仮日本語訳

Guidelines on Data Protection Officers (‘DPOs’)
データ保護オフィサー（DPO）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2016年12月13日に採択後、修正のうえ2017年4月5日に採択されたGuidelines on Data Protection Officers (‘DPOs’) の英語版の一部を個人情報保護委員会が翻訳したものである。本書面は参考のための仮日本語訳であって、その利用について当委員会は責任を負わないものとし、正確な内容については原文を参照されたい。

Table of Content

目次

1. Introduction

1. 序

The General Data Protection Regulation ('GDPR'),[1] due to come into effect on 25 May 2018, provides a modernised, accountability-based compliance framework for data protection in Europe. Data Protection Officers ('DPO's) will be at the heart of this new legal framework for many organisations, facilitating compliance with the provisions of the GDPR.

一般データ保護規則（GDPR）[1]は、2018 年 5 月 25 日に施行され、欧州のデータ保護のため、現代化したアカウンタビリティに基づく法令遵守の枠組みを与える。データ保護オフィサー（DPO）は多くの組織にとって、この新たな法的枠組みの核心であり、GDPR の規定の遵守を促進する。

Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO.[2] This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

GDPR のもとでは、一定の管理者と処理者が DPO を選任する義務を負う[2]。これはあらゆる公的な機関及び団体（どのようなデータを取扱うかは関係ない）、並びに、他の機関が――中心的業務として――体系的かつ大規模に個人を監視する又は特別な種類の個人データを大規模に取扱う時に当てはまる。

Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016). The GDPR is relevant for the EEA and will apply after its incorporation into the EEA Agreement.

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 95/46/EC の廃止に関する 2016 年 4 月 27 日の欧州議会及び理事会規則（EU）2016/679（一般データ保護規則）（OJ L119, 4.5.2016）。GDPR は EEA に関連するものであり、EEA 協定書に組み込まれた後、適用される。

[2] The appointment of a DPO is also mandatory for competent authorities under Article 32 of 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 (OJ L 119, 4.5.2016, p. 89 – 131), and national implementing legislation. While these guidelines focus on DPOs under the GDPR, the guidance is also relevant regarding DPOs under Directive 2016/680, with respect to their similar provisions.

DPO の選任は、犯罪の防止、捜査若しくは訴追又は刑事罰の執行を目的とする所轄当局による個人データの取扱いに係る自然人の保護及びかかるデータの自由な移動並びに理事会枠組決定 2008/977/JHA の廃止に関する 2016 年 4 月 27 日の欧州議会及び理事会指令（EU）2016/680 の第 32 条（OJ L 119, 4.5.2016, p.89-131）、並びに国内施行法に基づき、所轄当局にとっても義務である。本ガイドラインは GDPR に基づく DPO に焦点を当てるが、指針は指令 2016/680 に基づく DPO についても、同様の条項に関して関連性を有する。

GDPR が DPO の選任を特に要求しない時でも、組織はしばしば、自主的に DPO を選任するのが有益であると思うこともあろう。第 29 条データ保護作業部会（WP29）は、そうした自主的な取り組みを奨励する。

The concept of DPO is not new. Although Directive 95/46/EC[3] did not require any organisation to appoint a DPO, the practice of appointing a DPO has nevertheless developed in several Member States over the years.
DPO の概念は目新しいものではない。指令 95/46/EC[3] はいかなる組織にも DPO 選任を義務づけなかったが、DPO を選任する実務はそれでもなお、一部の加盟国で長年かけて培われてきた。

Before the adoption of the GDPR, the WP29 argued that the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses.[4] In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organization).
GDPR 採択に先立ち、WP29 は、DPO がアカウンタビリティの礎であり、DPO の選任が法令遵守を促進し、ひいては企業にとって競争上の優位になりうると主張した[4]。アカウンタビリティツール（データ保護影響評価の促進及び監査の実行又は促進など）の実施を通じた法令遵守促進のほか、DPO は関連利害関係者（例えば、監督当局、データ主体及び組織内の事業部門）の仲介者の役割も果たす。

DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a responsibility of the controller or the processor.
DPO は、GDPR 遵守違反があった場合、自ら責任を負うわけではない。規定に則した取扱いが実施されるように確実を期し、証明できるように義務づけられるのは管理者又は処理者であることを GDPR は明確にしている（第 24 条(1)）。データ保護遵守は管理者又は処理

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会指令 95/46/EC（OJ L 281, 23.11.1995, p.31）。

[4] See http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf 参照。

者の責任である。

The controller or the processor also has a crucial role in enabling the effective performance of the DPO's tasks. Appointing a DPO is a first step but DPOs must also be given sufficient autonomy and resources to carry out their tasks effectively.
管理者又は処理者は、DPO の任務の効果的遂行を可能にする点でも、重要な役割を担っている。DPO の選任は最初の一歩だが、DPO には任務を効果的に遂行するために、十分な自律性とリソースをも付与されなければならない。

The GDPR recognises the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks. The aim of these guidelines is to clarify the relevant provisions in the GDPR in order to help controllers and processors to comply with the law, but also to assist DPOs in their role. The guidelines also provide best practice recommendations, building on the experience gained in some EU Member States. The WP29 will monitor the implementation of these guidelines and may complement them with further details as appropriate.
GDPR は、DPO を新たなデータガバナンス体制のカギとなる担い手として認識しており、選任の条件、地位及び任務を示している。ガイドラインのねらいは、管理者や処理者の法令遵守を手助けし、DPO が役割を果たす支援をするため、GDPR の該当規定を明確にすることにある。ガイドラインはまた、一部の EU 加盟国で得られた経験を土台に、勧告されるベストプラクティスを提供する。WP29 はガイドラインの実施を監視し、さらに詳細を提供して適宜補完することもありうる。

2. Designation of a DPO
2. DPO の選任

2.1. Mandatory designation
2.1. 義務的選任

Article 37(1) of the GDPR requires the designation of a DPO in three specific cases:[5]
GDPR の第 37 条(1)は、三つの具体的なケースにおいて DPO の選任を義務づけている[5]。

a) where the processing is carried out by a public authority or body;[6]
a) 取扱いが公的機関又は団体によって行われる場合[6]
b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
b) 管理者又は処理者の中心的業務が、データ主体の大規模な定期的かつ体系的な監視を要する取扱作業である場合
c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data[7] or[8] personal data relating to criminal convictions and offences.[9]
c) 管理者又は処理者の中心的業務が、特別な種類のデータ[7]又は[8]有罪判決及び犯罪に関連する個人データの大規模な取扱いである場合[9]

In the following subsections, the WP29 provides guidance with regard to the criteria and terminology used in Article 37(1).
以下のサブセクションで、WP29 は第 37 条(1)で用いられる基準と用語に関する指針を示す。

[5] Note that under Article 37(4), Union or Member State law may require the designation of DPOs in other situations as well.
第 37 条(4)に基づき、欧州連合又は加盟国の法が、他の状況でも DPO の選任を義務づけることができる点に留意されたい。
[6] Except for courts acting in their judicial capacity. See Article 32 of Directive (EU) 2016/680.
司法的権限に基づき業務を行う裁判所を除く。EU 指令 2016/680 第 32 条参照。
[7] Pursuant to Article 9 these include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
第 9 条により、人種若しくは民族的素性、政治的思想、宗教的若しくは哲学的信条又は労働組合員資格を示す個人データ、及び、遺伝データ、自然人を一意に識別することを目的とした生体データ、健康に関するデータ又は自然人の性生活若しくは性的指向に関するデータの取扱いが含まれる。
[8] Article 37(1)(c) uses the word '*and*'. See Section 2.1.5 below for explanation on the use of '*or*' instead of '*and*.'
第 37 条(1)(c)は「及び（and）」の語を用いている。「及び」ではなく「又は（or）」を用いることについての説明は、下記セクション 2.1.5 を参照。
[9] Article 10.
第 10 条。

Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly.[10] This analysis is part of the documentation under the accountability principle. It may be required by the supervisory authority and should be updated when necessary, for example if the controllers or the processors undertake new activities or provide new services that might fall within the cases listed in Article 37(1).
DPO 選任を義務づけられていないことが明白でない限り、WP29 は、管理者と処理者に対して、関連要素が適切に考慮されたことを証明できるようにするため、DPO の選任の要否を決めるべく行われた内部分析を文書化することを勧告する[10]。この分析はアカウンタビリティの原則における文書化の一部である。それは監督機関から要求されうるし、例えば、管理者又は処理者が第 37 条(1)に掲示されている事例に該当する可能性のある新規の活動を行う場合又は新規のサービスを提供する場合には、必要に応じて、最新のものとしなければならない。

When an organisation designates a DPO on a voluntary basis, the requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been mandatory.
組織が自主的に DPO を選任する場合には、選任が義務的である場合と同様に、第 37 条から第 39 条に基づく要件が、その者の選任、地位及び任務に適用される。

Nothing prevents an organisation, which is not legally required to designate a DPO and does not wish to designate a DPO on a voluntary basis to nevertheless employ staff or outside consultants with tasks relating to the protection of personal data.
In this case it is important to ensure that there is no confusion regarding their title, status, position and tasks. Therefore, it should be made clear, in any communications within the company, as well as with data protection authorities, data subjects, and the public at large, that the title of this individual or consultant is not a 'data protection officer (DPO).[11]
法的に DPO の選任義務を負わず、自主的な DPO の選任を望まない組織が、それでもなお個人データ保護に関連する任務を行う職員や外部のコンサルタントを採用することを妨げ

[10] See Article 24(1).
第 24 条(1)を参照。
[11] This is also relevant for chief privacy officers ('CPO's) or other privacy professionals already in place today in some companies, who may not always meet the GDPR criteria, for instance, in terms of available resources or guarantees for independence, and therefore, cannot be considered and referred to as DPOs.
これは、一部の企業で既に配置されているチーフプライバシーオフィサー（CPO）や他のプライバシー専門家にも関連する。これらの者は、例えば利用可能なリソースや独立性の保証の点で、GDPR の基準を満たさない可能性があり、DPO と見なしたり、呼んだりすることができない。

