仮日本語訳

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

Version 2.0

Adopted on 7 July 2021

GDPR における管理者及び処理者の概念に関するガイドライン 07/2020

バージョン **2.0**

2021 年 7 月 7 日に採択

2021年7月7日、The European Data Protection Board (欧州データ保護会議)は、”Guidelines 07/2020 on the concepts of controller and processor in the GDPR " を採択した。本文書は、本ガイドラインを個人情報保護委員会が翻訳したものである。本書面は参考のための仮日本語訳であって、その利用について当委員会は責任を負わないものとし、正確な内容については原文を参照されたい。

Version history

バージョン履歴

Version 2.0	7 July 2021 2021 年 7 月 7 日	Adoption of the Guidelines after public consultation パブリックコンサルテーション後にガイドラインを採択
Version 1.0	2 September 2020 2020 年 9 月 2 日	Adoption of the Guidelines for public consultation パブリックコンサルテーションのためにガイドラインを採択

EXECUTIVE SUMMARY

概要

The concepts of controller, joint controller and processor play a crucial role in the application of the General Data Protection Regulation 2016/679 (GDPR), since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The precise meaning of these concepts and the criteria for their correct interpretation must be sufficiently clear and consistent throughout the European Economic Area (EEA).

管理者、共同管理者及び処理者の概念は、彼らが様々なデータ保護ルールの遵守に責任を負う者及びデータ主体が実際に自己の権利を行使できる方法を決定することから、一般データ保護規則2016/679（GDPR）の適用において重要な役割を果たす。これらの概念の正確な意義及び正しい解釈の基準は、EEA加盟国全体を通じて十分に明確、かつ、一貫性のあるものでなければならない。

The concepts of controller, joint controller and processor are *functional* concepts in that they aim to allocate responsibilities according to the actual roles of the parties and *autonomous* concepts in the sense that they should be interpreted mainly according to EU data protection law.

管理者、共同管理者及び処理者の概念は、当事者の実際の役割に応じて責任を割り当てることを目的とする機能的概念であり、主としてEUデータ保護法に準拠して解釈されるべきであるという意味で自律的概念である。

Controller

管理者

In principle, there is no limitation as to the type of entity that may assume the role of a controller but in practice it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller.

原則として、管理者の役割を担うことができる主体の種類に制限はないが、実際には、通常、管理者として行動するのは組織それ自体であり、組織内の個人（CEO、従業員、取締役会のメンバーなど）ではない。

A controller is a body that *decides* certain key elements of the processing. Controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. Certain processing activities can be seen as naturally

attached to the role of an entity (an employer to employees, a publisher to subscribers or an association to its members). In many cases, the terms of a contract can help identify the controller, although they are not decisive in all circumstances.

管理者は、取扱いに関する特定の重要な要素を決定する組織である。管理者職は法律によって定義される場合もあれば、事例の状況又は事実に基づく要素の分析から生じる場合もある。一定の取扱活動は、主体の役割（従業員に対する雇用者、購読者に対する発行者、又は協会会員に対する協会）に自然に付随しているとみなすことができる。多くの場合、契約条件は全ての状況において決定的なものではないが、管理者の識別に役立ち得る。

A controller determines the purposes and means of the processing, i.e. the *why* and *how* of the processing. The controller must decide on both purposes and means. However, some more practical aspects of implementation ("non-essential means") can be left to the processor. It is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.

管理者は、取扱いの目的及び手段、すなわち、取扱いの理由及び方法を決定する。管理者は、目的及び手段の双方を決定しなければならない。しかしながら、いくつかのより実用的な側面（「非本質的な手段」）は、処理者に任せることができる。管理者は、管理者として適格であるとみなされるために取扱い中のデータに実際にアクセスできる必要はない。

Joint controllers

共同管理者

The qualification as joint controllers may arise where more than one actor is involved in the processing. The GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. Joint participation can take the form of a *common decision* taken by two or more entities or result from *converging decisions* by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.

共同管理者としての適格性は、複数の行為者が取扱いに関与している場合に発生し得る。GDPRは、共同管理者に関する具体的なルールを導入し、彼らの関係を規律するための枠組みを設定している。共同管理が存在するための包括的な基準は、取扱業務の目的及び手段の決定における二者以上の主体の共同参加である。共同参加は、二者以上の主体によって行われる共同決定の形態を採ることも、二者以上の主体による相互補完的決定に起因することもある。相互補完的決定とは、その決定が互いを補完するものであり、かつ、取扱いの目的及び手段の決定に具体的な影響を与える態様で取扱いが発生するために必要である決定を指す。共同決定の重要な基準は、個々の当事者による取扱いが不可分である、すなわち、密接に関連しているという意味で、両当事者の参加なしには取扱いが可能とならない点である。共同参加には、一方で目的の決定を、他方で手段の決定を含める必要がある。

Processor

処理者

A processor is a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Two basic conditions for qualifying as processor exist: that it is a separate entity in relation to the controller and that it processes personal data on the controller's behalf.

処理者は、管理者に代わって個人データを取扱う自然人又は法人、公的機関、部局又はその他の組織である。処理者としての適格性を得るための、二つの基本的な条件がある。それは、管理者との関係において別個の主体であること、及び、管理者に代わって個人データを取り扱うことである。

The processor must not process the data otherwise than according to the controller's instructions. The controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means. A processor infringes the GDPR, however, if it goes beyond the controller's instructions and starts to determine its own purposes and means of the processing. The processor will then be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.

処理者は、管理者の指示に従う以外にデータを取扱ってはならない。管理者の指示は、管理者の利益に最も資する方法について処理者が最も適切な技術的及び組織的な方法を選択できるある程度の裁量の余地を残す場合がある。しかしながら、処理者が管理者の指示を超えて、自身の取扱いの目的及び手段の決定を始めた場合、GDPRを侵害することとなる。

その場合、処理者はその取扱いに関して管理者とみなされることになり、管理者の指示を超えたことにつき制裁の対象となり得る。

Relationship between controller and processor

管理者と処理者の関係

A controller must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR. Elements to be taken into account could be the processor's expert knowledge (e.g. technical expertise with regard to security measures and data breaches); the processor's reliability; the processor's resources and the processor's adherence to an approved code of conduct or certification mechanism.

管理者は、その取扱いがGDPRの要件を満たすように、適切な技術上及び組織上の措置を実施するための十分な保証を提供する処理者のみを利用しなければならない。考慮すべき要素には、処理者の専門知識（例：安全管理措置及びデータ侵害に関する技術的な専門知識）、処理者の信頼性、処理者のリソース及び処理者による承認された行動規範又は認証メカニズムの遵守があり得る。

Any processing of personal data by a processor must be governed by a contract or other legal act which shall be in writing, including in electronic form, and be binding. The controller and the processor may choose to negotiate their own contract including all the compulsory elements or to rely, in whole or in part, on standard contractual clauses.

処理者による個人データの取扱いは、書面（電子形式を含む）による、拘束力のある契約又はその他の法律行為により規律されなければならない。管理者及び処理者は、全ての必須要素を含む独自の契約を交渉するか、全体的又は部分的に標準契約条項に依拠するかを選択できる。

The GDPR lists the elements that have to be set out in the processing agreement. The processing agreement should not, however, merely restate the provisions of the GDPR; rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.

GDPRには、取扱契約に定めるべき要素のリストが記載されている。しかしながら、取扱契約には、GDPRの規定を単に再述すべきではなく、むしろ、要件がいかにして充足されるか、及び、取扱契約の目的である個人データの取扱いにどのレベルの安全管理が要求されるかに関する、より具体的で、明確な情報を記載するべきである。

Relationship among joint controllers

共同管理者間の関係

Joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the GDPR. The determination of their respective responsibilities must in particular regard the exercise of data subjects' rights and the duties to provide information. In addition to this, the distribution of responsibilities should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities.

共同管理者は、GDPRに定める義務の遵守に係るそれぞれの責任を透明性のある態様で決定し、合意しなければならない。それぞれの責任の決定に当たっては、特にデータ主体の権利の行使及び情報を提供する義務を考慮しなければならない。これに加えて、責任配分には、一般データ保護原則、法的根拠、安全管理措置、データ侵害通知義務、データ保護影響評価、処理者の利用、第三国への移転、並びに、データ主体及び監督機関との連絡などに関する、他の管理者の義務を考慮すべきである。

Each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.

個々の共同管理者には、データ取扱いの法的根拠を有することを確保し、当該データが、それを共有する管理者が最初に収集した目的と矛盾する態様でさらに取扱われないよう確保する義務がある。

The legal form of the arrangement among joint controllers is not specified by the GDPR. For the sake of legal certainty, and in order to provide for transparency and accountability, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject.

共同管理者間の取決めの法的形式は、GDPRには明記されていない。法的確実性の目的で、また、透明性及びアカウンタビリティを提供するため、EDPBは、そのような取決めを、契約又は管理者を対象とするEU又は加盟国の法律に基づく法的拘束力を有する行為など、拘束力を有する文書の形式で行うよう勧告する。

The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à- vis the data subjects and the essence of the arrangement shall be made available to the data subject.

取決めは、データ主体に対する共同管理者のそれぞれの役割及び関係を適切に反映しなければならず、当該取決めの要点はデータ主体が利用できるようにされなければならない。

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers. Supervisory authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point.

取決めの条件に関わらず、データ主体は、個々の共同管理者に関して、また、個々の共同管理者に対してその権利を行使することができる。監督機関は、共同管理者としての当事者の適格性の問題であれ、指定された連絡先の問題であれ、取決めの条件には拘束されない。

Table of contents

目次

The European Data Protection Board

欧州データ保護会議は

Having regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR" or "the Regulation"),

個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令95/46/EC を廃止する欧州議会及び理事会の2016年4月27日の規則(EU) 2016/679(以下「GDPR」又は「本規則」)第70条第1項(e)を考慮し、

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

2018年7月6日付EEA合同委員会第154/2018号の決定により修正された、EEA合意、特にその別紙XI及びその議定書37を考慮し[1]、

Having regard to Article 12 and Article 22 of its Rules of Procedure,

手続規則第12条及び第22条を考慮して、

Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a stakeholder event, in order to identify the most pressing challenges;

一方で、本ガイドラインの準備作業において、最も差し迫った課題を明らかにするため、書面及びステークホルダー(利害関係者)・イベント双方における利害関係者からのインプットの収集も行った上で、

HAS ADOPTED THE FOLLOWING GUIDELINES

以下のガイドラインを採択した。

INTRODUCTION

はじめに

1. This document seeks to provide guidance on the concepts of controller and processor

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
この文書全体でなされている「加盟国」「加盟各国」への言及は、「EEA加盟国」への言及と理解されるべきである。

based on the GDPR's rules on definitions in Article 4 and the provisions on obligations in chapter IV. The main aim is to clarify the meaning of the concepts and to clarify the different roles and the distribution of responsibilities between these actors.

