a data breach must satisfy the same requirements, detailed above (in particular for the use of clear and plain language), that apply to any other communication with a data subject in relation to their rights or in connection with conveying information under Articles 13 and 14.

70. 第 29 条作業部会では、データ侵害に関するガイドライン[57]を別途作成したものの、これらのガイドラインの目的上、データ主体に対するデータ侵害の通知に関するデータ管理者の義務については、第 12 条に定められた透明性の要件を十分に考慮しなければならない[58]。データ侵害の通知は、（特に明瞭かつ平易な言語の使用に関する）上記に詳述したデータ主体の権利に関する又は第 13 条及び第 14 条に基づく情報の伝達に関連するデータ主体とその他の通知に適用されるものと同じ要件を満たさなければならない。

[58] This is made clear by Article 12.1 which specifically refers to "…any communication under Articles 15 to 22 **and 34** relating to processing to the data subject..." {emphasis added}.
「取扱いに関する第 15 条から第 22 条**及び第 34 条**に定める通知をデータ主体に」と明記する第 12 条 1 項がこの点について明確にしている[強調追加]。

Annex
附属書

Information that must be provided to a data subject under Article 13 or Article 14
第 13 条又は第 14 条に基づきデータ主体に提供されなければならない情報

Required Information Type 必要な情報の種類	Relevant article (if personal data collected directly from data subject) 関連条文（個人データをデータ主体から直接収集した場合）	Relevant article (if personal data not obtained from the data subject) 関連条文（個人データをデータ主体から取得していない場合）	WP29 comments on information requirement 情報に関する要件に関する第 29 条作業部会のコメント
The identity and contact details of the controller and, where applicable, their representative [59] *管理者、また該当する場合はその担当者の身元と連絡先の詳細*[59]	Article 13.1(a) 第 13 条(1)(a)	Article 14.1(a) 第 14 条(1)(a)	This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address, etc.) この情報により、管理者の容易な識別が可能になるはずであり、また望ましくは、データ管理者とのさまざまな方法での通知（例えば電話番号、電子メールアドレス、郵送先など）が可能になるはずである。

[59] As defined by Article 4.17 of the GDPR (and referenced in Recital 80), "representative" means a natural or legal person established in the EU who is designated by the controller or processor in writing under Article 27 and represents the controller or processor with regard to their respective obligations under the GDPR.
GDPR 第 4 条（17）で定義（し、前文第 80 項で言及）しているように、「代理人」とは、第 27 条により管理者又は処理者によって書面で指名され、GDPR に基づく管理者又は処理者の各々の義務に関して彼等の代理をする EU 域内におかれた自然人又は法人をいう。

This obligation applies where, in accordance with Article 3.2, the controller or processor is not established in the EU but processes the personal data of data subjects who are in the EU, and the processing relates to the offer of goods or services to, or monitoring of the behaviour of, data subjects in the EU.
この義務は、第 3 条（2）に従い、管理者又は処理者が EU 内に拠点を持たないものの、EU 域内のデータ主体の個人データを取扱い、かつその取扱いが EU 域内のデータ主体への商品や役務の提供又はその行動のモニタリングに関連する場合に適用される。

Contact details for the data protection officer, where applicable 該当する場合、データ保護オフィサーの連絡先の詳細	Article 13.1(b) 第 13 条(1)(b)	Article 14.1(b) 第 14 条(1)(b)	See WP29 Guidelines on Data Protection OfficersG[60] データ保護オフィサーに関する第 29 条作業部会ガイドラインを参照 [60]
The purposes and legal basis for the processing 取扱目的とその法的根拠	Article 13.1(c) 第 13 条(1)(c)	Article 14.1(c) 第 14 条(1)(c)	In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security measures based on Article 6.1 is processed, where applicable the relevant Union or Member State law under which the processing is carried out should be specified. 個人データについて予定されている取扱いの目的を述べることに加え、第 6 条に基づき主張している関連する法的根拠を明示しなければならない。特別な種類の個人データの場合、第 9 条の関連規定（及び関連する場合には、データの取扱いを規律する EU 法又は加盟国の適用法）を明記するべきである。第 10 条に従い、第 6 条(1)に基づく有罪判決及び犯罪又はこれらに関連する安全管理措置に関係する個人データが

[60] Guidelines on Data Protection Officers, WP243 rev.01, last revised and adopted on 5 April 2017
データ保護オフィサーに関するガイドライン、WP243 rev.01（2017 年 4 月 5 日に最後に改訂及び採択された）

			取扱われる場合において、該当する場合には、取扱いが行われる根拠となるEU 法又は加盟国の法律を明示するべきである。
Where legitimate interests (Article 6.1(f)) is the legal basis for the processing, the legitimate interests pursued by the data controller or a third party 正当な利益（第 6 条(1)(f)）が取扱いの法的根拠とされている場合には、データ管理者又は第三者の追求する正当な利益	Article 13.1(d) 第 13 条(1)(d)	Article 14.2(b) 第 14 条(2)(b)	The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the controller can also provide the data subject with the information from the *balancing test,* which must be carried out to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data. To avoid information fatigue, this can be included within a layered privacy statement/ notice (see paragraph 35). In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the *balancing test* upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority. 当該利益は、データ主体の利益になるよう識別しなければならない。最も望ましい慣行の観点から、管理者は、*バランシングテスト*から得た情報をデータ主体に提供してもよく、それは取扱いの合法的な根拠として第 6 条(1)(f)を主張するためにデータ主体の個人データを収集する前に実施しなければならない。情報疲労を避けるため、これを階層的なプライ