るものではない。この場合、肩書き、職階、地位及び任務に混乱が生じないように確実を期すことが重要である。それゆえ、社内のほか、データ保護当局、データ主体及び一般市民に対する伝達でも、当該人物又はコンサルタントの肩書きが「データ保護オフィサー（DPO）」でないことを明確にするべきである[11]。

The DPO, whether mandatory or voluntary, is designated for all the processing operations carried out by the controller or the processor.
DPO は、義務的であれ、自主的であれ、管理者又は処理者が行う全ての取扱作業について選任される。

2.1.1 'PUBLIC AUTHORITY OR BODY'
2.1.1 「公的機関又は団体」

The GDPR does not define what constitutes a '*public authority or body*'. The WP29 considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.[12] In such cases, the designation of a DPO is mandatory.
GDPR は、何が「公的機関又は団体」を構成するかを定義していない。WP29 は、かかる概念が国内法で決められるべきであると考える。したがって、公的な機関及び又は団体は、国、地域、地方の機関を含むが、準拠する国内法に基づき、公法によって統轄される一定範囲の他の団体も含むのが通例である[12]。このような場合、DPO の選任は義務づけられる。

A public task may be carried out, and public authority may be exercised[13] not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.
公的任務の遂行や公的権限の行使は、公的機関又は団体だけでなく、公法又は私法によって統轄される他の自然人又は法人（例えば、各加盟国の国内規制に応じて、公共交通サービス、

[12] See, e.g. the definition of '*public sector body*' and '*body governed by public law*' in Article 2(1) and (2) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public-sector information (OJ L 345, 31.12.2003, p. 90).
例えば、公的機関の情報の再利用に関する 2003 年 11 月 17 日の欧州議会及び理事会指令 2003/98/EC の第 2 条(1)及び(2)における「公共団体」及び「公法により統轄される団体」の定義を参照（OJ L 345, 31.12.2003, p.90）。
[13] Article 6(1)(e).
第 6 条(1)(e)。

水道及びエネルギー供給、道路インフラ、公共放送、公営住宅並びに規制職種の職能団体といったセクターで）も行いうる[13]。

In these cases, data subjects may be in a very similar situation to when their data are processed by a public authority or body. In particular, data can be processed for similar purposes and individuals often have similarly little or no choice over whether and how their data will be processed and may thus require the additional protection that the designation of a DPO can bring.
この場合、データ主体は、自身のデータが公的機関又は団体に取扱われるのと非常に近い状態に置かれるかもしれない。特に、データが似た目的で取扱われる可能性があり、個々人が同様に、データが取扱われるか否かやどのように取扱われるかについて選択権をほとんど又はまったく得られないことが多く、DPO 選任がもたらしうる追加的保護が必要になるだろう。

Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that private organisations carrying out public tasks or exercising public authority designate a DPO. Such a DPO's activity covers all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).
このような場合にはたとえ義務がなくとも、WP29 は、望ましい慣行として、公的任務を遂行する又は公的権限を行使する民間組織が、DPO を選任することを勧告する。かかる DPO の活動は、公的任務の実行や公務執行に無関係なもの（例えば従業員データベースの管理）も含め、実行されるすべての取扱作業を対象とする。

2.1.2 'CORE ACTIVITIES'
2.1.2 「中心的業務」

Article 37(1)(b) and (c) of the GDPR refers to the '*core activities of the controller or processor*'. Recital 97 specifies that the core activities of a controller relate to '*primary activities and do not relate to the processing of personal data as ancillary activities*'. 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals.
GDPR 第 37 条(1)(b)及び(c)は、「管理者又は処理者の中心的業務」に言及している。前文第 97 項は、管理者の中心的業務が「主たる業務に関連し、副次的業務としての個人データの取扱いに関連しない」と明記する。「中心的業務」は、管理者又は処理者の目標達成に必要な重要作業と考えることができる。

However, 'core activities' should not be interpreted as excluding activities where the processing of

data forms an inextricable part of the controller's or processor's activity. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs.
ただし、「中心的業務」は、データ取扱いが管理者又は処理者の業務の切り離せない部分を形成している業務を除外すると解すべきでない。例えば、病院の中心的業務は医療の提供である。しかし、病院が患者の健康記録などの健康データを取扱わずに、安全かつ効果的に医療を提供するのは不可能であろう。それゆえ、このようなデータの取扱いは病院の中心的業務の一つと見なすべきで、病院は DPO を選任しなければならない。

As another example, a private security company carries out the surveillance of a number of private shopping centres and public spaces. Surveillance is the core activity of the company, which in turn is inextricably linked to the processing of personal data. Therefore, this company must also designate a DPO.
別の例として、ある民間警備会社が多くの民間ショッピングセンターや公共の場の監視を行っている。監視はこの会社の中心的業務であり、個人データの取扱いと不可分に結びついている。それゆえ、この会社も DPO を選任しなければならない。

On the other hand, all organisations carry out certain activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.
一方、あらゆる組織が、従業員の給与支払いや標準的な IT サポート業務などの一定の業務を行っている。これらは、組織の中心的業務又は主たる事業にとって、必要なサポート機能の例である。これらの業務は必要又は不可欠のものであっても、一般的には、中心的業務ではなく、副次的機能と見なされる。

2.1.3 'LARGE SCALE'
2.1.3 「大規模」

Article 37(1)(b) and (c) requires that the processing of personal data be carried out on a large scale in order for the designation of a DPO to be triggered. The GDPR does not define what constitutes large-scale processing, though recital 91 provides some guidance.[14]

[14] According to the recital, '*large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are*

第 37 条(1)(b)及び(c)は、DPO の選任が義務付けられるには、個人データの取扱いが大規模に行われる必要があるとしている。GDPR は何が大規模取扱いを構成するかを定義していないが、前文第 91 項はいくつかの指針を与えている [14]。

Indeed, it is not possible to give a precise number either with regard to the amount of data processed or the number of individuals concerned, which would be applicable in all situations. This does not exclude the possibility, however, that over time, a standard practice may develop, for identifying in more specific and/or quantitative terms what constitutes '*large scale*' in respect of certain types of common processing activities. The WP29 also plans to contribute to this development, by way of sharing and publicising examples of the relevant thresholds for the designation of a DPO.
実際のところ、取扱われるデータ量や関係する個人の数に関して、あらゆる状況に適用できる正確な数字を出すことは不可能である。しかし、これは、時間の経過に伴い、一定種類の共通した取扱業務に関して、より具体的及び／又は定量的観点から何が「大規模」を構成するのかの特定に資する一定の慣習が発展していく可能性を否定するものではない。WP29 も DPO 選任に関連する基準の例を共有・公開することで、そうした発展に寄与する方針である。

In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
いずれにせよ WP29 は、大規模に取扱われているかどうかを判断する際、特に下記の要素を考慮するよう勧告する。

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- 関係するデータ主体の数――具体的な数字又は関連する人口の割合

likely to result in a high risk' would be included, in particular. On the other hand, the recital specifically provides that '*the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer*'. It is important to consider that while the recital provides examples at the extremes of the scale (processing by an individual physician versus processing of data of a whole country or across Europe); there is a large grey zone in between these extremes. In addition, it should be borne in mind that this recital refers to data protection impact assessments. This implies that some elements might be specific to that context and do not necessarily apply to the designation of DPOs in the exact same way.
前文によると、「*地域、国内又は国際レベルで相当な量の個人データを取扱われることを目指し、多数のデータ主体に影響する可能性があり、高リスクにつながる可能性が高い大規模な取扱作業*」が、特に含まれる。一方、前文は「*取扱いが、個々の医師、他の医療専門職又は弁護士による患者や依頼人の個人データに関係する場合、個人データの取扱いが大規模と見なすべきではない*」と明確に定めている。前文は尺度の両極端で例を挙げているが（個々の医師による取扱いと、一国全体又は欧州全体のデータの取扱いの対比）、両極端の間に大きなグレーゾーンがあると考えることが重要である。さらに、この前文がデータ保護影響評価に触れている点に留意すべきである。これは、一部の要素がその文脈特有のものかもしれず、まったく同じように DPO の選任に適用されるとは限らないことを暗示する。

- The volume of data and/or the range of different data items being processed
- 取扱われるデータの量及び／又は異なるデータ項目の範囲
- The duration, or permanence, of the data processing activity
- データ取扱業務の期間又は永続性
- The geographical extent of the processing activity
- 取扱業務の地理的範囲

Examples of large-scale processing include:
大規模な取扱いの例は次のとおり

- processing of patient data in the regular course of business by a hospital
- 病院の通常業務内の患者データの取扱い
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- 市の公共交通機関を利用する個人の移動データの取扱い（例：乗車カードによる追跡）
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
- 専門的な処理者が統計目的のため行う国際的なファーストフードチェーンにおける顧客のリアルタイムな地理位置情報の取扱い
- processing of customer data in the regular course of business by an insurance company or a bank
- 保険会社又は銀行の通常業務内の顧客データの取扱い
- processing of personal data for behavioural advertising by a search engine
- 検索エンジンによる行動ターゲティング広告のための個人データの取扱い
- processing of data (content, traffic, location) by telephone or internet service providers
- 電話又はインターネットのサービス事業者によるデータ（コンテンツ、通信量、位置）の取扱い

Examples that do not constitute large-scale processing include:
大規模な取扱いを構成しない例は次のとおり。

- processing of patient data by an individual physician
- 個々の医師による患者データの取扱い
- processing of personal data relating to criminal convictions and offences by an individual lawyer

- 個々の弁護士による有罪判決及び犯罪に関連した個人データの取扱い

2.1.4 'REGULAR AND SYSTEMATIC MONITORING'
2.1.4 「定期的かつ体系的な監視」

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but the concept of 'monitoring of the behaviour of data subjects' is mentioned in recital 24[15] and clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising.
データ主体の定期的かつ体系的な監視の概念はGDPRで定義されていないが、「データ主体の行動の監視」の概念は前文第24項[15]で言及されており、行動ターゲティング広告の目的を含め、インターネット上のあらゆる形の追跡及びプロファイリングは明確に含まれる。

However, the notion of monitoring is not restricted to the online environment and online tracking should only be considered as one example of monitoring the behaviour of data subjects.[16]
ただし、監視の概念はオンライン環境に限定されず、オンライン追跡はデータ主体の行動監視の一例にすぎないと見なすべきである[16]。