この文書は、第4条の定義に係るGDPRのルール及び第4章の義務に係る条項に基づく管理者及び処理者の概念に関するガイダンスを提供することを目的としている。その主たる目的は、当該概念の意味並びに、これらの行為主体間の様々な役割及び責任の配分を明確にすることである。

2. The concept of controller and its interaction with the concept of processor play a crucial role in the application of the GDPR, since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The GDPR explicitly introduces the accountability principle, i.e. the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data in Article 5. Moreover, the GDPR also introduces more specific rules on the use of processor(s) and some of the provisions on personal data processing are addressed - not only to controllers - but also to processors.

管理者の概念及び当該概念と処理者の概念の相互関係は、GDPRの適用に重要な役割を果たす。それらが、様々なデータ保護規則の遵守に対する責任者が誰であるかということ及びデータ主体による実際の権利行使方法を決定するためである。GDPRは、アカウンタビリティの原則を明示的に導入している。すなわち、管理者は、第5条の個人データの取扱いに関連する原則に責任を負い、その遵守を証明できなければならないとしている。さらに、GDPRは、処理者の利用に関するより具体的なルールも導入しており、個人データの取扱いに関するいくつかの条項は、管理者だけでなく、処理者にも対処するものである。

3. It is therefore of paramount importance that the precise meaning of these concepts and the criteria for their correct use are sufficiently clear and shared throughout the European Union and the EEA.

したがって、これらの概念の正確な意味及びそれらを正しく利用するための基準が十分に明確であり、欧州連合及びEEA全体を通じて共有されていることが最も重要である。

4. The Article 29 Working Party issued guidance on the concepts of controller/processor

in its opinion 1/2010 (WP169)[2] in order to provide clarifications and concrete examples with respect to these concepts. Since the entry into force of the GDPR, many questions have been raised regarding to what extent the GDPR brought changes to the concepts of controller and processor and their respective roles. Questions were raised in particular to the substance and implications of the concept of joint controllership (e.g. as laid down in Article 26 GDPR) and to the specific obligations for processors laid down in Chapter IV (e.g. as laid down in Article 28 GDPR). Therefore, and as the EDPB recognizes that the concrete application of the concepts needs further clarification, the EDPB now deems it necessary to give more developed and specific guidance in order to ensure a consistent and harmonised approach throughout the EU and the EEA. The present guidelines replace the previous opinion of Working Party 29 on these concepts (WP169).

第29条作業部会は、これらの概念に関する説明及び具体例を提供するため、その意見書1/2010（WP169）[2]において、管理者/処理者の概念に関するガイダンスを発行した。GDPRが管理者及び処理者の概念並びにそれぞれの役割にどの程度の変化をもたらしたかにつき、GDPRの発効以来、多くの質問が提起されている。質問は、特に、共同管理の概念の本質及びその含意（例としてGDPR第26条に規定される内容）並びに第4章に規定されている処理者の具体的な義務（例として、GDPR第28条に規定される内容）について提起された。したがって、また、EDPBはこれらの概念の具体的な適用にはさらに明確化が必要であると認識していることから、EDPBは、現在、EU及びEEA全体で一貫性のある調和のとれたアプローチを確保するため、より発展した具体的なガイダンスを提供する必要があると考えている。現行のガイドラインは、これらの概念に関する第29条作業部会の従前の意見書（WP169）を置き換えるものである。

5. In part I, these guidelines discuss the definitions of the different concepts of controller, joint controllers, processor and third party/recipient. In part II, further guidance is provided on the consequences that are attached to the different roles of controller, joint controllers and processor.

本ガイドラインの第1部では、管理者、共同管理者、処理者及び第三者/取得者という、様々な概念の定義について説明する。第2部では、管理者、共同管理者及び処理者の

[2] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" adopted on 16 February 2010, 264/10/EN, WP 169.
2010年2月16日に採択された「管理者」及び「処理者」の概念に関する第29条作業部会意見書1/2010（264/10/EN、WP169）

様々な役割に付随する影響につき、追加的なガイダンスを提供する。

PART I – CONCEPTS

第1部－ 概念

1. GENERAL OBSERVATIONS

概説

6. The GDPR, in Article 5(2), explicitly introduces the accountability principle which means that:

GDPRは、第5条第2項において、以下を意味するアカウンタビリティの原則を明示的に導入している。

– the controller shall be *responsible for the compliance* with the principles set out in Article 5(1) GDPR; and that

管理者は、GDPR第5条第1項に定められた原則の*遵守に責任を負わなければならない*。そして、

– the controller shall be able to *demonstrate compliance* with the principles set out in Article 5(1) GDPR.

管理者は、GDPR第5条第1項に定められた原則の*遵守を証明できなければならない*。

This principle has been described in an opinion by the Article 29 WP[3] and will not be discussed in detail here.

この原則は、第29条作業部会による意見書[3]で説明されており、ここでは詳細に説明しない。

7. The aim of incorporating the accountability principle into the GDPR and making it a central principle was to emphasize that data controllers must implement appropriate and effective measures and be able to demonstrate compliance.[4]

アカウンタビリティの原則をGDPRに組み込み、それを中心的な原則とする目的は、データ管理者が適切かつ効果的な措置を講じ、かつその遵守を証明できなければならない

[3] Article 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 00062/10/EN WP 173.

2010年7月13日に採択された説明責任の原則に関する第29条作業部会意見書3/2010（、00062/10/EN WP173）。

[4] Recital 74 GDPR

GDPR前文（74）

ことを強調することであった。[4]

8. The accountability principle has been further elaborated in Article 24, which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able **to demonstrate** that processing is performed in accordance with the GDPR. Such measures shall be reviewed and updated if necessary. The accountability principle is also reflected in Article 28, which lays down the controller's obligations when engaging a processor.

アカウンタビリティの原則は第24条でさらに詳しく説明されており、管理者は取扱いがGDPRに準拠して実行されることを確保し、かつ、これを証明できるよう、適切な技術上及び組織上の措置を講じなければならないと規定されている。そのような措置は、必要に応じて見直され、更新されなければならない。アカウンタビリティの原則は第28条にも反映されており、処理者を従事させる際の管理者の義務が規定されている。

9. The accountability principle is directly addressed to the controller. However, some of the more specific rules are addressed to both controllers and processors, such as the rules on supervisory authorities' powers in Article 58. Both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them and both are directly accountable towards supervisory authorities by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders. At the same time, it should be recalled that processors must always comply with, and act only on, instructions from the controller.

アカウンタビリティの原則は、直接的には管理者に対応するものである。しかしながら、第58条の監督機関の権限に関するルールなど、より具体的なルールのいくつかは、管理者及び処理者の双方に対応している。管理者及び処理者に関連するGDPRの義務に違反した場合、制裁金を課せされる可能性は双方ともにあり、また、双方とも、適切な文書を保管し、要求に応じてこれを提供し、調査がある場合これに協力し、行政命令に従う義務に基づき、監督機関に対し直接に説明責任を負う。同時に、処理者は常に管理者の指示を遵守し、それにのみ基づき行動しなければならないことを想起すべきである。

10. The accountability principle, together with the other, more specific rules on how to comply with the GDPR and the distribution of responsibility, therefore makes it necessary to define the different roles of several actors involved in a personal data

processing activity.

したがって、アカウンタビリティの原則により、GDPRの遵守の方法及び責任の配分に関する他のより具体的なルールと相俟って、個人データ取扱活動に関与する複数の行為主体の様々な役割の定義の策定が必須となるよう至らしめる。

11. A general observation regarding the concepts of controller and processor in the GDPR is that they have not changed compared to the Directive 95/46/EC and that overall, the criteria for how to attribute the different roles remain the same.

概説として、GDPRにおける管理者及び処理者の概念は、指令95/46/ECと比較して変更されておらず、全体として、様々な役割をどのように帰属させるかの基準は同様のままであるということが言える。

12. The concepts of controller and processor are *functional* concepts: they aim to allocate responsibilities according to the actual roles of the parties.[5] This implies that the legal status of an actor as either a "controller" or a "processor" must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a "controller" or "processor" (e.g. in a contract).[6] This means that the allocation of the roles usually should stem from an analysis of the factual elements or circumstances of the case and as such is not negotiable.

管理者及び処理者の概念は機能的概念であり、当事者の実際の役割に応じて責任を割り当てることを目的としている。[5] これは、「管理者」であれ、「処理者」であれ、行為主体の法的地位は、原則として、(契約などにおいて)行為主体を「管理者」又は「処理者」とする形式的な指定によるのではなく、具体的な状況における実際の活動により決定されなければならないことを意味している。[6] つまり、役割の割り当ては、交渉することはできず、通常、事実上の要素や状況の分析に基づいて行われるべきである。

---

[5] Article 29 Working Party Opinion 1/2010, WP 169, p. 9.
第29条作業部会WP意見書1/2010, WP 169、9ページ。

[6] See also the Opinion of Advocate General Mengozzi, in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:57, paragraph 68 ("*For the purposes of determining the 'controller' within the meaning of Directive 95/46, I am inclined to consider [….] that excessive formalism would make it easy to circumvent the provisions of Directive 95/46 and that, consequently, it is necessary to rely upon a more factual than formal analysis […].*")
*Jehovah's witnesses事件*におけるMengozzi法務官の意見書(C-25/17, ECLI:EU:C:2018:57)、第68段落(「*指令95/46の意味の範囲内で「管理者」を決定する目的において、私は[…]過度の形式主義においては指令95/46の規定の回避が容易となってしまう。したがって、形式的な分析よりもより事実に基づく分析に依拠する必要があると考える傾向にある[…]。*」)も参照。

13. The concepts of controller and processor are also *autonomous* concepts in the sense that, although external legal sources can help identifying who is a controller, it should be interpreted mainly according to EU data protection law. The concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights or competition law.

管理者及び処理者の概念は、外部の法源は管理者が誰であるかを識別するのに役立ちうるが、主としてEUデータ保護法に準拠して解釈されるべきであるという意味において、自律的概念でもある。管理者の概念は、知的財産権法又は競争法上の制作者又は権利保有者など、他の法律分野における他の（しばしば、衝突したり重複したりする）概念によって損なわれるべきではない。

14. As the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, the concept of 'controller' should be interpreted in a sufficiently broad way, favouring as much as possible effective and complete protection of data subjects[7] so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules, while at the same time not diminishing the role of the processor.