			バシーステートメント／通知に含めてもよい（35 項を参照）。いずれにせよ、請求すればバランシングテストに関する情報を取得できることをデータ主体に提供する情報に明示すべきであるというのが第 29 条作業部会の見解である。これは、バランシングテストが公正に実施されたかどうかをめぐってデータ主体に疑問があるか又は彼らが監督機関に不服を申し立てたい場合に効果的な透明性を実現する上で不可欠である。
Categories of personal data concerned 関係する個人データの種類	Not required 不要	Article 14.1(d) 第 14 条(1)(d)	This information is required in an Article 14 scenario because the personal data has not been obtained from the data subject, who therefore lacks an awareness of which categories of their personal data the data controller has obtained. 第 14 条の場合では、個人データをデータ主体から取得しておらず、データ管理者がどの種類の個人データを取得しているかについてデータ主体が意識していないため、この情報が必要である。
Recipients [61] (or categories of recipients) of the personal data 個人データの取得者[61]（又は取得者の種類）	Article 13.1(e) 第 13 条(1)(e)	Article 14.1(e) 第 14 条(1)(e)	The term “recipient” is defined in Article 4.9 as *“a natural or legal person, public authority, agency or another body, to which the personal data are disclosed,* ***whether a third party or not****” [emphasis added]*. As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data

[61] As defined by Article 4.9 of the GDPR and referenced in Recital 31
GDPR 第 4 条(9)で定義され、前文第 31 項で言及しているとおり。

			is transferred or disclosed are covered by the term “recipient” and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients. 「取得者」という用語は、第 4 条(9)において「***第三者であるか否かにかかわらず***、*データの開示を受ける自然人、法人、公的機関、行政機関又はその他の団体」［強調追加］*であると定義されている。このため、取得者が第三者である必要はない。したがって、データの移転又は開示を受ける他のデータ管理者、共同管理者及び処理者は「取得者」という用語の範囲に含まれ、第三者の取得者に関する情報に加え、そのような取得者に関する情報が提供されるべきである。 個人データの実際の（記名された）取

			得者又は取得者の種類を提示しなければならない。公正さの原則に従い、管理者は、データ主体にとって最も意味のある取得者に関する情報を提供しなければならない。実際には、データ主体が自分の個人データを保有する者を正確に知ることができるよう、一般に記名された取得者の情報がこれに該当する。管理者が取得者の種類を提示することを選択した場合、(取得者が実施する活動に言及することによる) 取得者のタイプ、業界、産業部門及び産業部門の下位区分、及び取得者の場所を示すなど、できる限り具体的な情報を提示すべきである。
Details of transfers to third countries, the fact of same and the details of the relevant safeguards[62] (including the existence or absence of a Commission adequacy decision [63]) and the means to obtain a copy of them or where they have been made available 第三国への移転の詳細、移転の事実及び関連する保護措置 [62] の詳細 (委員会による十	Article 13.1(f) 第 13 条(1)(f)	Article 14.1(f) 第 14 条(1)(f)	The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 45/ binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean

[62] As set out in Article 46.2 and 46.3
第 46 条(2)及び第 46 条(3)で定めるとおり。
[63] In accordance with Article 45
第 45 条に従う。

分性決定の有無を含む[63]) 及びそれらのコピーを入手する方法又はどこで利用可能となっているか。			that the third countries be named. 移転及び対応する仕組みを可能にする GDPR の関連条文（例えば、第 45 条に基づく十分性決定／第 47 条に基づく拘束的企業準則／第 46 条(2)に基づく標準的なデータ保護条項／第 49 条に基づく例外及び保護措置等）を明示すべきである。また、例えば利用するメカニズムへのリンクを提供するなどにより、関連する文書にアクセスできる又はこれを取得できる場所及び方法に関する情報も提供するべきである。公正さの原則に従い、第三国への移転について提供される情報は、データ主体にとってできる限り意味のあるものとするべきであり、これは一般に、第三国の国名が表示されることを意味する。
The storage period (or if not possible, criteria used to determine that period) 保存期間（又はそれが可能ではない場合には、その期間を決定するために利用される基準）	Article 13.2(a) 第 13 条(2)(a)	Article 14.2(a) 第 14 条(2)(a)	This is linked to the data minimization requirement in Article 5.1(c) and storage limitation requirement in Article 5.1(e). The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or

			different processing purposes, including where appropriate, archiving periods. これは、第 5 条(1)(c)のデータ最小化に関する要件と第 5 条（1）(e)の保管の制限に関する要件と関連している。 保存期間（又はそれを決定する基準）は、法で定められた要件や業界のガイドラインなどの要素によって決まるものの、データ主体が、それぞれのデータ／目的に応じ、自分の状況に基づいて適切な保存期間を評価できるような方法で表現するべきである。データ管理者が、取扱うための正当な目的に必要な限り個人データを保管する等、包括的に述べるのみでは不十分である。関連する場合には、適切な場合に保存期間を定めることを含め、個人データの種類及び又はそれぞれの取扱いの目的に応じた異なる保存期間を定めるべきである。