WP29 interprets 'regular' as meaning one or more of the following:
WP29は「定期的（regular）」について、次の一つ以上の意味を有すると解釈する。

- Ongoing or occurring at particular intervals for a particular period
- 現在継続している又は一定期間内において一定の間隔で発生する
- Recurring or repeated at fixed times
- 決まった時期に繰り返し発生又は繰り返される
- Constantly or periodically taking place
- 常時又は周期的（periodically）に発生する

[15] *'In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'.*
「取扱い業務がデータ主体の行動を監視するためのものと見なせるかどうかを判定するには、特にその者に関する決定を下すため又はその者の個人的な選好、行動及び態度を分析若しくは予測する目的で、自然人のプロファイリングの要素を持つ個人データ取扱技術が後に使用される可能性を含め、自然人がインターネット上で追跡されているかどうかを確認するべきである。」

[16] Note that Recital 24 focuses on the extra-territorial application of the GDPR. In addition, there is also a difference between the wording '*monitoring their behaviour'* (Article 3(2)(b)) and *'regular and systematic monitoring of data subjects'* (Article 37(1)(b)) which could therefore be seen as constituting a different notion.
前文第24項がGDPRの域外適用に焦点を当てていることに留意すべきである。加えて、「行動を監視する（第3条(2)(b)）」と、「データ主体の定期的かつ体系的な監視（第37条(1)(b)」の表現の違いもあるが、これらはその相違のため異なる概念を構成すると解しえる。

WP29 interprets ‘systematic’as meaning one or more of the following:
WP29は「体系的（systematic）」について、下記の一つ以上の意味を有すると解釈する。

- Occurring according to a system
- システムに従って発生する
- Pre-arranged, organised or methodical
- 予め決められている、組織立っている又は方法論に従っている
- Taking place as part of a general plan for data collection
- データ収集の全体計画の一環として行われる
- Carried out as part of a strategy
- 戦略の一環として行われる

Examples of activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.
データ主体の定期的かつ体系的な監視を構成しうる活動事例：電気通信ネットワークの運営；電気通信サービスの提供；リターゲティングメール；データドリブンマーケティング活動；リスク評価目的のプロファイリングとスコアリング（例えば、クレジットスコアリング、保険料の確定、不正防止、マネーロンダリングの検知のため）；位置追跡（例えばモバイルアプリによる）；ロイヤルティプログラム；行動ターゲティング広告；ウェアラブルデバイスを通じた健康データの監視；閉回路テレビ（CCTV）；例えばスマートメーター、スマートカー、ホームオートメーションなどの接続機器。

2.1.5 SPECIAL CATEGORIES OF DATA AND DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES
2.1.5 特別な種類のデータ並びに有罪判決及び犯罪に関連するデータ

Article 37(1)(c) addresses the processing of special categories of data pursuant to Article 9, and personal data relating to criminal convictions and offences set out in in Article 10. Although the provision uses the word ‘and’, there is no policy reason for the two criteria having to be applied simultaneously. The text should therefore be read to say ‘or’.

第 37 条(1)(c)は、第 9 条に基づく特別な種類のデータと第 10 条に定める有罪判決及び犯罪に関連する個人データの取扱いに触れている。この規定は「及び・並びに（and)」の語を用いているが、二つの基準を同時に適用しなければならない政策的理由はない。それゆえ、文言は「又は（or)」と読むべきである。

2.2. DPO of the processor
2.2. 処理者の DPO

Article 37 applies to both controllers[17] and processors[18] with respect to the designation of a DPO. Depending on who fulfils the criteria on mandatory designation, in some cases only the controller or only the processor, in other cases both the controller and its processor are required to appoint a DPO (who should then cooperate with each other).
第 37 条は DPO 選任に関して、管理者 [17] と処理者 [18] の両方に適用される。義務的選任の基準を誰が満たすかによって、場合によっては管理者のみ又は処理者のみ、場合によっては管理者と処理者両方が、DPO を選任しなければならない（DPO は互いに協力すべきである)。

It is important to highlight that even if the controller fulfils the criteria for mandatory designation its processor is not necessarily required to appoint a DPO. This may, however, be a good practice.
管理者が義務的選任の基準を満たす場合でも、その処理者が必ずしも DPO を選任する必要はないことを強調するのが重要である。ただし、そうするのは望ましい慣行ではあろう。

Examples:
例は次のとおり。

- A small family business active in the distribution of household appliances in a single town uses the services of a processor whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large-scale', considering the small number of customers and the relatively limited activities. However, the activities of the processor, having many customers like this small enterprise, taken together, are carrying out large-scale processing. The processor must therefore designate a DPO under Article 37(1)(b). At the same time, the family business itself is not under an obligation to designate a DPO.

[17] The controller is defined by Article 4(7) as the person or body, which determines the purposes and means of the processing.
管理者は、第 4 条(7)で、取扱いの目的と手段を決定する人又は団体と定義されている。
[18] The processor is defined by Article 4(8) as the person or body, which processes data on behalf of the controller.
処理者は、第 4 条(8)で、管理者を代理してデータを取扱う人又は団体と定義されている。

- ある町で家電製品の流通に参入している家族経営の零細企業が、処理者のサービスを用いる。処理者の中心的業務は、ウェブサイト分析サービスと、ターゲティング広告やマーケティングの支援の提供である。この家族経営の会社の業務とその顧客は、顧客数が少ないことと比較的業務が限定的であることを考えると、「大規模」なデータの取扱いを生じない。しかし処理者はこの小規模事業者のような顧客を多数抱えており、合算すると、処理者の業務は、大規模な取扱いを実行している。したがって処理者は第 37 条(1)(b)に基づき、DPO を選任しなければならない。半面、この家族経営の会社自体は DPO を選任する義務を負わない。
- A medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO under Article 37(1)(c) provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.
- 中規模のタイル製造企業が、職場の保険サービスを外部の処理者に外注している。処理者は同様の顧客を多数抱えている。処理者は、取扱いが大規模であれば、第 37 条(1)(c)に基づき DPO を選任しなければならない。しかし製造会社は必ずしも DPO を選任する義務を負うわけではない。

DPO designated by a processor also oversees activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).
処理者から選任された DPO は、処理者の組織が自らデータ管理者として行動する時、当該組織が行う業務も監督する（例えば、人事、IT、ロジスティクス）。

2.3. Designation of a single DPO for several organisations
2.3. 「複数の組織を担当する一人の DPO の選任」

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects[19], the supervisory authority[20] but also internally within the organisation, considering that one of the tasks of the DPO is *'to inform and advise the controller and the processor and the employees who carry out processing of their obligations pursuant to this*

[19] Article 38(4): '*data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this regulation*'.
第 38 条(4)：「*データ主体は、自分の個人データの取扱い及び本規則に基づく権利行使に関するあらゆる問題について、データ保護オフィサーに連絡を取ることができる。*」
[20] Article 39(1)(e): '*act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 and to consult, where appropriate, with regard to any other matter*'.
第 39 条(1)(e)：「*監督機関にとって、第36 条で述べた事前協議を含め、取扱いに関する問題での、及び他の何らかの問題で適宜協議するための、連絡先の役割を果たす。*」

Regulation'.[21]
第 37 条(2)は、「*各拠点から容易にアクセスできる*」ことを条件に、企業グループが単一の DPO を選任することを認めている。このアクセス可能性の概念は、DPO がデータ主体[19]や監督機関[20]に関してのみならず、組織内部においても、連絡先の任務を担うことを示している。これは、DPO の任務の一つが、「*管理者及び処理者並びに取扱いを実行する従業員に、本規則に則した義務を通知し、助言する*」[21]ことを踏まえている。

In order to ensure that the DPO, whether internal or external, is accessible it is important to make sure that their contact details are available in accordance with the requirements of the GDPR.[22]
内部か外部かを問わず、DPO に確実にアクセスできる状況を確保するため、連絡先の詳細が GDPR の要件に則して確実に入手できるようにすることが重要である[22]。

He or she, with the help of a team if necessary, must be in a position to efficiently communicate with data subjects[23] and cooperate[24] with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.
DPO は、必要に応じチームの支援を得て、データ主体と円滑に連絡し[23]、関係する監督機関に協力する[24]立場でなければならない。これは、関係する監督機関及びデータ主体が用いる言語又は複数言語で連絡を行わなければならないことも意味する。DPO の可用性は、（物理的に職員と同じ場所であれ、ホットライン又は他の確実な連絡手段によってであれ）データ主体が DPO と連絡できることを確保するために不可欠である。

According to Article 37(3), a single DPO may be designated for several public authorities or bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the

[21] Article 39(1)(a).
第 39 条(1)(a)。
[22] See also Section 2.5 below.
下記セクション 2.5 参照。
[23] Article 12(1): *'The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.'*
第 12 条 1 項：「*管理者は、簡潔、明快、理解しやすく容易にアクセスできる形で、明確かつ平易な言葉を用い、特に子供向け情報はなおのこと、取扱いに関して第 13 条及び第 14 条で言及された情報並びに第 15 条から第 22 条及び第 34 条に基づく連絡をデータ主体に与えるように、適切な措置を講じなければならない。*」
[24] Article 39(1)(d) *: 'to cooperate with the supervisory authority'*
第 39 条(1)(d)：「*監督機関に協力する*」

controller or processor must ensure that a single DPO, with a help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.
第 37 条(3)により、複数の公的な機関又は団体は、その組織構造及び規模を考慮して、単一の DPO を選任することができる。リソース及び連絡に関して同様の考慮事項が適用される。DPO が幅広い任務を担っていることを踏まえ、管理者又は処理者は、単一の DPO が、必要に応じてチームの支援を得て、複数の公的な機関及び団体の担当として選任されていても効率よくその任務を遂行できるようにしなければならない。

2.4. Accessibility and localization of the DPO
2.4. DPO のアクセス可能性とローカライゼーション

According to Section 4 of the GDPR, the accessibility of the DPO should be effective.
GDPR のセクション 4 に従い、DPO のアクセス可能性は実効的でなければならない。

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union.
DPO へのアクセスを確保するため、管理者又は処理者が EU 内に設置されていると否とにかかわらず、DPO が EU 内に所在することを勧告する。

However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union[25], a DPO may be able to carry out his or her activities more effectively if located outside the EU.
しかしながら、管理者又は処理者が EU[25] 内に拠点を有していない場合には、時として、DPO が EU 外に所在していた方が、その活動をより効果的に行うことができる可能性を排除することはできない。

2.5. Expertise and skills of the DPO
2.5. DPO の専門知識と技能

Article 37(5) provides that the DPO '*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*'. Recital 97 provides that the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.