管理者の役割を帰属させる基本的な目的は、アカウンタビリティ及び個人データの効果的かつ包括的な保護を確保することであるから、「管理者」の概念は、十分広義に解釈されるべきであり、EUデータ保護法の完全な効果を確保し、ルールの欠陥を回避し、脱法行為の可能性を防止するため、データ主体[7]の効果的かつ完全な保護を可能な限り優先し、同時に処理者の役低下させないようにすべきである。

2. DEFINITION OF CONTROLLER

管理者の定義

[7] CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014, paragraph 34; CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, judgment of 5 June 2018, paragraph 28;CJEU, Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, judgment of 29 July 2019, paragraph 66.
CJEUの判決文（C-131/12）、Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González、2014年5月13日、第34段落; CJEUの判決文（C-210/16）、Wirtschaftsakademie Schleswig-Holstein、2018年6月5日、第28段落;CJEUの判決文（C-40/17）、Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV、2019年7月29日、パラグラフ66, judgment of 29 July 2019、第66段落。

2.1 Definition of controller
管理者の定義

15. A controller is defined by Article 4(7) GDPR as

管理者は、GDPR第4条第7項において、次のとおり定義されている。

> *"**the natural or legal person, public authority, agency or other body** which, **alone or jointly with others, determines** the **purposes and means** of the **processing of personal data**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be **provided for by Union or Member State law**".*
>
> *「**自然人又は法人、公的機関、部局又はその他の組織**であって、**単独で又は他の者と共同**で、**個人データの取扱いの目的及び手段を決定する**者を意味する。その取扱いの目的及び手段が**EU**法又は加盟国の国内法によって決定される場合、管理者又は管理者を指定するための特定の基準は、**EU法又は加盟国の国内法によって定める**ことができる」。*

16. The definition of controller contains five main building blocks, which will be analysed separately for the purposes of these Guidelines. They are the following:

管理者の定義には、五つの主要な構成要素が含まれており、これらは、本ガイドラインの目的において個別に分析される。それらは、以下のとおり。

- "the natural or legal person, public authority, agency or other body"
  「自然人又は法人、公的機関、部局又はその他の組織」
- "determines"
  「決定する」
- "alone or jointly with others"
  「単独で、又は他の者と共同で」
- "the purposes and means"
  「目的及び方法」
- "of the processing of personal data".
  「個人データの取扱いの」

2.1.1 "Natural or legal person, public authority, agency or other body"
「自然人又は法人、公的機関、部局又はその他の組織」

17. The first building block relates to the type of entity that can be a controller. Under

the GDPR, a controller can be "*a natural or legal person, public authority, agency or other body*". This means that, in principle, there is no limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.[8] In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR. As far as data processing within a company group is concerned, special attention must be paid to the question of whether an establishment may be acting as a controller or processor, e.g. when processing data on behalf of the parent company.

第一の構成要素は、管理者になり得る主体の種類に関連している。GDPRの下では、管理者には「*自然人又は法人*、*公的機関*、*部局又はその他の組織*」がなり得る。これは、原則として、管理者の役割を引き受けることができる主体の種類に制限がないことを意味する。組織の場合があるかもしれず、個人又は個人のグループの場合もあるかもしれない。[8] しかしながら、実際には、通常は管理者として行動するのはGDPRの意義の範囲内で管理者として行動する組織であり、組織内の個人（CEO、従業員又は取締役会のメンバーなど）ではない。企業グループ内のデータ取扱いに関する限り、例えば、親会社に代わってデータを取扱う場合、拠点が管理者として行動するか又は処理者として行動するかの問題に特別な注意を払う必要がある。

18. Sometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing activity. Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller. In the same vein, even if a particular department or unit of an organisation has operational responsibility for ensuring compliance for certain processing activity, it does not mean that this department or unit (rather than the organisation as a whole) becomes the controller.

会社や公的組織は、しばしば、取扱業務の実施に責任を持つ特定の者を任命する。デ

[8] For example, in its Judgment in Jehovah's witnesses, C-25/17, ECLI:EU:C:2018:551, paragraph 75, the CJEU considered that a religious community of Jehovah's witnesses acted as a controller, jointly with its individual members. Judgment in Jehovah's witnesses, C-25/17, ECLI:EU:C:2018:551, paragraph 75.

例えば、Jehovah's witnesses事件の判決文（C-25/17、ECLI:EU:C:2018:551）、第75段落において、CJEUは、エホバの証人の宗教的共同体は個々のメンバーと共同で管理者として行動したと見なした。Jehovah's witnesses事件の判決文（C-25/17、ECLI:EU:C:2018:551）、第75段落。

ータ保護ルールの遵守を確保するために特定の自然人が任命された場合においても、その者は、管理者とはならず、同ルール違反の場合に管理者の立場で最終的に責任を負う法的主体（会社又は公的組織）に代わって行動する。同様に、組織の特定の部署やユニットが、特定の取扱業務のコンプライアンスを確保する運営上の責任を持っていたとしても、（組織全体ではなく）その部署やユニットが管理者になるわけではない。

Example:
The marketing department of Company ABC launches an advertising campaign to promote ABC's products. The marketing department decides the nature of campaign, the means to be used (e-mail, social media ...), which customers to target and what data to use in order to make the campaign as successful as possible. Even if the marketing department acted with considerable independence, Company ABC will in principle be considered as the controller seeing as the advertising campaign is launched by the company and takes place within the realm of its business activities and for its purposes.

例:
ABC社のマーケティング部門は、ABC社の製品を宣伝するための広告キャンペーンを開始する。マーケティング部門は、キャンペーンを可能な限り成功させるために、キャンペーンの性質、使用する手段（電子メール、ソーシャルメディア...）、対象とする顧客、使用するデータを決定する。マーケティング部門がかなり独立して行動したとしても、広告キャンペーンがABC社によって開始され、その事業活動の範囲内で、その目的のために行われていることを考えると、原則としてABC社が管理者であると考えられる。

19. In principle, any processing of personal data by employees which takes place within the realm of activities of an organisation may be presumed to take place under that organisation's control.[9] In exceptional circumstances, however, it may occur that an employee decides to use personal data for his or her own purposes, thereby unlawfully exceeding the authority that he or she was given. (e.g. to set up his own company or similar). It is therefore the organisation's duty as controller to make sure that there are adequate technical and organizational measures, including e.g.

[9] Employees who have access to personal data within an organisation are generally not considered as "controllers" or "processors", but rather as "persons acting under the authority of the controller or of the processor" within the meaning of article 29 GDPR.
組織内で個人データにアクセスできる従業員は、一般的に「管理者」または「処理者」とはみなされず、GDPR第29条の意味における「管理者または処理者の権限の下で行動する者」とみなされる。

training and information to employees, to ensure compliance with the GDPR.[10]

原則として、組織の活動範囲内で行われる従業員による個人データの取扱いは、その組織の管理下で行われると推定される。[9] しかし、例外的に、従業員が自分の目的のために個人データを使用することを決定し、与えられた権限を違法に超えてしまうことがあります。(例：自分の会社を設立する場合など)。) したがって、GDPRの遵守を確保するために、従業員への研修や情報提供など、技術的・組織的に適切な安全管理措置を講じることは、管理者である組織の義務である。[10]

2.1.2 "Determines"
「決定する」

20. The second building block of the controller concept refers to the controller's *influence* over the processing, by virtue of an *exercise of decision-making power*. A controller is a body that *decides* certain key elements about the processing. This controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. One should look at the specific processing operations in question and understand who determines them, by first considering the following questions: "*why is this processing taking place*?" and "*who decided that the processing should take place for a particular purpose?*".

管理者の概念の第二の構成要素は、*意思決定権限の行使*に基づく、取扱いに対する管理者の*影響*に言及する。管理者は、取扱いに関する一定の重要な要素を*決定する*組織である。管理者職は、法律によって定義される場合もあれば、事案の状況又は事実にもとづく要素の分析から生じる場合もある。問題となっている特定の取扱業務に関して、誰がそれを決定するかを理解するにあたり、最初に次の質問を検討するべきである。「*なぜこの取扱いが発生しているのか？*」及び「*誰が、特定の目的のためにこの取扱いを行うべきであると決定したのか？*」

Circumstances giving rise to control

管理を生じさせる状況

21. Having said that the concept of controller is a functional concept, it is therefore based on a **factual rather than a formal analysis**. In order to facilitate the analysis, certain rules of thumb and practical presumptions may be used to guide and simplify the process. In most situations, the "determining body" can be easily and clearly

[10] Article 24(1) GDPR.
GDPR第24条第1項。

identified by reference to certain legal and/or factual circumstances from which "influence" normally can be inferred, unless other elements indicate the contrary. Two categories of situations can be distinguished: (1) control stemming from *legal provisions*; and (2) control stemming from *factual influence*.

管理者の概念は機能的概念であると述べた。したがって、それは**形式的な分析ではなく事実に基づく分析**に依拠している。分析を促進する目的で、その過程を導き、簡素化するため、一定の経験則及び実務的な推定を利用する場合がある。ほとんどの場合、「決定を行う組織」は、他の要素が反対のことを示さない限り、通常は「影響」が推測できる一定の法的状況及び/又は事実に基づく状況を参照することにより、容易かつ明確に識別できる。このような状況は次の二つの類型に区分できる。(1) *法規定*に起因する管理、及び、(2) *事実に基づく影響*に起因する管理。

1) *Control stemming from legal provisions*

法規定に起因する管理

22. There are cases where control can be inferred from explicit legal competence e.g., when the controller or the specific criteria for its nomination are designated by national or Union law. Indeed, Article 4(7) states that *"where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."* While Article 4(7) only refers to "the controller" in the singular form, the EDPB considers that it may also be possible for Union or Member State law to designate more than one controller, possibly even as joint controllers.

明示的な法的権限から管理を推測できる場合がある。例えば、管理者又はその指名に関する具体的な基準が国内法又はEU法によって指定されている場合である。実際、第4条第7項は、*「その取扱いの目的及び手段がEU法又は加盟国の国内法によって決定される場合、管理者又は管理者を指定するための特定の基準は、EU法又は加盟国の国内法によって定めることができる」*と規定している。第4条第7項は、単体の「管理者」にのみ言及しているが、EDPBは、EU法又は加盟国の国内法が複数の管理者を指定することも可能であり、場合によっては共同管理者とすることも可能であると考えている。

23. Where the controller has been specifically identified by law this will be determinative for establishing who is acting as controller. This presupposes that the legislator has designated as controller the entity that has a genuine ability to exercise control. In some countries, the national law provides that public authorities are responsible for

processing of personal data within the context of their duties.

管理者が法律によって特定的に識別されている場合、これは、管理者として行動している者を確立するための決定要因になる。これは、立法者が、管理を実行する真の能力を有する主体を管理者として指定したことを前提とする。一部の国では、国内法において、公的機関がその義務の範囲内で個人データを取扱うことに責任を負うと規定している。

24. However, more commonly, rather than directly appointing the controller or setting out the criteria for its appointment, the law will establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task. For example, this would be the case where an entity which is entrusted with certain public tasks (e.g., social security) which cannot be fulfilled without collecting at least some personal data, sets up a database or register in order to fulfil those public tasks. In that case, the law, albeit indirectly, sets out who is the controller. More generally, the law may also impose an obligation on either public or private entities to retain or provide certain data. These entities would then normally be considered as controllers with respect to the processing that is necessary to execute this obligation.