The rights of the data subject to: • access; • rectification; • erasure; • restriction on processing; • objection to processing and • portability. データ主体の次の権利。 • アクセス、 • 訂正、 • 消去、 • 取扱いの制限、 • 取扱いに対する異議 • ポータビリティ。	Article 13.2(b) 第 13 条(2)(b)	Article 14.2(c) 第 14 条(2)(c)	This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right (see paragraph 68 above). In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.[64] In relation to the right to portability, see WP29 Guidelines on the right to data portability.[65] この情報は、取り扱う場合に固有のものとし、権利に付随する内容、データ主体がその権利を行使するための措置を講じる方法及び権利に対する制限の概要を含めるべきである（上記 68 項を参照）。 特に、取扱いに異議を述べる権利は、遅くともデータ主体への初めての通知時にデータ主体にはっきりとした形で知らされなければならず、明瞭にかつ他の情報とは分けて提示されなければならない[64]。 ポータビリティの権利については、データポータビリティの権利に関する第 29 条作業部会ガイドラインを参照[65]。

[64] Article 21.4 and Recital 70 (which applies in the case of direct marketing)
第 21 条(4)及び前文第 70 項（ダイレクトマーケティングの場合に適用される）

[65] Guidelines on the right to data portability, WP 242 rev.01, last revised and adopted on 5 April 2017
データポータビリティの権利に関するガイドライン、WP 242 rev.01（2017 年 4 月 5 日に最後に改訂及び採択された）

Where processing is based on consent (or explicit consent), the right to withdraw consent at any time 取扱いが同意（又は明示的同意）に基づくものである場合、同意を随時取り消す権利	Article 13.2(c) 第 13 条(2)(c)	Article 14.2(d) 第 14 条(2)(d)	This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.[66] この情報には同意を撤回する方法を含めるべきであり、データ主体にとって同意を撤回することが同意するのと同程度に容易なものとなるよう配慮する[66]。
The right to lodge a complaint with a supervisory authority 監督機関に不服を申し立てる権利	Article 13.2(d) 第 13 条(2)(d)	Article 14.2(e) 第 14 条(2)(e)	This information should explain that, in accordance with Article 77, a data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or of an alleged infringement of the GDPR. この情報では、第 77 条に従い、特に常居所、職場、又は問題とされる GDPR 違反の起きた場所の加盟国の監督機関に不服申立てを行う権利がデータ主体にあることを説明するべきである。
Whether there is a statutory or contractual requirement to provide the information or whether it is necessary to enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure.	Article 13.2(e) 第 13 条(2)(e)	Not required 不要	For example in an employment context, it may be a contractual requirement to provide certain information to a current or prospective employer. Online forms should clearly identify which fields are “required”, which are not, and what will be the consequences of not filling in the required fields. 例えば雇用関係であれば、現在又は見込みの雇用主に一定の情報を提供する契約上の要件がこれに該当する可

[66] Article 7.3
第 7 条(3)

情報を提供する法的若しくは契約上の要件が存在するかどうか、又は契約を締結する必要があるかどうか、又は情報を提供する義務が存在するかどうか、及びそうしなかった場合に考えられる結果。			能性がある。 オンラインフォームでは、どのフィールドが「必須」であり、また必須ではないか、及び必須フィールドに入力しなかった場合の結果を明示すべきである。
The source from which the personal data originate, and if applicable, whether it came from a publicly accessible source 個人データが発生した情報源、もしあてはまるならば、一般の人々がアクセスできる情報源から来たものであるか否か	Not required 不要	Article 14.2(f) 第 14 条(2)(f)	The specific source of the data should be provided unless it is not possible to do so – see further guidance at paragraph 60. If the specific source is not named then information provided should include: the nature of the sources (i.e. publicly/ privately held sources) and the types of organisation/ industry/ sector. データの情報源を明示することが不可能でない限り、そうするべきである - 詳細は 60 項の指針を参照。情報源を明記しない場合には、情報に次の内容を含めるべきである。情報源の性質（すなわち、公的／私的に保有されている情報源）及び組織／業界／産業部門のタイプ。
The existence of automated decision-making including profiling and, if applicable, meaningful information about the	Article 13.2(f) 第 13 条(2)(f)	Article 14.2(g) 第 14 条(2)(g)	See WP29 Guidelines on automated individual decisionmaking and Profiling.[67] 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第 29 条作業部会ガイドラインを参照[67]。

[67] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251
2016/679 規則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, WP 251

logic used and the significance and envisaged consequences of such processing for the data subject プロファイリングを含む自動化された意思決定の存在、及び該当すれば、使われているロジック及びそのような取扱いのデータ主体にとっての重要性及び想定される結果に関する意味のある情報。			