[25] See Article 3 of the GDPR on the territorial scope.
地理的範囲については、GDPR の第 3 条参照。

第 37 条(5)は、DPO が「*専門的資質並びに、特に、データ保護法及び実務の専門知識並びに第 39 条で言及された任務を遂行する能力に基づいて、選任されることとする*」と定めている。前文第 97 項は、専門知識の必要水準が、行われるデータ取扱作業と取扱われる個人データに必要な保護に即して決められるべきであるとしている。

- **Level of expertise**
- **専門知識の水準**

The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation.
専門知識の必要水準は、厳密に定義されてはいないが、組織が取扱うデータの機密性、複雑性及び量に見合わなければならない。例えば、データ取扱業務が特に複雑な場合、あるいは大量の機密データが含まれる場合、DPO にはより高い水準の専門知識とサポートが必要となろう。組織が EU 域外に組織的に個人データを移転するかどうか、そのような移転が散発的かどうかによる違いもある。したがって DPO は、組織内で生じるデータ保護問題をきちんと考慮した上で、慎重に選ばれるべきである。

- **Professional qualities**
- **専門的資質**

Although Article 37(5) does not specify the professional qualities that must be considered when designating the DPO, it is a relevant element that DPOs must have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs.
第 37 条(5)は DPO 選任時に考慮されなければならない専門的資質を明記していないが、DPO が自国及び欧州のデータ保護法及び実務の専門知識と、GDPR の深い理解を有さなければならないということが一つの考慮要素である。監督機関が DPO 向けの適切かつ定期的な研修を促進すれば、それも有益である。

Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have a good understanding of the processing operations carried out, as well as the information

systems, and data security and data protection needs of the controller.
管理者の事業分野や組織を知っていることも有益である。DPO はまた、行われる取扱作業のほか、管理者の情報システム、データセキュリティやデータ保護の必要性をよく理解しておくべきである。

In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.
公的機関又は団体の場合、DPO は組織の運営規則や手続の十分な知識も有するべきである。

- **Ability to fulfil its tasks**
- **任務遂行能力**

Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organization. Personal qualities should include for instance integrity and high professional ethics; the DPO's primary concern should be enabling compliance with the GDPR. The DPO plays a key role in fostering a data protection culture within the organization and helps to implement essential elements of the GDPR, such as the principles of data processing[26], data subjects' rights[27], data protection by design and by default[28], records of processing activities [29], security of processing [30], and notification and communication of data breaches.[31]
DPO が担う任務を遂行する能力は、個人的資質と知識を両方参照して理解するべきだが、組織内の地位も参照するべきである。個人的資質には、例えば誠実さや高い職業倫理観も含まれるべきである。DPO はもっぱら、GDPR を遵守できるようにすることに関心を寄せるべきである。DPO は、組織内のデータ保護の文化を育むのに重要な役割を果たし、データ取扱いの諸原則[26]、データ主体の権利[27]、データ保護バイ・デザイン及びバイ・デフォルト[28]、取扱業務の記録[29]、取扱いの安全性[30]、データ侵害の通知と連絡[31]など、GDPR の必須要素の実施を手助けする。

[26] Chapter II.
第 II 章。
[27] Chapter III.
第 III 章。
[28] Article 25.
第 25 条。
[29] Article 30.
第 30 条。
[30] Article 32.
第 32 条。
[31] Articles 33 and 34.
第 33 条及び第 34 条。

- **DPO on the basis of a service contract**
- **業務契約に基づく DPO**

The function of the DPO can also be exercised on the basis of a service contract concluded with an individual or an organization outside the controller's/processor's organization. In this latter case, it is essential that each member of the organization exercising the functions of a DPO fulfils all applicable requirements of Section 4 of the GDPR (e.g., it is essential that no one has a conflict of interests). It is equally important that each such member be protected by the provisions of the GDPR (e.g. no unfair termination of service contract for activities as DPO but also no unfair dismissal of any individual member of the organization carrying out the DPO tasks). At the same time, individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients.
DPO の職務は、管理者／処理者の組織外の個人又は組織と交わす業務契約に基づいて果たすこともできる。後者の場合、DPO の職責を果たす組織のメンバーそれぞれが、GDPR セクション 4 の適用要件をすべて満たすことが必須である（例えば、利益相反を抱えた者が一人もいないことは不可欠である）。各メンバーが GDPR の規定によって保護されることも、等しく重要である（例えば、DPO 業務に関する業務契約の不公正な打ち切りはなく、DPO 任務を遂行する組織の個々のメンバーが不当に解雇されることもない）。その一方、数人がチームを組み、より効率的に顧客に応対できるように、個人の技能や長所を結びつけることができる。

For the sake of legal clarity and good organization and to prevent conflicts of interests for the team members, it is recommended to have a clear allocation of tasks within the DPO team and to assign a single individual as a lead contact and person 'in charge' for each client. It would generally also be useful to specify these points in the service contract.
法的な明確性及び良好な組織運営のため並びにチームメンバー間の利益相反を防止するため、DPO チーム内で任務の割当てを明確に行い、各顧客について、特定の個人を主要窓口及び「担当者」として割り当てることが勧告される。一般的には、このような点を業務契約に明記することも有益である。

2.6. Publication and communication of the DPO's contact details
2.6. DPO の連絡先の詳細の公開と連絡

Article 37(7) of the GDPR requires the controller or the processor:
GDPR の第 37 条(7)は、管理者と処理者に、下記の項目を行うように義務づけている。

- to publish the contact details of the DPO and

- DPO の詳細な連絡先の公開
- to communicate the contact details of the DPO to the relevant supervisory authorities.
- 関連する監督機関への DPO の詳細な連絡先の連絡

The objective of these requirements is to ensure that data subjects (both inside and outside of the organization) and the supervisory authorities can easily and directly contact the DPO without having to contact another part of the organization. Confidentiality is equally important: for example, employees may be reluctant to complain to the DPO if the confidentiality of their communications is not guaranteed.
この義務の目的は、データ主体（組織の内部・外部ともに）と監督機関が組織の他部門を通すことなく、容易に、直接、DPO と接触できることを確保することにある。秘密保持義務は等しく重要である。例えば、従業員は DPO との連絡について秘密保持義務が保証されない場合には、DPO に対する苦情に消極的となるであろう。
The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)).
DPO は、連合又は加盟国法（第 38 条(5)）により、その任務の遂行に関し、守秘義務又は秘密保持義務を負っている。

The contact details of the DPO should include information allowing data subjects and the supervisory authorities to reach the DPO in an easy way (a postal address, a dedicated telephone number, and/or a dedicated e-mail address). When appropriate, for purposes of communications with the public, other means of communications could also be provided, for example, a dedicated hotline, or a dedicated contact form addressed to the DPO on the organization's website.
DPO の連絡先の詳細には、データ主体や監督機関が容易な方法で DPO と接点をもつことができる情報（郵便用住所、専用電話番号及び／又は専用電子メールアドレス）を含むべきである。一般市民とやり取りするため、他の連絡手段（例えば専用ホットラインや、組織のウェブサイトにおける DPO 宛ての専用フォーム）が適宜提供されることもありえる。

Article 37(7) does not require that the published contact details should include the name of the DPO. Whilst it may be a good practice to do so, it is for the controller or the processor and the DPO to decide whether this is necessary or helpful in the particular circumstances.[32]
第 37 条(7)は、公開された連絡先が DPO の氏名を含むように義務づけていない。そのよう

[32] It is notable that Article 33(3)(b), which describes information that must be provided to the supervisory authority and to the data subjects in case of a personal data breach, unlike Article 37(7), specifically also requires the name (and not only the contact details) of the DPO to be communicated.
個人データ侵害があった場合に監督機関及びデータ主体に提供しなければならない情報を述べた第 33 条(3)(b)が、第 37 条(7)と異なり、DPO の氏名（及び連絡先の詳細）の通知を明確に義務づけているのは、注目に値する。

にすることが望ましい慣行かもしれないが、特定の状況でそれが必要又は有益かどうかは管理者又は処理者と DPO が決めることとなる[32]。

However, communication of the name of the DPO to the supervisory authority is essential in order for the DPO to serve as contact point between the organisation and the supervisory authority (Article 39(1)(e).
しかしながら、DPO の氏名の監督機関への連絡は、DPO が当該組織と監督機関の間の連絡先となる上で不可欠である（第 39 条(1)(e)）。

As a matter of good practice, the WP29 also recommends that an organization informs its employees of the name and contact details of the DPO. For example, the name and contact details of the DPO could be published internally on organisation's intranet, internal telephone directory, and organisational charts.
WP29 は、望ましい慣行の一例として、組織がその従業員に、DPO の氏名と連絡先の詳細を伝えることについても勧告する。例えば、DPO の氏名と連絡先の詳細は、組織のイントラネット、内線簿や組織図によって、内部で公開することができよう。

3 Position of the DPO
3 DPO の立場

3.1. Involvement of the DPO in all issues relating to the protection of personal data
3.1. 個人データ保護に関するあらゆる問題に対する DPO の関与

Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO is *'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'*.
GDPR 第 38 条は、DPO が「*個人データ保護に関するあらゆる問題に、適切かつ適時に関与する*」ように、管理者及び処理者が確実を期さなければならないと定めている。

It is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.[33] Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, promote a privacy by design approach and should therefore be standard procedure within the organisation's governance. In addition, it is important that the DPO be seen as a discussion partner within the organisation and that he or she be part of the relevant working groups dealing with data processing activities within the organization.
DPO 又はそのチームがデータ保護関連のあらゆる問題で、可能な限り最も初期の段階から関与することが極めて重要である。データ保護影響評価に関しては、GDPR は DPO の初期の関与を明確に定めており、管理者はかかる影響評価を実行する際、DPO の助言を求めることとすると明記している[33]。最初の段階から DPO に確実に通知し、見解を仰ぐことは、GDPR 遵守を促進し、プライバシー・バイ・デザインのアプローチを促進することになり、それゆえ組織のガバナンス内で標準手順にするべきである。さらに、DPO が組織内で話し合う相手と受け止められ、組織内でデータ取扱業務を担当する関連作業グループの一員であることが重要である。

Consequently, the organisation should ensure, for example, that:
以上のことから、組織は、例えば下記の項目を確実に行うべきである。

- The DPO is invited to participate regularly in meetings of senior and middle management.
- DPO が幹部及び中間管理職の会議に定期的に参加するように招かれる。
- His or her presence is recommended where decisions with data protection implications are

[33] Article 35(2).
第 35 条 2 項。

taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.