しかしながら、より一般的には、法律は、管理者を直接任命する又はその任命の基準を定めるのではなく、職務を設けるか、一定のデータを収集し取扱う義務を誰かに課す。そのような場合、取扱いの目的は多くの場合法律によって決定される。管理者は、通常、この目的、この公的な職務を実現するために法律で指定された者になる。例えば、これは、少なくとも一部の個人データを収集しなければ遂行できない一定の公的な職務（例、社会保障）を委託された主体が、これらの公的な職務を遂行するためデータベースの構築または登録簿の設定を行う場合であろう。その場合、法律は、間接的ではあるが、誰が管理者であるかを定める。より一般的には、法律は、公的主体又は民間の主体に対し、一定のデータを保持又は提供する義務を課す場合もある。そこで、これらの主体は、通常、この義務を遂行するために必要な取扱いに関して管理者とみなされる。

Example: Legal provisions

The national law in Country A lays down an obligation for municipal authorities to provide social welfare benefits such as monthly payments to citizens depending on their financial situation. In order to carry out these payments, the municipal authority must collect and process data about the applicants' financial circumstances. Even though the law does

not explicitly state that the municipal authorities are controllers for this processing, this follows implicitly from the legal provisions.

例:法規定

A国の国内法は、市民の財務状況に応じて毎月の支払いなどの社会福祉給付を行う義務を市当局に対して定めている。これらの支払いを実行するため、市当局は申請者の財務状況に関するデータを収集し取扱わなければならない。国内法が市当局は管理者であると明示的に規定していない場合においても、このことは法規定から黙示的に理解される。

2) Control stemming from factual influence

事実にもとづく影響に起因する管理

25. In the absence of control arising from legal provisions, the qualification of a party as controller must be established on the basis of an assessment of the factual circumstances surrounding the processing. All relevant factual circumstances must be taken into account in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question.

法規定に起因する管理が存在しない場合、管理者としての当事者の適格性は、その取扱いを取り巻く事実にもとづく状況の評価に基づき確立されなければならない。問題の個人データの取扱いに関して特定の主体が決定的な影響力を行使するかどうかについて結論を出すためには、関連するすべての事実にもとづく状況が考慮されなければならない。

26. The need for factual assessment also means that the role of a controller does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity.

事実に基づく評価の必要性は、管理者の役割が、データを取扱う主体の性質ではなく、特定の文脈における管理者の具体的な行動に起因することも意味する。すなわち、同一の主体が、ある取扱業務の管理者として行動すると同時に、他の取扱業務の処理者として行動する場合がある。そして、管理者又は処理者としての適格性は、具体的なデータの取扱活動ごとに評価されなければならない。

27. In practice, certain processing activities can be considered as naturally attached to the role or activities of an entity ultimately entailing responsibilities from a data protection point of view. This can be due to more general legal provisions or an established legal practice in different areas (civil law, commercial law, labor law etc.). In this case, existing traditional roles and professional expertise that normally imply a certain responsibility will help in identifying the controller, for example: an employer in relation to processing personal data about his employees, a publisher processing personal data about its subscribers, or an association processing personal data about its members or contributors. When an entity engages in processing of personal data as part of its interactions with its own employees, customers or members, it will generally be the one who determines the purpose and means around the processing and is therefore acting as a controller within the meaning of the GDPR.

実際には、一定の取扱活動は、データ保護の観点から、最終的に責任を伴う主体の役割又は活動に必然的に付随しているとみなすことができる。これは、様々な分野（民法、商法、労働法など）における一般的な法規定又は確立された法律実務が原因である可能性がある。この場合、通常、一定の責任を意味する既存の伝統的な役割及び専門知識は、管理者（例えば、従業員の個人データの取扱いに関連する雇用者、購読者の個人データを取り扱う発行者、又は、協会の会員又は寄付者の個人データを取り扱う協会）を識別するのに役立つ。主体がその従業員、顧客又は会員とのやり取りの一環として個人データの取扱いに従事する場合、当該主体は、一般に取扱いの目的及び手段を事実にもとづいて決定する者であり、したがって、GDPRの意義の範囲内で管理者として行動している。

Example: Law Firms

The company ABC hires a law firm to represent it in a dispute. In order to carry out this task, the law firm needs to process personal data related to the case. The reasons for processing the personal data is the law firm's mandate to represent the client in court. This mandate however is not specifically targeted to personal data processing. The law firm acts with a significant degree of independence, for example in deciding what information to use and how to use it, and there are no instructions from the client company regarding the personal data processing. The processing that the law firm carries out in order to fulfil the task as legal representative for the company is therefore linked to the functional role of the law firm so that it is to be regarded as controller for this processing.

例:法律事務所

ABC社は、ある紛争において同社を代理する法律事務所を雇う。この職務を実行するため、法律事務所は、事件に関連する個人データを取り扱う必要がある。個人データを取り扱う理由は、法廷において顧客を代理するという法律事務所の責務である。しかしながら、この責務は、特に個人データの取扱いに的を絞ったものではない。法律事務所は、利用する情報やその利用方法の決定などについて、かなりの独立性を持って行動し、個人データの取扱いに関して顧客会社からの指示はない。したがって、法律事務所が会社の法定代理人としての職務を遂行するために実行する取扱いは、法律事務所の機能的役割に関連しており、法律事務所はこの取扱いの管理者とみなされる。

Example: Telecom operators[11]

Providing an electronic communications service such as an electronic mail service involves processing of personal data. The provider of such services will normally be considered a controller in respect of the processing of personal data that is necessary for the operation of the service as such (e.g., traffic and billing data). If the sole purpose and role of the provider is to enable the transmission of email messages, the provider will not be considered as the controller in respect of the personal data contained in the message itself. The controller in respect of any personal data contained inside the message will normally be considered to be the person from whom the message originates, rather than the service provider offering the transmission service.

例:通信事業者[11]

電子メールサービスなどの電子通信サービスの提供には、個人データの取扱いが伴う。このようなサービスの提供者は、通常、そのようなサービスの運営に必要な個人データの取扱い（例:通信及び請求データ）において、管理者とみなされる。プロバイダの唯一の目的及び役割が電子メールの送信を可能にすることである場合、プロバイダはメッセージ自体に含まれる個人データの管理者とはみなされない。メッセージに含まれる個人データに関する管理者は、通常、送信サービスを提供するサービス・プロバイダではなく、メッセージの発信元である個人であると考えられる。

28. In many cases, an assessment of the contractual terms between the different parties involved can facilitate the determination of which party (or parties) is acting as

[11] The EDPB considers that this example, previously included in Recital (47) of Directive 95/46/EC, remains relevant also under the GDPR.
EDPBは、指令95/46/ECの前文47に含まれていた本例は、GDPRの下でも関連性があると考えている。

controller. Even if a contract is silent as to who is the controller, it may contain sufficient elements to infer who exercises a decision-making role with respect to the purposes and means of the processing. It may also be that the contract contains an explicit statement as to the identity of the controller. If there is no reason to doubt that this accurately reflects the reality, there is nothing against following the terms of the contract. However, the terms of a contract are not decisive in all circumstances, as this would simply allow parties to allocate responsibility as they see fit. It is not possible either to become a controller or to escape controller obligations simply by shaping the contract in a certain way where the factual circumstances say something else.

多くの場合、関係する様々な当事者間の契約条件を評価することにより、いずれの当事者（又は複数当事者）が管理者として行動しているかの判断が促進される。契約が管理者を規定していない場合においても、取扱いの目的及び手段に関して誰が意思決定の役割を果たすかを推測するに十分な要素を含んでいる場合がある。契約が管理者の身元を明示的に規定している場合もある。これが現実を正確に反映していることにつき疑う理由がなければ、契約の条件に従うことに何ら問題もない。しかしながら、契約の条件は、全ての状況において決定的なものではない。全ての状況において決定的である場合、当事者がそれぞれが適切と見做すように責任を割り当てることになるからである。事実に基づく状況が別のことを示している場合に、契約をある一定の形式に整えるだけでは、管理者になることも、管理者の義務を免れることもできない。

29. If one party in fact decides why and how personal data are processed that party will be a controller even if a contract says that it is a processor. Similarly, it is not because a commercial contract uses the term “subcontractor” that an entity shall be considered a processor from the perspective of data protection law.[12]

ある当事者が実際に個人データを取り扱う理由及び方法を決定する場合、契約においてその者が処理者であると定められていたとしても、当該当事者は管理者となる。同様に、主体がデータ保護法の観点から処理者とみなされるのは、商業契約において「下請け業者」という用語が使用されているからではない。[12]

[12] See e.g., Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, WP128, p. 11.
例えば、2006年11月22日、国際銀行間通信協会 (SWIFT)による個人情報の取扱いに対する第29条作業部会の意見書、WP128, p. 11を参照。

30. In line with the factual approach, the word “determines” means that the entity that actually exerts a decisive influence on the purposes and means of the processing is the controller. Normally, a processor agreement establishes who the determining party (controller) and the instructed party (processor) are. Even if the processor offers a service that is preliminary defined in a specific way, the controller has to be presented with a detailed description of the service and must make the final decision to actively approve the way the processing is carried out and request changes if necessary. Furthermore, the processor cannot at a later stage change the essential elements of the processing without the approval of the controller.

事実に基づくアプローチにおいて、「決定する」という用語は、取扱いの目的及び手段に実際に決定的な影響を与える主体が管理者であることを意味する。通常、処理者契約において、誰が決定者（管理者）であり、誰が被指示者（処理者）であるかを規定する。処理者が特定の方法で事前に定義されたサービスを提供する場合においても、管理者は、サービスの詳細な説明を提示される必要があり、取扱いの実行方法を積極的に承認する最終的な決定を下し、必要に応じて変更を要求する。さらに、処理者は、管理者の承認なしに、後の段階において取扱いに係る重要な要素を変更することはできない。

Example: standardised cloud storage service

A large cloud storage provider offers its customers the ability to store large volumes of personal data. The service is completely standardised, with customers having little or no ability to customise the service. The terms of the contract are determined and drawn up unilaterally by the cloud service provider, provided to the customer on a “take it or leave it basis”. Company X decides to make use of the cloud provider to store personal data concerning its customers. Company X will still be considered a controller, given its decision to make use of this particular cloud service provider in order to process personal data for its purposes. Insofar as the cloud service provider does not process the personal data for its own purposes and stores the data solely on behalf of its customers and in accordance with instructions, the service provider will be considered as a processor.