- データ保護に影響する決定を下す際、DPO が列席することが勧告される。DPO が適切な助言を提供できるように、DPO にあらゆる関連情報を適時渡さなければならない。
- The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
- DPO の意見は常に、十分に考慮しなければならない。見解の相違がある場合、WP29 は望ましい慣行として、DPO の助言に従わない理由を文書化することを勧告する。
- The DPO must be promptly consulted once a data breach or another incident has occurred.
- データ侵害又は他の事案が発生した場合、DPO に速やかに諮問しなければならない。

Where appropriate, the controller or processor could develop data protection guidelines or programmes that set out when the DPO must be consulted.
管理者又は処理者は適宜、DPO に諮問しなければならない時期を示したデータ保護ガイドライン又はプログラムを作成することも考えられる。

3.2. Necessary resources
3.2. 必要なリソース

Article 38(2) of the GDPR requires the organisation to support its DPO by *'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'*. The following items, in particular, are to be considered:
GDPR 第 38 条(2)は、「*任務の遂行、個人データ及び取扱作業へのアクセス、並びに専門知識の維持に必要なリソースを提供すること*」により、組織が DPO を支援することを義務づけている。特に下記の項目を考慮するべきである。

- Active support of the DPO's function by senior management (such as at board level).
- 幹部（例えば取締役会レベル）による、DPO の職務への積極的なサポート
- Sufficient time for DPOs to fulfil their duties. This is particularly important where an internal DPO is appointed on a part-time basis or where the external DPO carries out data protection in addition to other duties. Otherwise, conflicting priorities could result in the DPO's duties being neglected. Having sufficient time to devote to DPO tasks is paramount. It is a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. It is also good practice to determine the time needed to carry

out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.

- DPOが任務を全うするための十分な時間。これは、内部DPOが非常勤として選任される場合や、外部DPOが他の職務に加えてデータ保護を行う場合に、特に重要である。もしこれが満たされない場合、優先課題が相反することで、DPOの職務がないがしろにされる事態につながる恐れがある。DPOの任務に専念する時間を十分確保することは、最も重要である。DPOの職務が常勤として行われない場合、その職務に向けた時間の割合を決めておくことが望ましい慣行である。また、職務遂行に必要な時間や、DPO職務の適切な優先順位を決めたり、DPO（又は組織）が作業計画を作成することも、望ましい慣行である。
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
- 資金、インフラ（敷地、施設、設備）及び人員（適宜）に関する適切な支援。
- Official communication of the designation of the DPO to all staff to ensure that their existence and function are known within the organisation.
- 選任されたDPOの存在と職務を組織内で確実に周知するために全職員に向けたDPOの選任についての正式な連絡。
- Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
- DPOが、組織内の他のサービス（人事、法務、ＩＴ、セキュリティー等）から不可欠なサポート、インプット又は情報を得るための当該サービスへの必要なアクセス。
- Continuous training. DPOs must be given the opportunity to stay up to date with regard to developments within the field of data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.
- 継続的な研修。DPOは、データ保護の分野における動向に関する最新事情を知る機会を与えられなければならない。DPOの専門知識の水準を絶えず引き上げることをねらいとするべきであり、DPOはデータ保護の研修コースや他の形の職能開発への参加、例えばプライバシーフォーラムやワークショップなどへの参加を奨励されるべきである。
- Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals

working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.

- 組織の規模と構造を考えた場合、DPO チーム（DPO とその部下）を設置する必要がある可能性がある。このような場合、チームの内部構成並びに各メンバーの任務及び責任は、明確に作成しておくべきである。同様に、外部のサービス事業者が DPO の役割を果たす場合、当該事業者の職員のチームが、顧客の主たる指定連絡先の責任のもと、DPO の任務をチームとして効果的に遂行できる可能性がある。

In general, the more complex and/or sensitive the processing operations, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out.
総じて、取扱作業が複雑及び／又はセンシティブになればなるほど、DPO に与えられる資源を増やさなければならない。データ保護の職務は、実行されているデータ取扱いに応じて、効果的かつ十分なリソースを得ていなければならない。

3.3. Instructions and 'performing their duties and tasks in an independent manner'
3.3. 指示及び「独立した態様でのその義務及び任務の遂行」

Article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers/processors are required to ensure that the DPO '*does not receive any instructions regarding the exercise of [his or her] tasks.*' Recital 97 adds that DPOs, '*whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner*'.
第 38 条(3)は、DPO が組織内で十分な自律性を持ち、任務を確実に遂行できるように支えるため、いくつかの基本的保障を定めている。特に、管理者／処理者は、DPO が「*(自らの)任務遂行に関して何ら指示を受けない*」ように確実を期すことが、義務づけられる。前文第 97 項は、DPO が「*管理者の従業員かどうかによらず、独立した態様で職責と任務を果たす立場にあるべき*」と付け加えた。

This means that, in fulfilling their tasks under Article 39, DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law.
これは第 39 条に基づく任務を遂行する際、DPO は、問題をどのように取扱うか、例えばどのような結果を達成するべきか、どのように苦情を調査するか、あるいは監督機関に相談するべきかをめぐって、指示を受けてはならないことを意味する。さらに、データ保護法に関

する問題で、一定の見解（例えば、特定の法解釈）を取るように指示されてはならない。

The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.
ただし、DPO の自律性は、第 39 条に基づく任務を越えて決定権を有するという意味ではない。

The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance.[34] If the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to the highest management level and to those making the decisions. In this respect, Article 38(3) provides that the DPO *'shall directly report to the highest management level of the controller or the processor'*. Such direct reporting ensures that senior management (e.g. board of directors) is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller or the processor. Another example of direct reporting is the drafting of an annual report of the DPO's activities provided to the highest management level.
管理者又は処理者はデータ保護法の遵守に責任を負い続け、遵守を証明できなければならない[34]。管理者又は処理者が、GDPR と DPO の助言が整合しないと判断する場合、DPO は最高経営者レベル及び判断を下す者に対し、反対意見を明確にする機会を与えられるべきである。この点に関し、第 38 条第 3 項は、DPO は、「直接、管理者又は処理者の最高経営者レベルに対し報告するものとする」と規定している。このような直接の報告によって、幹部（例、取締役会）が、DPO の助言及び勧告が管理者又は処理者に対する報告及び助言という DPO の使命の一部であることが確かに認識できるようになる。最高経営者レベル提供される DPO の年間活動報告の作成も直接の報告の別例である。

3.4. Dismissal or penalty for performing DPO tasks
3.4. DPO 任務の遂行を理由とした解雇又は処罰

Article 38(3) requires that DPOs should *'not be dismissed or penalised by the controller or the processor for performing [their] tasks'*.
第 38 条(3)は、DPO が「*自らの任務の遂行を理由に、管理者又は処理者から解雇又は処罰をされない*」ように義務づけている。

This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and

[34] Article 5(2).
第 5 条(2)。

enjoy sufficient protection in performing their data protection tasks.
この義務はDPOの自律性を強化し、DPOが独立して行動し、データ保護任務の遂行時に十分な保護を確かに受けられるようになることに役立つ。

Penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. For example, a DPO may consider that a particular processing is likely to result in a high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.
処罰がGDPRに基づいて禁止されるのは、DPOがDPOとしての職責を果たす結果課せられる場合のみである。例えば、DPOは、ある特定の取扱いが高いリスクをもたらす可能性が高いと考え、管理者又は処理者にデータ保護影響評価の実施を助言するかもしれない。しかし管理者又は処理者は、DPOの評価に同意しないとする。このような状況では、この助言の提供を理由にDPOを解雇することはできない。

Penalties may take a variety of forms and may be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to his/her DPO activities.
処罰はさまざまな形を取りうるし、直接的にも間接的にもなりうる。例えば、昇進の否定又は遅れ、キャリア開発の妨害、他の従業員が受ける福利厚生の拒否も処罰になりうる。処罰は、実際に課される必要はなく、DPOの任務に関連する理由でDPOを罰するために用いられる限り、単なる警告で十分である。

As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).
通常の管理規則及び他の従業員や委託業者にも適用される国内契約又は労働法若しくは刑法に基づき、DPOは、DPOとしての任務遂行以外の理由で（例えば、窃盗、身体的・精神的・セクシャルハラスメント、又は同様の重大な違反行為があった場合）、変わらず合法的に解雇されうる。

In this context it should be noted that the GDPR does not specify how and when a DPO can be dismissed or replaced by another person. However, the more stable a DPO's contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent

manner. Therefore, the WP29 would welcome efforts by organisations to this effect.
この文脈では、いつどのようにDPOを解雇できるか、又は他の者と交代できるかをGDPRが明記していないことに留意すべきである。ただし、DPOの契約が安定的であればあるほど、また不公正な解雇に対する保障が大きければ大きいほど、独立した態様で行動できる可能性が高くなる。それゆえWP29は、そのような趣旨の組織の取り組みを歓迎する。

3.5. Conflict of interests
3.5. 利益相反

Article 38(6) allows DPOs to '*fulfil other tasks and duties*'. It requires, however, that the organisation ensure that '*any such tasks and duties do not result in a conflict of interests*'.
第38条(6)は、DPOが「他の任務及び職務を果たす」ことを容認している。ただし「そのような任務及び職務が利益相反につながらない」ように、組織が確実を期す必要がある。

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.
利益相反がないことは、独立した態様で行動する義務と密接に結びついている。DPOは他の役割を担うことが認められているが、利益相反が生じないことを条件として、はじめて他の任務や職務を任せてもらうことができる。これは特に、DPOが組織内において個人データの取扱いの目的及び方法を決めることにつながる地位に就けないことを伴う。各組織に特有の組織構造があるため、この点は事例ごとに検討されなければならない。

As a rule of thumb, conflicting positions within the organisations may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organizational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.
大まかに言って、組織内における利益相反の立場には、幹部の地位（最高経営責任者、最高執行責任者、最高財務責任者、最高医務責任者、マーケティング部長、人事部長又はIT部長など）のほか、組織構造内でそれよりも低い地位も、その地位又は役職が個人データの取

扱いの目的及び方法の決定につながる場合には、含まれよう。また、利益相反は、例えば、データ保護が絡む事件の法廷において、外部の DPO が管理者又は処理者の代理を要請された場合にも生じうる。

Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:
組織の業務、規模及び構造に応じて、管理者又は処理者は下記の項目を行うことが望ましい慣行になりうる。

- to identify the positions which would be incompatible with the function of DPO
- DPO の役割と整合しない地位を特定する。
- to draw up internal rules to this effect in order to avoid conflicts of interests
- 利益相反を避けるため、その趣旨の内規を作成する。
- to include a more general explanation about conflicts of interests
- 利益相反に関するより一般的な説明を行う。
- to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
- この義務の認知度を高める一つの方策として、DPO の職務に関して、DPO に利益相反はないと宣言する。
- to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally.
- 組織の内規に保護措置を取り入れ、利益相反を避けるために DPO の地位の人材募集又は業務契約が十分厳密で、詳細なものであるように確実を期す。これに関連して、DPO を内部と外部のどちらで採用するかによって、利益相反がさまざまな形を取りうることにも留意すべきである。

4 Tasks of the DPO
4 DPO の任務

4.1. Monitoring compliance with the GDPR
4.1. GDPR 遵守の監視

Article 39(1)(b) entrusts DPOs, among other duties, with the duty to monitor compliance with the GDPR. Recital 97 further specifies that DPO '*should assist the controller or the processor to monitor internal compliance with this Regulation*'.
第 39 条(1)(b)は DPO に対し、とりわけ、GDPR の遵守を監視する職責を託している。前文第 97 項はさらに、DPO が「*本規則の内部遵守を監視するため、管理者又は処理者を支援すべき*」と明記している。

As part of these duties to monitor compliance, DPOs may, in particular:
遵守を監視する職責の一環として、DPO は特に下記の項目を行うことができる。

- collect information to identify processing activities
- 取扱業務を特定するため情報を収集する。
- analyse and check the compliance of processing activities
- 取扱業務の遵守を分析し、チェックする。
- inform, advise and issue recommendations to the controller or the processor
- 管理者又は処理者に通知し、助言し、勧告を行う。

Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to '*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*' (Article 24(1)). Data protection compliance is a corporate responsibility of the data controller, not of the DPO.
遵守の監視は、不遵守の事例があった時に、DPO が個人的に責任を負うという意味ではない。GDPR は、「取扱いが本規則に従って行われるように確実を期し、それを証明できるように、適切な技術的及び組織的措置を実施する」ことを義務づけられるのが、DPO ではなく管理者であることを明確にしている（第 24 条(1)）。データ保護遵守は、DPO ではなく、データ管理者の企業責任である。

4.2. Role of the DPO in a data protection impact assessment
4.2. データ保護影響評価における DPO の役割

According to Article 35(1), it is the task of the controller, not of the DPO, to carry out, when necessary, a data protection impact assessment ('DPIA'). However, the DPO can play a very important and useful role in assisting the controller. Following the principle of data protection by design, Article 35(2) specifically requires that the controller '*shall seek advice'* of the DPO when carrying out a DPIA. Article 39(1)(c), in turn, tasks the DPO with the duty to '*provide advice where requested as regards the [DPIA] and monitor its performance* pursuant to Article 35'.
第 35 条(1)によれば、必要に応じてデータ保護影響評価（DPIA）を行うのは、DPO ではなく管理者の責任である。しかし、DPO は管理者を支援する際に、非常に重要かつ有益な役割を果たすことができる。データ保護バイ・デザインの原則に従い、第 35 条(2)は、管理者が DPIA 実行時に DPO の「*助言を求めなければならない*」ことを特に求めている。第 39 条(1)(c)はさらに、DPO が、「*第 35 条に従い、(DPIA に）関して助言を求められた場合、助言を行い、実行状況を監視する*」義務を課している。

The WP29 recommends that the controller should seek the advice of the DPO, on the following issues, amongst others[35]:
WP29 は、管理者がとりわけ下記の問題に関して DPO に助言を求めるように勧告している[36]。

- whether or not to carry out a DPIA
- DPIA を行うかどうか
- what methodology to follow when carrying out a DPIA
- DPIA を行う際、どのような方法を採るか
- whether to carry out the DPIA in-house or whether to outsource it

[35] Article 39(1) mentions the tasks of the DPO and indicates that the DPO shall have '*at least*' the following tasks. Therefore, nothing prevents the controller from assigning the DPO other tasks than those explicitly mentioned in Article 39(1), or specifying those tasks in more detail.
第 39 条(1)は DPO の任務に言及し、DPO が「*少なくとも*」下記の任務を有することを示している。それゆえ、管理者が第 39 条(1)で明確に言及されたもの以外の任務を DPO に割り当てたり、そのような任務をより詳しく指定することを妨げるものではない。

[36] Article 24(1) provides that '*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure* ***and to be able to demonstrate*** *that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*'.
第 24 条 1 項は「*管理者は、取扱いの性質、範囲、状況及び目的、さらに自然人の権利と自由に対して確率と重大性が異なるリスク群を考慮し、取扱いが本規則に従って行われるように確実を期し、それを****証明できるようにするため****、適切な技術的及び組織的措置を実施するものとする。かかる措置は必要に応じて、見直し及び更新されることとする*」と定めている。

- DPIA を内部で実行するか、外注するか
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- データ主体の権利及び利益に対するリスクを緩和するため、どのような保護措置（技術的及び組織的措置を含む）を適用するか
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR
- DPIA が正しく行われたか、及び結論（取扱いを進めるかどうか及びどのような保護措置を適用するか）が GDPR に準拠しているか

If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account.
DPO からの助言に対し、管理者が異議を唱える場合、DPIA 文書は特に、助言が考慮されなかった理由を書面で説明するべきである。

The WP29 further recommends that the controller clearly outline, for example in the DPO's contract, but also in information provided to employees, management (and other stakeholders, where relevant), the precise tasks of the DPO and their scope, in particular with respect to carrying out the DPIA.
WP29 はまた、管理者が、例えば、DPO の連絡先や、職員、幹部（及び関連性がある場合は他の利害関係者）に提供される情報の中で、正確な DPO の任務と範囲（特に DPIA の実行に関して）を明確に概説するように勧告している。

4.3. Cooperating with the supervisory authority and acting as a contact point
4.3. 監督機関との協力及び連絡先としての活動

According to Article 39(1)(d) and (e), the DPO should '*cooperate with the supervisory authority*' and '*act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter*'.
第 39 条(1)(d)及び(e)により、DPO は、「*監督機関と協力*」及び「*第 36 条で言及する事前相談を含む取扱いに関する問題につき、監督機関のために連絡先として活動し、また、適切である場合には、それ以外のいかなる事項についても相談*」すべきである。

These tasks refer to the role of 'facilitator' of the DPO mentioned in the introduction to these Guidelines. The DPO acts as a contact point to facilitate access by the supervisory authority to the

documents and information for the performance of the tasks mentioned in Article 57, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers mentioned in Article 58. As already mentioned, the DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)). However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. Article 39(1)(e) provides that the DPO can consult the supervisory authority on any other matter, where appropriate.

これらの任務は、これらガイドラインの序文において言及されている DPO の「促進者」としての役割を指している。DPO は、第 57 条で言及されている任務の遂行に必要な書類及び情報への監督機関によるアクセスを促進させるため、第 58 条に言及されている当該監督機関の調査、是正、認証及び助言に関する権限の執行のための連絡先として活動する。既述したように、DPO は、その任務の遂行に関し、連合又は加盟国法（第 38 条(5)）に従い、守秘義務又は秘密保持義務を負っている。しかしながら、この守秘義務/秘密保持義務は、DPO が監督機関に接触し助言を求めることを禁止するものではない。第 39 条(1)(e)は、DPO は、適切な場合、他のいかなる事項についても監督機関に相談できると規定している。

4.4. Risk-based approach
4.4. リスクに応じたアプローチ

Article 39(2) requires that the DPO '*have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing*'.

第 39 条(2)は、DPO が「*取扱いの性質、範囲、文脈及び目的を踏まえ、取扱作業に付随するリスクをきちんと考慮する*」ように義務づけている。

This article recalls a general and common sense principle, which may be relevant for many aspects of a DPO's day-to-day work. In essence, it requires DPOs to prioritise their activities and focus their efforts on issues that present higher data protection risks. This does not mean that they should neglect monitoring compliance of data processing operations that have comparatively lower level of risks, but it does indicate that they should focus, primarily, on the higher-risk areas.

同条は、DPO の日常的な業務の多くの側面に関連するであろう一般的かつ常識的な原則に基づいている。本質的に、業務に優先順位を付け、より高いデータ保護リスクを生じさせる問題に注力するように、DPO に求めている。これは、リスク水準が比較的低いデータ取扱作業の法令遵守監視をおろそかにすべきという意味ではなく、よりリスクの高い領域にもっぱら焦点を当てるべきと示しているのである。

This selective and pragmatic approach should help DPOs advise the controller what methodology to use when carrying out a DPIA, which areas should be subject to an internal or external data protection audit, which internal training activities to provide to staff or management responsible for data processing activities, and which processing operations to devote more of his or her time and resources to.