例：標準化されたクラウドストレージサービス

ある大手クラウドストレージプロバイダは、顧客に大容量の個人データを保存する機能を提供している。このサービスは完全に標準化されており、顧客がサービスをカスタマイズすることはほとんどできないか。契約条件は、クラウド・サービス・プロバイダが一方的に決定・作成し、

「契約するか、しないか」で顧客に提供される。X社は、自社の顧客に関する個人データを保存するためにクラウドプロバイダーを利用することを決定した。X社は、自社の目的のために個人データを取扱うために、この特定のクラウド・サービス・プロバイダを利用することを決定したので、依然として管理者とみなされる。クラウド・サービス・プロバイダが自らの目的で個人データを取扱わず、顧客の代わりに、指示に従いデータを保存する場合は、サービス・プロバイダは処理者とみなされる。

2.1.3 “Alone or jointly with others”
「単独で、又は他の者と共同で」

31. Article 4(7) recognizes that the “purposes and means” of the processing might be determined by more than one actor. It states that the controller is the actor who “alone or jointly with others” determines the purposes and means of the processing. This means that several different entities may act as controllers for the same processing, with each of them then being subject to the applicable data protection provisions. Correspondingly, an organisation can still be a controller even if it does not make all the decisions as to purposes and means. The criteria for joint controllership and the extent to which two or more actors jointly exercise control may take different forms, as clarified later on.[13]

第4条第7項は、取扱いの「目的及び手段」が複数の者によって決定される可能性があることを認識している。同条は、管理者とは、「単独で又は他の者と共同で」取扱いの目的及び手段を決定する行為主体と規定している。これは、複数の異なる主体が同一の取扱いにおける管理者として行動でき、それぞれが適用可能なデータ保護規定の対象となることを意味する。これに対応して、組織は、目的及び手段に関してすべての決定を下さない場合にも、依然として管理者であり得る。共同管理の基準及び複数の者が共同で管理を行う範囲は、後述の通り、異なる形態をとる場合がある。[13]

2.1.4 “Purposes and means”
「目的及び手段」

32. The fourth building block of the controller definition refers to the object of the controller’s influence, namely the “purposes and means” of the processing. It represents the substantive part of the controller concept: what a party should determine in order to qualify as controller.

[13] See Part I, Section 3 (“Definition of joint controllers”).
第1章セクション3 (「共同管理者の定義」)を参照。

管理者の定義における第四の構成要素は、管理者の影響の対象、すなわち、取扱いの「目的及び手段」である。これは、管理者の概念の実質的な部分、管理者として適格であるために当事者が何を決定すべきかを示している。

33. Dictionaries define “purpose” as “an anticipated outcome that is intended or that guides your planned actions” and “means” as “how a result is obtained or an end is achieved”.

辞書では、「目的」を「意図された、または計画された行動の指針となる予想される結果」と定義し、「手段」を「結果が得られる方法又は目的が達成される方法」と定義している。

34. The GDPR establishes that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Determination of the "purposes" of the processing and the "means" to achieve them is therefore particularly important.

GDPRは、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態様で追加的取扱いをしてはならないと定めている。したがって、取扱いの「目的」及びそれらを達成するための「手段」の決定は、特に重要である。

35. Determining the purposes and the means amounts to deciding respectively the "why" and the "how" of the processing: [14] given a particular processing operation, the controller is the actor who has determined *why* the processing is taking place (i.e., “to what end”; or “what for”) and *how* this objective shall be reached (i.e. which means shall be employed to attain the objective). A natural or legal person who exerts such influence over the processing of personal data, thereby participates in the determination of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR.[15]

目的及び手段を決定することは、取扱いの「理由」及び「方法」をそれぞれ決定することとなる。[14] 特定の取扱業務の場合、管理者は、当該取扱いを行っている*理由*（すなわち、「何の目的で」又は「何のために」）及びこの目的を達成する*方法*（すなわち、その目的を

[14] See also the Opinion of Advocate General Bot in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, paragraph 46.
*Wirtschaftsakademie事件*のBot法務官の意見書（C-210/16, ECLI:EU:C:2017:796）、第46段落も参照。
[15] Judgment in *Jehovah’s witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 68.
*Jehovah’s witnesses事件*の判決文（C-25/17, ECLI:EU:C:2018:551）、第68段落。

達成するために採用される手段）を決定した行為主体である。個人データの取扱いにそのような影響を及ぼす自然人又は法人は、それにより、GDPR第4条第7項の定義に従って、当該取扱いの目的及び手段の決定に参加する。[15]

36. The controller must decide on both purpose and means of the processing as described below. As a result, the controller cannot settle with only determining the purpose. It must also make decisions about the means of the processing. Conversely, the party acting as processor can never determine the purpose of the processing.

管理者は、以下に説明するように、取扱いの目的及び手段の双方を決定しなければならない。結果的に、管理者は目的を決定するだけで解決することはできない。管理者は、手段についても決定しなければならない。逆に、処理者として行動する当事者は、取扱いの目的を決定することは決してできない。

37. In practice, if a controller engages a processor to carry out the processing on its behalf, it often means that the processor shall be able to make certain decisions of its own on how to carry out the processing. The EDPB recognizes that some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing. In this perspective, there is a need to provide guidance about which **level of influence** on the "why" and the "how" should entail the qualification of an entity as a controller and to what extent a processor may make decisions of its own.

実際に、管理者が自己に代わって取扱いを遂行する処理者を従事させる場合、それは、しばしば、処理者が取扱いの実行方法につき独自の一定の決定を行うことができることを意味する。EDPBは、処理者にも取扱いに関連していくつかの決定を下すことができるべく、ある程度の余地が存在し得ることを認識している。この観点から、「理由」及び「方法」に対するどの**程度の影響**が管理者としての主体の適格性に必要か、そして、処理者がどの程度独自の決定を下すことができるかに関し、ガイダンスを提供する必要がある。

38. When one entity clearly determines purposes and means, entrusting another entity with processing activities that amount to the execution of its detailed instructions, the situation is straightforward, and there is no doubt that the second entity should be regarded as a processor, whereas the first entity is the controller.

ある主体が目的及び手段を明確に決定し、詳細な指示の実行となる取扱活動を別の主体に委託する場合、状況は単純であり、二番目の主体は処理者とみなされるのに対し、最

初の主体は管理者とされることに疑いの余地はない。

Essential vs. non-essential means

本質的手段 対 非本質的手段

39. The question is where to draw the line between decisions that are reserved to the controller and decisions that can be left to the discretion of the processor. Decisions on the purpose of the processing are clearly always for the controller to make.

問題は、管理者に留保されている決定と、処理者の裁量に任せることができる決定との間の線引きである。取扱いの目的に関する決定は、明らかに常に管理者が行うものである。

40. As regards the determination of means, a distinction can be made between essential and non-essential means. “Essential means” are traditionally and inherently reserved to the controller. While nonessential means can also be determined by the processor, essential means are to be determined by the controller. “Essential means” are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed (“*which data shall be processed*?”), the duration of the processing (“*for how long shall they be processed?*”), the categories of recipients (“*who shall have access to them?*”) and the categories of data subjects (“*whose personal data are being processed?*”). Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate. “Non- essential means” concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.

手段の決定に関しては、本質的な手段と非本質的な手段を区別することができる。「本質的な手段」は、伝統的かつ本質的にコントローラに留保されている。非本質的な手段は処理者が決定することもできるが、本質的な手段は管理者が決定することになっている。「本質的な手段」とは、取り扱われる個人データの種類（「*どのデータが取り扱われるべきか*」）、取扱いの期間（「*どのくらいの期間データが取り扱われるべきか*」）、取得者の類型（「*誰がデータにアクセスするべきか*」）及びデータ主体の類型（「*誰の個人データが取り扱われているか*」）のような処理の目的と範囲に密接に関連する手段である。本質的な手段は、取扱いの目的とともに、合法的であるかどうか、必要であるかどうか、妥当であるかどうかという問題にも密接に関連している。「非本質的な手段」は、実施のより実用的な側面に

関係しており、特定の種類のハードウェア又はソフトウェアの選択や、詳細な安全管理措置など、処理者に決定を任せることができるものである。

Example: Payroll administration

Employer A hires another company to administer the payment of salaries to its employees. Employer A gives clear instructions on who to pay, what amounts, by what date, by which bank, how long the data shall be stored, what data should be disclosed to the tax authority etc. In this case, the processing of data is carried out for Company A's purpose to pay salaries to its employees and the payroll administrator may not use the data for any purpose of its own. The way in which the payroll administrator should carry out the processing is in essence clearly and tightly defined. Nevertheless, the payroll administrator may decide on certain detailed matters around the processing such as which software to use, how to distribute access within its own organisation etc. This does not alter its role as processor as long as the administrator does not go against or beyond the instructions given by Company A.

例:給与管理

雇用主Aは、従業員への給与の支払いを管理することになる別の会社を雇用する。雇用主Aは、誰に支払うか、支払額、支給日、振込先銀行、データ保存期間、税務当局に開示すべきデータなどについて明確な指示を出す。この場合、データの取扱いは、企業Aの従業員への給与支払の目的で実行され、給与管理者はそのデータを自己の目的で利用することはできない。給与管理者がその取扱いを実行する方法は、本質的に明確かつ厳密に定義されている。それにもかかわらず、給与管理者は、使用するソフトウェア、自己の組織内でアクセスを分散する方法など、取扱いに関する一定の詳細事項を決定できる。このことは、給与管理者が企業Aからの指示に反対しない限り(又はそれを超えない限り)、処理者としての役割を変更するものではない。

Example: Bank payments

As part of the instructions from Employer A, the payroll administration transmits information to Bank B so that they can carry out the actual payment to the employees of Employer A. This activity includes processing of personal data by Bank B which it carries out for the purpose of performing banking activity. Within this activity, the bank decides independently from Employer A on which data that have to be processed to provide the service, for how long the data must be stored etc. Employer A cannot have any influence

on the purpose and means of Bank B's processing of data. Bank B is therefore to be seen as a controller for this processing and the transmission of personal data from the payroll administration is to be regarded as a disclosure of information between two controllers, from Employer A to Bank B.

例:銀行支払い

雇用主Aからの指示の一部として、給与管理者は、銀行Bに情報を送付する。雇用主Aの従業員への実際の支払いを実行できるようにするためである。この活動には、銀行業務を遂行する目的で銀行Bが実行する個人データの取扱いが含まれる。この業務の範囲内で、銀行Bは、サービスを提供するために取扱う必要のあるデータ、当該データを保存しなければならない期間などを、雇用主から独立して決定する。雇用主Aは、銀行Bのデータ取扱いの目的及び手段に何らの影響も与えることはできない。したがって、銀行Bは、この取扱いにおける管理者とみなされ、給与管理者からの個人データの送付は、雇用主Aから銀行Bへの、二者の管理者間の情報の開示とみなされる。

Example: Accountants

Employer A also hires Accounting firm C to carry out audits of their bookkeeping and therefore transfers data about financial transactions (including personal data) to C. Accounting firm C processes these data without detailed instructions from A. Accounting firm C decides itself, in accordance with legal provisions regulating the tasks of the auditing activities carried out by C, that the data it collects will only be processed for the purpose of auditing A and it determines what data it needs to have, which categories of persons that need to be registered, how long the data shall be kept and what technical means to use. Under these circumstances, Accounting firm C is to be regarded as a controller of its own when performing its auditing services for A. However, this assessment may be different depending on the level of instructions from A. In a situation where the law does not lay down specific obligations for the accounting firm and the client company provides very detailed instructions on the processing, the accounting firm would indeed be acting as a processor. A distinction could be made between a situation where the processing is - in accordance with the laws regulating this profession - done as part of the accounting firm's core activity and where the processing is a more limited, ancillary task that is carried out as part of the client company's activity.