この選択的かつ現実的アプローチは、DPO が管理者に対し、DPIA 実行時にどの方法を採るか、どの領域が内部又は外部のデータ保護監査を受けるべきか、データ取扱業務担当の職員や幹部にどの内部研修を受けてもらうか、どの取扱作業に自身の時間やリソースをより多く注ぐかについて、助言するのに役立つだろう。

4.5. Role of the DPO in record-keeping
4.5. 記録作成における DPO の役割

Under Article 30(1) and (2), it is the controller or the processor, not the DPO, who is required to '*maintain a record of processing operations under its responsibility*' or *'maintain a record of all categories of processing activities carried out on behalf of a controller'*.

第 30 条(1)及び(2)に基づき、「*自身の責任に基づく取扱作業の記録を保持する*」又は「*管理者を代理して行われるあらゆる種類の取扱業務の記録を保持する*」ことを義務づけられるのは、DPO ではなく、管理者又は処理者である。

In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.[37]

実務上は、DPO が個人データの取扱いを担当する組織内の各部門から提供された情報をもとに、目録を作成し、取扱作業記録簿を保管することが多い。この実務は、多くの現行国内法や EU 諸機関が準拠するデータ保護規則に基づき確立されてきている[37]。

Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller or the processor. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.

[37] Article 24(1)(d), Regulation (EC) 45/2001.
規則(EC)45/2001 第 24 条(1)(d)。

第 39 条 1 項は、DPO が最低限担当しなければならない任務リストを定めている。よって、管理者又は処理者がその責任の下で、取扱作業の記録保存の任務を DPO に割り当てることを妨げるものではない。かかる記録は、DPO がその任務である遵守監視、管理者又は処理者への通知及び助言といった任務を遂行できるようにするツールの一つと考えるべきである。

In any event, the record required to be kept under Article 30 should also be seen as a tool allowing the controller and the supervisory authority, upon request, to have an overview of all the personal data processing activities an organisation is carrying out. It is thus a prerequisite for compliance, and as such, an effective accountability measure.

いずれにせよ、第 30 条に基づき保存しなければならない記録は、管理者及び監督機関が、要求に基づき、組織が行うすべての個人データ取扱業務の概要を知るためのツールでもあると見なすべきである。よって、これは法令遵守の必要条件であり、それ自体が効果的なアカウンタビリティの手段でもある。

5 ANNEX - DPO GUIDELINES: WHAT YOU NEED TO KNOW

5 付録－DPO ガイドライン：知っておくべき事項

The objective of this annex is to answer, in a simplified and easy-to-read format, some of the key questions that organisations may have regarding the new requirements under the General Data Protection Regulation (GDPR) to appoint a DPO.

この付録の目的は、組織が DPO を任命するに当たり、一般データ保護規則（GDPR）上の新しい要件に関し抱くであろう主要な疑問につき、簡潔かつ理解し易い形で回答することである。

Designation of the DPO
DPO の選任

---

1 Which organisations must appoint a DPO?

1 いずれの組織が DPO を任命しなければならないか？

The designation of a DPO is an obligation:
DPO の選任は、以下の場合、義務である：

- if the processing is carried out by a public authority or body (irrespective of what data is being processed)
- 取扱いが公的機関又は団体によって行われる場合（取扱われたデータの種類を問わない）
- if the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale
- 管理者又は処理者の中心的業務が、データ主体の大規模な定期的かつ体系的な監視を必要とする取扱作業である場合
- if the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences
- 管理者又は処理者の中心的業務が、特別な種類のデータ又は有罪判決及び犯罪に関連する個人データの大規模な取扱いである場合

Note that Union or Member State law may require the designation of DPOs in other situations as well. Finally, even if the designation of a DPO is not mandatory, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts. When an organisation designates a DPO on a voluntary basis, the same requirements will apply to his or her designation, position and tasks as if the designation

had been mandatory.

欧州連合又は加盟国の法律が、他の状況においても同様に、DPO の選任を要求する場合があることに留意されたい。最後に、DPO の選任が強制でない場合においても、組織が自主的に DPO を選任することが有益である場合がある。第 29 条データ保護作業部会（WP29）は、このような自主的な努力を奨励する。組織が自主的に DPO を選任する場合には、その者の選任、地位及び任務に対し、選任が強制的であったとした場合と同様の要件が適用される。

Source: Article 37(1) of the GDPR
根拠規定：GDPR 第 37 条(1)

2 What does 'core activities' mean?
2 「中心的業務」とはどのような意味か？

'Core activities' can be considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms as inextricable part of the controller's or processor's activity. For example, processing health data, such as patient's health records, should be considered as one of any hospital's core activities and hospitals must therefore designate DPOs.

「中心的業務」とは、管理者又は処理者の目的を達成するための重要作業と考えることができる。これには、データ取扱いが管理者又は処理者の業務の切り離せない部分を形成する場合におけるすべての業務が含まれる。例えば、患者の健康記録等の健康データの取扱いは、いかなる病院においても中心的業務の一つと考えるべきであり、よって、病院は DPO を選任しなければならない。

On the other hand, all organisations carry out certain supporting activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.
一方、あらゆる組織が、従業員の給与支払いや標準的な IT サポート業務などの一定のサポート業務を行っている。これらは、組織の中心的業務又は主たる事業にとって、必要なサポート機能の例である。これらの業務は必要又は不可欠のものであっても、一般的には、中心的業務ではなく、副次的機能とみなされる。

Source: Article 37(1)(b) and (c) of the GDPR

根拠規定：GDPR 第 37 条(1)(b)及び(c)

3 What does 'large scale' mean?

3 「大規模」とはどのような意味か？

The GDPR does not define what constitutes large-scale processing. The WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

GDPR は、何が大規模取扱いを構成するかを定義していない。WP29 は、大規模に取扱われているかどうかを判断する際、特に、下記の要素を考慮するよう勧告する。

- the number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- 関係するデータ主体の数－具体的な数字又は関連する人口の割合
- the volume of data and/or the range of different data items being processed
- 取扱われるデータの量及び/又は異なるデータ項目の範囲
- the duration, or permanence, of the data processing activity
- データ取扱業務の期間又は永続性
- the geographical extent of the processing activity
- 取扱業務の地理的範囲

Examples of large scale processing include:

大規模な取扱いの例は、次のとおり

- processing of patient data in the regular course of business by a hospital
- 病院の通常業務内の患者データの取扱い
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- 市の公共交通機関を利用する個人の移動データの取扱い（例：乗車カードによる追跡）
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
- 専門的な処理者が統計目的のため行う国際的なファーストフードチェーンにおける顧客のリアルタイムな地理位置情報の取扱い
- processing of customer data in the regular course of business by an insurance company or a bank

- 保険会社又は銀行の通常業務内の顧客データの取扱い
- processing of personal data for behavioural advertising by a search engine
- 検索エンジンによる行動ターゲティング広告のための個人データの取扱い
- processing of data (content, traffic, location) by telephone or internet service providers
- 電話又はインターネットサービス事業者によるデータ（コンテンツ、通信量、位置）の取扱い

Examples that do not constitute large-scale processing include:
大規模な取扱いを構成しない例は次のとおり。

- processing of patient data by an individual physician
- 個々の医師による患者データの取扱い
- processing of personal data relating to criminal convictions and offences by an individual lawyer
- 個々の弁護士による有罪判決及び犯罪に関連した個人データの取扱い

Source: Article 37(1)(b) and (c) of the GDPR
法的根拠：GDPR 第 37 条(1)(b)及び(c)

4 What does 'regular and systematic monitoring' mean?
4 「定期的かつ体系的な監視」とはどのような意味か？

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. However, the notion of monitoring is not restricted to the online environment.
データ主体の定期的かつ体系的な監視の概念は GDPR で定義されていないが、行動ターゲティング広告の目的を含め、インターネット上のあらゆる形の追跡及びプロファイリングは明確に含まれる。ただし、監視の概念はオンライン環境に限定されない。

Examples of activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention,

detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.
データ主体の定期的、かつ、体系的監視を構成しうる業務の事例：電気通信ネットワークの運営；電気通信サービスの提供；電子メールのリターゲティング；データドリブンマーケティング業務；リスク評価目的のプロファイリングとスコアリング（例えば、クレジットスコアリング、保険料の確定、不正防止、マネーロンダリングの検知のため）；位置追跡（例えば、モバイルアプリによる）；ロイヤルティプログラム；行動ターゲティング広告；ウェアラブル機器を用いた健康データの監視；CCTV；例えば、スマートメーター、スマートカー、ホームオートメーションなどのコネクテッドデバイス。

WP29 interprets 'regular' as meaning one or more of the following:
WP29 は「定期的」について、次の一つ以上の意味を有すると解釈する。

- ongoing or occurring at particular intervals for a particular period
- 現在継続している又は一定期間において一定の間隔で発生する
- recurring or repeated at fixed times
- 決まった時期に繰り返し発生又は繰り返される
- constantly or periodically taking place
- 常時又は周期的に発生する

WP29 interprets 'systematic' as meaning one or more of the following:
WP29 は「体系的」について、次の一つ以上の意味を有すると解釈する。

- occurring according to a system
- システムに従って発生する
- pre-arranged, organised or methodical
- 予め決められている、組織立っている又は方法論に従っている
- taking place as part of a general plan for data collection
- データ収集の全体計画の一環として行われる
- carried out as part of a strategy
- 戦略の一環として行われる

Source: Article 37(1)(b) of the GDPR
根拠規定：GDPR 第 37 条(1)(b)

5 Can organisations appoint a DPO jointly? If so, under what conditions?

5 組織は DPO を共同で選任できるか？それはどのような条件の下か？

Yes. A group of undertakings may designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority and also internally within the organisation. In order to ensure that the DPO is accessible, whether internal or external, it is important to make sure that their contact details are available. The DPO, with the help of a team if necessary, must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.