例:会計事務所

雇用主Aは、さらに、自社の帳簿監査のため会計事務所Cを雇用し、財務取引に関するデータ(個人データを含む)をCに移転する。会計事務所Cは、Aからの詳細な指示なしにこれらのデータを取り扱う。会計事務所Cは、Cが実施する監査業務の職務を規制する法規定に準拠して、収集したデータはAを監査する目的でのみ取り扱うことを自ら決定し、必要なデータ、登録する必要のある者の類型、そのデータの保存期間及び利用する技術的手段を決定する。このような状況の下では、会計事務所Cは、Aへの監査サービスの遂行において、自身の管理者とみなされる。しかしながら、この評価は、Aからの指示のレベルによって異なり得る。法律が会計事務所の具体的な義務を定めておらず、顧客企業が取扱いについて非常に詳細な指示をしている状況においては、その会計事務所は、実際に処理者として行動することとなろう。その取扱いが(この職業を規制する法律に準拠して)会計事務所の中核的業務の一部として行われる状況と、その取扱いがより限定された、顧客企業の業務の一部として実行される補助的な職務である状況は、区別することができる。

Example: Hosting services

Employer A hires hosting service H to store encrypted data on H's servers. The hosting service H does not determine whether the data it hosts are personal data nor does it process data in any other way than storing it on its servers. As storage is one example of a personal data processing activity, the hosting service H is processing personal data on employer A's behalf and is therefore a processor. Employer A must provide the necessary instructions to H and a data processing agreement according to Article 28 must be concluded, requiring H to implement technical and organisational security measures. H must assist A in ensuring that the necessary security measures are taken and notify it in case of any personal data breach.

例:ホスティング・サービス

雇用主Aは、暗号化されたデータをホスティング・サービスHのサーバーに保存するためにHを雇用する。ホスティング・サービスHは、ホスティングするデータが個人データであるかどうかを判断せず、そのサーバーに保存する以外の方法でデータを取り扱うこともしない。保存は個人データ取扱活動の一例であるため、ホスティング・サービスHは雇用主Aに代わって個人データを取扱っており、したがって処理者である。雇用主Aは、Hに対し必要な指示を与え、第28条に準拠したデータ取扱い契約を締結し、Hに技術的・組織的な安全管理措置の実施を求めなければならない。Hは、必要な安全管理措置が講じられることを確保するにあたり、Aを支援しなければならず、個人データの侵害が発生した場合には通知しなければならない。

41. Even though decisions on non-essential means can be left to the processor, the controller must still stipulate certain elements in the processor agreement, such as – in relation to the security requirement, e.g. an instruction to take all measures required pursuant to Article 32 of the GDPR. The agreement must also state that the processor shall assist the controller in ensuring compliance with, for example, Article 32. In any event, the controller remains responsible for the implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation (Article 24). In doing so, the controller must take into account the nature, scope, context and purposes of the processing as well as the risks for rights and freedoms of natural persons. For this reason, the controller must be fully informed about the means that are used so that it can take an informed decision in this regard. In order for the controller to be able to demonstrate the lawfulness of the processing, it is advisable to document at the minimum necessary technical and organisational measures in the contract or other legally binding instrument between the controller and the processor.

非本質的手段に関する決定は処理者に任せることができるが、依然として管理者は、例えば、安全管理要件に関連して、GDPRの第32条に準拠して要求されるすべての措置を講じる指示など、一定の要素を処理者契約に規定しなければならない。契約では、また、処理者が、例えば、第32条の遵守を確保する上で管理者を支援することも規定しなければならない。いずれにしても、管理者は、その取扱いがGDPR(第24条)に準拠して実行されることを確保し、かつ、証明できるための適切な技術的措置及び組織的措置の実装に引き続き責任を負う。その際、管理者は、取扱いの性質、範囲、文脈及び目的のほか、自然人の権利及び自由に対するリスクを考慮しなければならない。このため、管理者は、この点に関して情報に基づいた決定が下せるよう、利用される手段につき十分に情報提供されなければならない。管理者が取扱いの適法性を証明できるようにするため、管理者と処理者の間の契約又はその他の法的拘束力のある証書に、最低限必要な技術的措置及び組織的措置を文書化することが望ましい。

Example: Call centre

Company X decides to outsource a part of its customer service relations to a call centre. The call centre receives identifiable data about customer purchases, as well contact information. The call centre uses its own software and IT infrastructure to manage the personal data concerning Company X's customers. Company X signs a processor

agreement with the provider of the call centre in accordance with Article 28 GDPR, after determining that the technical and organisational security measures proposed by the call centre are appropriate for the risks concerned and that the call centre will only process the personal data for the purposes of Company X and in accordance with its instructions. Company X does not provide any further instructions to the call centre as to specific software to be used nor any detailed instructions regarding the specific security measures to be implemented. In this example, Company X remains a controller, despite the fact that the call centre has determined certain non-essential means of the processing.

例:コールセンター

X社は、カスタマーサービスの一部をコールセンターに委託することを決定した。コールセンターは、顧客の購入に関する特定可能なデータや連絡先情報を受け取る。コールセンターでは、独自のソフトウェアとITインフラを使用して、X社の顧客に関する個人データを管理している。X社は、コールセンターが提案する技術的・組織的な安全管理措置が当該リスクに対して適切であること、コールセンターがX社の目的のために、X社の指示に従ってのみ個人データを取扱うことを判断した上で、GDPR第28条に基づき、コールセンターのプロバイダと処理者契約を締結する。X社は、コールセンターに対して、使用するソフトウェアやセキュリティ対策に関する詳細な指示を出していない。この例では、コールセンターが取扱いの非本質的な手段を決定したにもかかわらず、X社は引き続き管理者となる。

2.1.5 "Of the processing of personal data"
「個人データの取扱いに係る」

42. The purposes and means determined by the controller must relate to the "processing of personal data". Article 4(2) GDPR defines the processing of personal data as "*any operation or set of operations which is performed on personal data or on sets of personal data*". As a result, the concept of a controller can be linked either to a single processing operation or to a set of operations. In practice, this may mean that the control exercised by a particular entity may extend to the entirety of processing at issue but may also be limited to a particular stage in the processing.[16]

[16] Judgment in *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 74: "*(A)s the Advocate General noted, [...-] it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it*

管理者が決定する目的及び手段は、「個人データの取扱い」に関連していなければならない。GDPR第4条第2項は、個人データの取扱いを*「個人データ若しくは一群の個人データに実施される業務又は一群の業務」*と定義している。その結果、管理者の概念は、単一の取扱業務又は一群の業務のいずれかにリンクされ得る。実務上は、これは、特定の主体によって実行される管理は問題の取扱いの全体に及ぶ場合があるが、取扱いにおける特定の段階に限定される場合もあることを意味する場合がある。[16]

43. In practice, the processing of personal data involving several actors may be divided into several smaller processing operations for which each actor could be considered to determine the purpose and means individually. On the other hand, a sequence or set of processing operations involving several actors may also take place for the same purpose(s), in which case it is possible that the processing involves one or more joint controllers. In other words, it is possible that at "micro-level" the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at "macro-level" these processing operations should not be considered as a "set of operations" pursuing a joint purpose using jointly defined means.

実際には、複数の関係者が関与する個人データの取扱いは、各関係者が個別に目的と手段を決定すると考えられるいくつかの小さな処理作業に分割されることがある。一方で、複数の関係者が関与する一連の処理作業が同じ目的で行われることもあり、その場合、処理には1人以上の共同管理者が関与する可能性がある。言い換えれば、「ミクロレベル」では、チェーンの異なる処理作業は、それぞれが異なる目的を持っている可能性があるため、切断されているように見える可能性がある。しかし、「マクロレベル」では、これらの処理操作が、共同で定義された手段を用いて共同の目的を追求する「一連の操作」とみなされるべきではないかどうかを再確認する必要がある。

---

determines jointly the purposes and means. By contrast, […] that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means".

*ファッションID*の判決、C-40/17, ECLI:EU:C:2019:629、第74段落:「*(A) 法務官は次のように述べている。[…-] 自然人又は法人は、指令95/46の第2条(d)の意義の範囲内で、事故が共同でその目的及び方法を決定する個人データの取り扱いを含む業務に関してのみ、他者と共同で管理者となり得る。対照的に、[…]自然人又は法人は、当該規定の意義の範囲内で、その者が目的又は方法を決定しない取扱連鎖全体に先行する又は後続する業務の文脈においては、管理者とみなされない。*」

44. Anyone who decides to process data must consider whether this includes personal data and, if so, what the obligations are according to the GDPR. An actor will be considered a “controller” even if it does not deliberately target personal data as such or has wrongfully assessed that it does not process personal data.

データを取扱うことを決定した者は誰しも、これに個人データが含まれるかどうか、そして、含まれる場合にはGDPRに準拠した義務が何であるかを検討しなければならない。行為主体は、意図的に個人データを個人データとしての対象としない場合も、個人データを取扱わないと誤って評価した場合においても、「管理者」とみなされることとなろう。

45. It is not necessary that the controller actually has access to the data that is being processed.[17] Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data.

管理者が取扱中のデータに実際にアクセスできる必要はない。[17] 取扱活動を外部委託し、その際、その取扱いの目的及び（本質的な）手段に決定的な影響を（誰の個人データが取り扱われるべきかを左右するような形でサービスのパラメータを調整することなどにより）与える者は、当該データに実際にアクセスすることは決してない場合においても、管理者とみなされることとなる。

Example: Market research 1

Company ABC wishes to understand which types of consumers are most likely to be interested in its products and contracts a service provider, XYZ, to obtain the relevant information.

Company ABC instructs XYZ on what type of information it is interested in and provides a list of questions to be asked to those participating in the market research. Company ABC receives only statistical information (e.g., identifying consumer trends per region) from XYZ and does not have access to the personal data itself.

Nevertheless, Company ABC decided that the processing should take place, the

[17] Judgment in *Wirtschaftsakademie*, C-201/16, ECLI :EU :C :2018 :388, paragraph 38.
*Wirtschaftsakademie*の判決文（C-201/16、ECLI:EU:C:2018:388）、第38段落。

processing is carried out for its purpose and its activity and it has provided XYZ with detailed instructions on what information to collect. Company ABC is therefore still to be considered a controller with respect of the processing of personal data that takes place in order to deliver the information it has requested. XYZ may only process the data for the purpose given by Company ABC and according to its detailed instructions and is therefore to be regarded as processor.

例:市場調査1

ABC社は、どの類型の消費者が自社製品に興味を持つ可能性が最も高いかを知りたいと考え、関連情報を入手するためサービス・プロバイダXYZと契約する。ABC社は、XYZに対し関心のある情報の種類を指示し、市場調査参加者に尋ねる質問のリストを提供する。

ABC社は、XYZから統計情報(地域ごとの消費者動向の識別など)のみを受け取り、個人データ自体にはアクセスしない。それにもかかわらず、ABC社は、取扱いを行うべきであると決定し、その取扱いは同社の目的及び活動のために実行され、同社は、収集する情報に関する詳細な指示をXYZに対して行った。したがって、ABC社は、同社が要求した情報の引き渡しのために行われる個人データの取扱いに関して、依然として管理者とみなされる。XYZは、ABC社から与えられた目的、及び、ABC社の詳細な指示のみに従ってデータを取り扱うことができ、したがって、処理者とみなされる。

Example: Market research 2

Company ABC wishes to understand which types of consumers are most likely to be interested in its products. Service provider XYZ is a market research agency which has collected information about consumer interests through a variety of questionnaires which pertain to a wide variety of products and services. Service provider XYZ has collected and analysed this data independently, according to its own methodology without receiving any instructions from Company ABC. To answer Company ABC's request, service provider XYZ will generate statistical information, but does so without receiving any further instructions about which personal data should be processed or how to process it in order to generate these statistics. In this example, service provider XYZ acts as the sole controller, processing personal data for market research purposes, autonomously determining the means for doing so. Company ABC does not have any particular role or responsibility under data protection law in relation to these processing activities, as Company ABC receives anonymised statistics and is not involved in determining the purposes and means of the processing.

例：市場調査2

ABC社は、どの類型の消費者が自社の製品に興味を持つ可能性が最も高いかを知りたいと考えている。サービス・プロバイダXYZは、市場調査機関であり、多種多様な製品やサービスに関する様々なアンケートを通じて、消費者の関心事に関する情報を収集している。サービス・プロバイダXYZは、ABC社からの指示を受けることなく、独自の方法でこのデータを収集し、分析している。ABC社の要求に答えるために、サービス・プロバイダXYZは、統計情報を作成するが、これらの統計情報を作成するためにどの個人データを処理すべきか、どのように処理するかについての追加の指示を受けることなく行う。この例では、サービス・プロバイダXYZが唯一の管理者として、市場調査の目的で個人データを処理し、そのための手段を自律的に決定している。会社ABCは、匿名化された統計を受け取り、処理の目的と手段の決定に関与していないため、これらの処理活動に関連して、データ保護法の下で特定の役割や責任を負わない。

3. DEFINITION OF JOINT CONTROLLERS

共同管理者の定義

3.1 Definition of joint controllers

共同管理者の定義

46. The qualification as joint controllers may arise where more than one actor is involved in the processing.

共同管理者としての適格性は、複数の行為主体が取扱いに関与している場合に発生する場合がある。

47. While the concept is not new and already existed under Directive 95/46/EC, the GDPR, in its Article 26, introduces specific rules for joint controllers and sets a framework to govern their relationship. In addition, the Court of Justice of the European Union (CJEU) in recent rulings has brought clarifications on this concept and its implications.[18]

[18] See in particular, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (C-40/17). To be noted that while these judgments were issued by the CJEU on the interpretation of the concept of joint controllers under Directive 95/46/CE, they remain valid in the

この概念は新しいものではなく、指令95/46/ECの下ですでに存在しているが、GDPRは、第26条において、共同管理者に関する具体的なルールを導入し、それらの関係を規律するための枠組みを設定している。さらに、欧州連合司法裁判所（CJEU）は、最近の判決において、この概念及びその含意について明確にした。[18]

48. As further elaborated in Part II, section 2, the qualification of joint controllers will mainly have consequences in terms of allocation of obligations for compliance with data protection rules and in particular with respect to the rights of individuals.

第2部のセクション2においてさらに詳しく説明されているように、共同管理者としての適格性は、主として、データ保護規則の遵守義務の割り当てに関し、特に個人の権利に関して影響をもたらす。

49. In this perspective, the following section aims to provide guidance on the concept of joint controllers in accordance with the GDPR and the CJEU case law to assist entities in determining where they may be acting as joint controllers and applying the concept in practice.

この観点から、次のセクションは、共同管理者として行動し実務上その概念を適用できる状況の見極めにあたって主体を支援するべく、GDPR及びCJEUの判例法に準拠した共同管理者の概念に関するガイダンスを提供することを目的としている。

3.2 Existence of joint controllership
共同管理の存在

3.2.1 General considerations
一般的考察

50. The definition of a controller in Article 4 (7) GDPR forms the starting point for determining joint controllership. The considerations in this section are thus directly related to and supplement the considerations in the section on the concept of controller. As a consequence, the assessment of joint controllership should mirror

---

context of the GDPR, given that the elements determining this concept under the GDPR remain the same as under the Directive.

特に、*UnabhängigesLandeszentrum für Datenschutz Schleswig-Holstein対Wirtschaftsakademie*、(C-210/16)、*Tietosuojavaltuutettu対Jehovan todistajat – uskonnollinen yhdyskunta*(C-25/17)、*Fashion ID GmbH & Co.KG対Verbraucherzentrale NRW eV*(C-40/17)を参照。これらの判断判決文は、指令95/46/CEに基づく共同管理者の概念の解釈に関してCJUEUによって発布下されたが、GDPRの下でのこの概念を決定する要素が指令の下でのそれと同様であるという前提において、GDPRの文脈で引き続き有効であることに留意されたい。

the assessment of "single" control developed above.

GDPR第4条第7項における管理者の定義は、共同管理者を決定するための出発点を形成する。したがって、このセクションにおける考察は、管理者の概念に関するセクションの考察に直接関連し、これを補足する。結果として、共同管理の評価は、前述で展開された「単一の」管理の評価を反映すべきこととなる。

51. Article 26 GDPR, which reflects the definition in Article 4 (7) GDPR, provides that *"[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."* In broad terms, joint controllership exists with regard to a specific processing activity when different parties determine *jointly* the purpose and means of this processing activity. Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party. "Jointly" must be interpreted as meaning "together with" or "not alone", in different forms and combinations, as explained below.

GDPR第4条第7項の定義を反映するGDPR第26条は、「*二者以上の管理者が共同して取扱いの目的及び手段を決定する場合、それらの者は共同管理者となる*」と規定している。広い意味では、共同管理は、具体的な取扱活動に関して様々な当事者が*共同*でこの取扱いの目的及び手段を決定する状況において共同管理存在する。したがって、共同管理者の存在を評価するには、管理者を特徴付ける目的及び手段の決定が複数の当事者によって決定されているかどうかを調べることが要求される。「共同で」は、以下で説明するように、様々な形態及び組み合わせにおいて、「と共に」又は「単独でなく」を意味すると解釈されなければならない。

52. The assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing. All existing or envisaged arrangements should be checked against the factual circumstances regarding the relationship between the parties. A merely formal criterion would not be sufficient for at least two reasons: in some cases, the formal appointment of a joint controller - laid down for example by law or in a contract - would be absent; in other cases, it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing.

共同管理の評価は、取扱いの目的及び手段に対する実際の影響について、形式的な分析ではなく、事実に基づく分析に基づき実行されるべきである。既存の取決め又は想定されるすべての取決めは、当事者間の関係に関する事実に基づく状況と照合されるべきである。単なる形式的な基準では不十分であろうことの理由として、次のとおり少なくとも次の二点が挙げられる。まず、法律または契約書などにより定められる共同管理者の正式な任命がない場合があろう。また、別の場合には、取扱いの目的及び手段を実際に「決定」する立場にない主体に管理者の役割を形式的に委託するという、形式的な任命が取決めの現実を反映していない場合があり得るためである。

53. Not all processing involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the **joint participation of two or more entities in the determination of the purposes and means** of a processing. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.

複数の主体が関与するすべての取扱いが共同管理を生じさせるわけではない。共同管理が存在するための包括的な基準は、取扱いの**目的及び手段の決定において二者以上の主体が共同参加すること**である。より具体的には、共同参加には、一方で目的の決定が、他方で手段の決定が含まれる必要がある。これらの要素のそれぞれが、関係するすべての主体によって決定される場合、彼らは問題の取扱いの共同管理者とみなされるべきである。

3.2.2 Assessment of joint participation
共同参加の評価

54. Joint participation in the determination of purposes and means implies that more than one entity have a decisive influence over whether and how the processing takes place. In practice, joint participation can take several different forms. For example, joint participation can take the form of a **common decision** taken by two or more entities or result from **converging decisions** by two or more entities regarding the purposes and essential means.

目的及び手段の決定における共同参加は、複数の主体が、取扱いが行われるかどうか、及び、どのように行われるかにつき決定的な影響を与えることを意味している。実務的には、共同参加はいくつかの異なる形態をとることができる。例えば、共同参加は、二者以上の

主体による**共同決定**の形態をとることができるし、目的及び本質的手段に関しての、二者以上の主体による**相互補完的決定**の結果生じる場合もある。

55. Joint participation through a *common decision* means deciding together and involves a common intention in accordance with the most common understanding of the term "jointly" referred to in Article 26 of the GDPR.

The situation of joint participation through *converging decisions* results more particularly from the case law of the CJEU on the concept of joint controllers. Decisions can be considered as converging on purposes and means **if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing.** As such, an important criterion to identify converging decisions in this context is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. It should be highlighted that the notion of converging decisions needs to be considered in relation to the purposes and means of the processing but not other aspects of the commercial relationship between the parties.[19] As such, an important criterion to identify converging decisions in this context **is whether the processing would not be possible without both parties' participation in the purposes and means in the sense that the processing by each party is inseparable, i.e. inextricably linked.** The situation of joint controllers acting on the basis of converging decisions should however be distinguished from the case of a processor, since the latter – while participating in the performance of a processing – does not process the data for its own purposes but carries out the processing on behalf of the controller.

共同決定による共同参加とは、共同で決定することを意味し、GDPRの第26条で定められている「共同で」という用語の最も一般的な理解に従った*共通の意図*を伴う。

決定が目的と手段に対して収束すると考えられるのは、**決定が互いに補完し合い、処理の目的と手段の決定に具体的な影響を与えるような方法で処理が行われるために必要である場合**である。そのため、この文脈で収束する決定を識別するための重要な基準は、各

[19] Indeed, all commercial arrangements involve converging decisions as part of the process by which an agreement is reached.