選任できる。企業グループは、その DPO に「各拠点から容易にアクセスできる」ことを前提として、単一の DPO を選任することができる。アクセス可能性の概念は、データ主体、監督機関に関してのみならず、組織内における連絡先としての任務をも示している。内部か外部かを問わず、DPO にアクセスできる状況にあることを確保するため、DPO の連絡先の詳細を確実に入手できるようにすることは重要である。DPO は、必要に応じチームの支援を得て、データ主体と円滑に連絡し、かつ、関係する監督機関に協力する立場でなければならない。これは、関係する監督機関及びデータ主体が使用する特定の言語又は複数の言語で連絡を行われなければならないことを意味する。DPO の可用性は、（物理的に職員と同じ事務所であれ、ホットライン又は他の確実な連絡手段によってであれ）データ主体が DPO と連絡できることを確保するために不可欠である。

A single DPO may be designated for several public authorities or bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the controller or the processor must ensure that a single DPO, with the help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.

複数の公的な機関又は団体は、その組織構造及び規模を考慮して、単一の DPO を選任することができる。リソース及び連絡に関して同様の考慮事項が適用される。DPO が幅広い任務を担っていることを踏まえ、管理者又は処理者は、単一の DPO が、必要に応じてチームの支援を得て、複数の公的な機関及び団体の担当として選任されていても効率よくその任務を遂行できるようにしなければならない。

Source: Article 37(2) and (3) of the GDPR
根拠規定：GDPR 第 37 条(2)及び(3)

6 Where should the DPO be located?
6 DPO は何処に配置されるべきか？

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union. However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union, a DPO may be able to carry out his or her activities more effectively if located outside the EU.
WP29 は、DPO へのアクセスを確保するため、管理者又は処理者が EU 内に設置されているか否かにかかわらず、DPO が EU 内に所在することを勧告する。しかしながら、管理者又は処理者が EU 内に拠点を有していない場合には、時として、DPO が EU 外に所在していた方が、その活動をより効果的に行うことができる可能性を排除することはできない。

7 Is it possible to appoint an external DPO?
7 外部 DPO を選任することは可能か？

Yes. The DPO may be a staff member of the controller or the processor (internal DPO) or fulfil the tasks on the basis of a service contract. This means that the DPO can be external, and in this case, his/her function can be exercised based on a service contract concluded with an individual or an organisation.
可能である。DPO は管理者又は処理者の職員（内部 DPO）でも良いし、業務契約に基づきその任務を果たすこともできる。このことは、DPO は外部者がなることも可能であり、この場合、その職務は個人又は組織と交わす業務契約に基づいて果たすことができることを意味している。

When the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the DPO tasks as a team, under the responsibility of a designated lead contact and 'person in charge' of the client. In this case, it is essential that each member of the external organisation exercising the functions of a DPO fulfils all applicable

requirements of the GDPR.
DPO の職務が外部の受託者によって果たされる場合、そこで勤務している従業員のチームは、顧客の選任された主要窓口及び「担当者」の責任の下で、チームとして DPO の任務を効率的に果たしうる。この場合、DPO の職務を果たす外部組織の各メンバーが、適用されるすべての GDPR の要件を満たすことが不可欠である。

For the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, the Guidelines recommend to have, in the service contract, a clear allocation of tasks within the external DPO team and to assign a single individual as a lead contact and person 'in charge' of the client.
法的な明確性及び良好な組織運営のため並びにチームメンバー間の利益相反を防止するため、本ガイドラインは、業務契約において、外部 DPO のチーム内における任務の割当てを明確に行い、特定の個人を顧客の主要窓口及び「担当者」として任命するよう勧告する。

Source: Article 37(6) of the GDPR
根拠規定：GDPR 第 37 条(6)

8 What are the professional qualities that the DPO should have?
8 DPO が備えているべき専門的資質とは何か？

The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil his or her tasks.
DPO は、専門的資質、特に、データ保護法及び実務の専門知識並びにその任務を遂行する能力に基づいて選任されなければならない。

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.
専門知識の必要水準は、行われるデータ取扱作業と取扱われる個人データに必要な保護に即して決められるべきである。例えば、データ取扱業務が特に複雑である場合、あるいは、大量のセンシティブデータが含まれる場合、DPO にはより高い水準の専門知識とサポート

が必要となろう。

Relevant skills and expertise include:
関連する技能及び専門知識には次のものがある。

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- 自国及び欧州のデータ保護法及び実務（GDPR の深い理解を含む）。
- understanding of the processing operations carried out
- 行われる取扱作業についての理解
- understanding of information technologies and data security
- 情報システム及びデータセキュリティについての理解
- knowledge of the business sector and the organization
- 事業分野及び組織についての知識
- ability to promote a data protection culture within the organization
- 組織内においてデータ保護の文化を促進させる能力

Source: Article 37(5) of the GDPR
根拠規定：GDPR 第 37 条(5)

9 What resources should be provided to the DPO by the controller or the processor?
9 DPO は管理者又は処理者からいかなるリソースを与えられるべきか？

The DPO must have the resources necessary to be able to carry out his or her tasks.
DPO はその任務を遂行するために必要なリソースを持たなければならない。

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:
取扱作業の性質及び組織の業務と規模に応じて、次に掲げるリソースが DPO に与えられるべきである。

- active support of the DPO's function by senior management
- 幹部によるDPOの職務への積極的なサポート
- sufficient time for DPOs to fulfil their tasks
- DPOが任務を全うするための十分な時間
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- 資金、インフラ（敷地、施設、設備）及び人員（適宜）に関する適切な支援
- official communication of the designation of the DPO to all staff
- 全ての職員に向けた DPO の選任についての正式な連絡
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- DPOが、組織内の他のサービス（人事、法務、ＩＴ、セキュリティー等）から不可欠なサポート、インプット又は情報を得るための当該サービスへのアクセス。
- continuous training
- 継続的な研修

Source: Article 38(2) of the GDPR
根拠規定：GDPR 第 38 条(2)

10 What are the safeguards to enable the DPO to perform her/his tasks in an independent manner? What does 'conflict of interests' mean?

10 DPOが独立した態様でその任務を遂行できるための保護措置は何か？「利益相反」とはどのような意味か？

Several safeguards exist in order to enable the DPO to act in an independent manner:
DPOを独立した態様で活動させるための保護措置がいくつか存在する。

- no instructions by the controllers or the processors regarding the exercise of the DPO's tasks
- DPOの任務遂行に関する管理者又は処理者による指示がないこと。
- no dismissal or penalty by the controller for the performance of the DPO's tasks
- DPOの任務遂行を理由とした管理者による解雇又は処罰がないこと
- no conflict of interest with possible other tasks and duties
- 発生しうる他の任務又は義務との利益相反がないこと

The other tasks and duties of a DPO must not result in a conflict of interests. This means, first, that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.
DPOの他の任務及び義務は利益相反するものであってはならない。このことは、第一に、DPOが組織内において個人データの取扱いの目的及び方法を決めることにつながる地位に就けないことを意味する。各組織に特有の組織構造があるため、この点は事例ごとに検討されなければならない。

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.
大まかにいって、組織内において利益相反の立場には、幹部の地位（最高経営責任者、最高執行責任者、最高財務責任者、最高医務責任者、マーケティング部長、人事部長又はIT部

長など）のほか、組織構造内でそれよりも低い地位も、その地位又は役職が個人データの取扱いの目的及び方法の決定につながる場合には、含まれよう。また、利益相反は、例えば、データ保護が絡む事件の法廷において、外部の DPO が管理者又は処理者の代理を依頼された場合にも生じうる。

Source: Article 38(3) and 38(6) of the GDPR
根拠規定：GDPR 第 38 条(3)及び第 38 条(6)

11 What does 'monitoring compliance' mean?
11 「遵守の監視」とはどのような意味か？

As part of these duties to monitor compliance, DPOs may, in particular:
遵守を監視する職責の一環として、DPO は特に下記の項目を行うことができる。

- collect information to identify processing activities
- 取扱業務を特定するため情報を収集する
- analyse and check the compliance of processing activities
- 取扱業務の遵守状況を分析し、チェックする
- inform, advise and issue recommendations to the controller or the processor
- 管理者又は処理者に通知し、助言し、勧告を行う

Source: Article 39(1)(b) of the GDPR
根拠規定：GDPR 第 39 条(1)(b)

12 Is the DPO personally responsible for non-compliance with data protection requirements?
12 DPO はデータ保護に係る義務の不遵守に対し個人的に責任を負うか？

No. DPOs are not personally responsible for non-compliance with data protection requirements. It is the controller or the processor who is required to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Data protection compliance is the responsibility of the controller or the processor.
負わない。DPO は、データ保護に係る義務の不遵守に対し個人的に責任を負わない。取扱いがこの規則に従って行われるように確実を期し、それを証明できるように求められているのは管理者又は処理者である。データ保護の遵守は管理者や処理者の責任である。

13 What is the role of the DPO with respect to data protection impact assessments and records of processing activities?
13 データ保護影響評価及び取扱活動の記録における DPO の役割は何か？

As far as the data protection impact assessment is concerned, the controller or the processor should seek the advice of the DPO, on the following issues, amongst others:
データ保護影響評価に関する限り、管理者又は処理者は、とりわけ、下記の問題について DPO の助言を求めるべきである。

- whether or not to carry out a DPIA
- DPIA を行うかどうか
- what methodology to follow when carrying out a DPIA
- DPIA を行う際、どのような方法を採るか
- whether to carry out the DPIA in-house or whether to outsource it
- DPIA を内部で実行するか、外注するか
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- データ主体の権利及び利益に対するリスクを緩和するため、どのような保護措置（技術的及び組織的措置を含む）を適用するか
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements
- DPIA が正しく行われたか、及び結論（取扱いを進めるかどうか及びどのような保護措置を適用するか）がデータ保護に係る義務に準拠しているか

As far as the records of processing activities are concerned, it is the controller or the processor, not the DPO, who is required to maintain records of processing operations. However, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the records of processing operations under the responsibility of the controller or the processor. Such records should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.
取扱業務の記録に関する限り、取扱作業の記録を保持することを要求されているのは DPO ではなく、管理者又は処理者である。しかしながら、管理者又は処理者がその責任の下で、取扱作業の記録保存の任務を DPO に割り当てることを妨げるものではない。かかる記録は、DPO がその任務である遵守監視、管理者又は処理者への通知及び助言といった任務を遂行できるようにするツールの一つと考えるべきである。

Source: Article 39(1)(c) and Article 30 of the GDPR

根拠規定：GDPR 第 39 条(1)(c)及び第 30 条