実際、すべての商業上の契約は、合意に至るまでのプロセスの一部として、収束する決定を伴う。

当事者による処理が不可分であるという意味で、両当事者の参加なしには処理が不可能であるかどうかということである（すなわち、密接に関連しています）。相互補完的決定という概念は、取扱いの目的と手段に関連して考慮される必要があるが、当事者間の商業関係の他の側面は考慮されないことを強調しておく。[19] そのため、この文脈で収束する決定を特定するための重要な基準は、**各当事者による処理が不可分であるという意味で、両当事者が目的と手段に参加しなければ処理が不可能であるかどうか、すなわち密接に関連しているかどうかある**。しかし、相互補完的決定に基づいて行動する共同管理者の状況は、処理者の場合とは区別する必要がある。というのも、処理者は、処理の実行に参加しているものの、自らの目的のためにデータを処理するのではなく、管理者に代わって処理を実行するからである。

56. The fact that one of the parties does not have access to personal data processed is not sufficient to exclude joint controllership.[20] For example, in *Jehovah's Witnesses*, the CJEU considered that a religious community must be considered a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching.[21] The CJEU considered that it was not necessary that the community had access to the data in question, or to establish that that community had given its members written guidelines or instructions in relation to the data processing.[22] The community participated in the determination of purposes and means by organising and coordinating the activities of its members, which helped to achieve the objective of the Jehovah's Witnesses community.[23] In addition, the community had knowledge on a general level of the fact that such processing was carried out in order to spread its faith.[24]

当事者のうちの一者が取扱われた個人データにアクセスを有しないという事実は、共同管理を排除するには十分ではない。[20] 例えば、「*Jehovah's Witnesses*」では、CJEUは、宗教団体は、説教に従事するメンバーと共同で、個別訪問による説教の文脈で後者によ

[20] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 38.
*Wirtschaftsakademie事件*の判決文（C-210/16、ECLI:EU:C:2018:388）、第38段落。
[21] *Judgment in Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75.
*Jehovah's witnesses事件*の判決文（C-25/17、ECLI:EU:C:2018:551）、第75段落。
[22] Ibid.
同上。
[23] Ibid, paragraph 71.
同上、第71段落。
[24] Ibid.
同上。

って実行される個人データの取扱いの管理者とみなされなければならないと考えた。[21] CJEUは、当該団体が問題のデータにアクセスする必要はなく、当該団体がデータの取扱いに関連してメンバーに書面によるガイドライン又は指示を与えたことを立証する必要もないと考えた。[22] 当該団体は、メンバーの活動を組織化し調整することにより、目的及び手段の決定に参加し、これが、「Jehovah's Witnesses」の団体の目的を達成するのに役立った。[23] さらに、当該団体は、その信仰を広めるためにそのような取扱いが行われたという事実について一般的な水準における知識を持っていた。[24]

57. It is also important to underline, as clarified by the CJEU, that an entity will be considered as joint controller with the other(s) only in respect of those operations for which it determines, jointly with others, the means and the purposes of the same data processing in particular in case of converging decisions. If one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operation.[25]

また、CJEUによって明確にされているように、主体が、他の主体と共同で同一の取扱いの手段及び目的を決定する業務に関してのみ、特に決定されている場合には、その主体が他の主体との共同管理者とみなされることを強調することも重要である。これらの主体の一つが、取扱いの連鎖において先行する(又は後続する)業務の目的及び手段を単独で決定する場合、この主体は、この先行する(又は後続する)業務における唯一の管理者とみなされなければならない。[25]

58. The existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, the CJEU has clarified that those operators may be involved at different stages of that processing and to different degrees so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.

共同責任の存在は、必ずしも個人データの取扱いに関与する様々な行為者の同等の

[25] Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 74 "*By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means*".
*Fashion ID事件*の判決文(C-40/17, ECLI:EU:2018:1039)、第74段落「*対照的に、この点に関して国内法で規定されている民事責任に影響を与えることなく、当該自然人又は法人は当該規定の意義の範囲内で、その者が目的又は手段を決定しない取扱連鎖全体に先行する(又は後続する)業務の文脈においては、管理者であると見なされることはできない。*」

責任を意味するものではない。むしろ、CJEUは、これらの行為者は当該取扱いにおける様々な段階及び様々な程度に関与し得るため、個々の行為者の責任のレベルは、特定の事案における全ての関連する状況に関して評価されなければならないことを明確にしている。

3.2.2.1 Jointly determined purpose(s)
共同で決定された目的

59. Joint controllership exists when entities involved in the same processing carry out the processing for jointly defined purposes. This will be the case if the entities involved process the data for the same, or common, purposes.

共同管理は、同一の取扱業務に関与する主体が共同で定義した目的で取扱うときに存在する。これは、関係する主体が同一又は共通の目的でデータを取扱う場合に当てはまる。

60. In addition, when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved pursue purposes which are closely linked or complementary. Such may be the case, for example, when there is a mutual benefit arising from the same processing operation, provided that each of the entities involved participates in the determination of the purposes and means of the relevant processing operation. However, the notion of mutual benefit is not decisive and can only be an indication. In *Fashion ID*, for example, the CJEU clarified that a website operator participates in the determination of the purposes (and means) of the processing by embedding a social plug-in on a website in order to optimize the publicity of its goods by making them more visible on the social network. The CJEU considered that the processing operations at issue were performed in the economic interests of both the website operator and the provider of the social plug-in.[26]

さらに、主体が取扱いに対する同一の目的を持っていない場合でも、共同管理は、CJEU判例法に照らせば、関係する主体が密接に関連する又は補完する目的を追求するときに確立し得る。これは、例えば、関係する個々の主体が関連する取扱業務の目的及び手段の決定に参加する場合で、同一の取扱業務から生じる相互利益がある場合に当てはまるであろう。しかし、相互利益という概念は決定的なものではなく、あくまでも目安にし

[26] Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 80.
*Fashion ID事件*の判決文(C-40/17, ECLI:EU:2018:1039)、第80段落。

か過ぎない。例えば、*Fashion ID事件*では、CJEUは、ウェブサイトの運営者が、ソーシャル・ネットワーク上で商品をより目立たせることによって商品の宣伝を最適化するためソーシャル・プラグインをウェブサイトに埋め込むことにより、取扱いの目的（及び手段）の決定に参加していることを明確にした。CJEUは、問題の取扱業務は、ウェブサイト運営者とソーシャル・プラグインのプロバイダ双方の経済的利益のために遂行されたと考えた。[26]

61. Likewise, as noted by the CJEU in *Wirtschaftsakademie*, the processing of personal data through statistics of visitors to a fan page is intended to enable Facebook to improve its system of advertising transmitted via its network and to enable the administrator of the fan page to obtain statistics to manage the promotion of its activity.[27] Each entity in this case pursues its own interest but both parties participate in the determination of the purposes (and means) of the processing of personal data as regards the visitors to the fan page.[28]

同様に、CJEUが*Wirtschaftsakademie事件*において指摘しているように、ファン・ページへの訪問者の統計を介した個人データの取扱いは、Facebookがそのネットワーク経由で送信する広告システムを改善できるようにすること、及びファン・ページの管理者がその活動の促進を管理するために統計を取得できるようにすることを目的としている。[27] この場合、個々の主体が自己の利益を追求するが、両当事者は、ファン・ページへの訪問者に関する個人データの取扱いの目的（及び手段）の決定に参加する。[28]

62. In this respect, it is important to highlight that the mere existence of a mutual benefit (for ex. commercial) arising from a processing activity does not give rise to joint controllership. If the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, but is merely being paid for services rendered, it is acting as a processor rather than as a joint controller.

この点で、取扱活動から生じる相互利益（例えば商業的利益）が単に存在するというだけでは、共同管理を生じさせるものではないことを強調することが重要である。取扱いに関与する主体が、取扱活動に関連して自己の目的を追求せず、提供したサービスに対して単に支払を受けるのみである場合には、当該主体は共同管理者としてではなく、むしろ処理者として行動している。

[27] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 34.
*Wirtschaftsakademie事件*の判決文（C-210/16、ECLI:EU:C:2018:388）、第34段落。
[28] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 39.
*Wirtschaftsakademie事件*の判決文（C-210/16、ECLI:EU:C:2018:388）、第39段落。

3.2.2.2 Jointly determined means
共同で決定された手段

63. Joint controllership also requires that two or more entities have exerted influence over the means of the processing. This does not mean that, for joint controllership to exist, each entity involved needs in all cases to determine all of the means. Indeed, as clarified by the CJEU, different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so.

共同管理には、さらに、二者以上の主体が取扱いの方法に影響を及ぼしていることが要求される。これは、共同管理が存在するためには、関係する個々の主体が全ての場合において全ての手段決定する必要があることを意味するものではない。実際、CJEUによって明確にされているように、様々な主体がその取扱いの様々な段階において、様々な程度に関与している場合がある。したがって、様々な共同管理者は、誰が事実上そうする立場にあるかに応じて、様々な程度に取扱いの手段を決定することができる。

64. It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.

関係する主体のうちの一者が取扱いの手段を提供し、他の主体による個人データの取扱活動に利用できるようにする場合もあり得る。個人データを特定の目的で取扱えるようにこれらの手段を利用することを決定する主体も、取扱いの手段の決定に参加する。

65. This scenario can notably arise in case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up.[29] The use of an already existing technical system does not

[29] The provider of the system can be a joint controller if the criteria mentioned above are met, i.e. if the provider participates in the determination of purposes and means. Otherwise, the provider should be considered as a processor.
システムのプロバイダーは、上記の基準が満たされる場合、すなわち、プロバイダーが目的及び手段の決定に参加する場合に、共同管理者となり得る。それ以外の場合は、プロバイダーは処理者と見なされるべきである。

exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context.

このシナリオは、当事者が同じ個人データを処理することを可能にするプラットフォーム、標準化されたツール、またはその他のインフラを、当事者の一方が一定の方法で設定し、その設定方法を決定できる他の当事者が使用できるようになっている場合に特に生じる可能性がある。[29] 既存の技術システムのユーザーが、この文脈で実行される個人データの取扱いについて決定できる場合、当該システムの利用によって共同管理は排除されない。

66. As an example of this, the CJEU held in *Wirtschaftsakademie* that the administrator of a fan page hosted on Facebook, by defining parameters based on its target audience and the objectives of managing and promoting its activities, must be regarded as taking part in the determination of the means of the processing of personal data related to the visitors of its fan page.

この一例として、CJEUは、*Wirtschaftsakademie 事件*において、Facebookがホスティングしているファン・ページの管理者が、その想定対象者（ターゲット・オーディエンス）及びその活動を管理・促進する目的に基づいてパラメータを定義することにより、そのファン・ページの訪問者に関連する個人データの取扱手段の決定に参加しているとみなされなければならないとした。

67. Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities. This follows from the Fashion ID case where the CJEU concluded, that by embedding on its website the Facebook Like button made available by Facebook to website operators, Fashion ID has exerted a decisive influence in respect of the operations involving the collection and transmission of the personal data of the visitors of its website to Facebook and had thus jointly determined with Facebook the means of that processing.[30]

さらに、ある主体が、別の主体によって開発された個人データの取扱いを可能にするツール又は他のシステムを、自らの目的のために利用するという選択は、それらの主体による当該取扱いの手段に関する共同決定になる可能性が高い。これは、CJEUが、Facebookがウェブサイト運営者に提供するFacebookのいいね！ボタンをウェブサイトに

[30] Judgment in Fashion ID, C-40/17, ECLI:EU:2018:1039, paragraphs 77-79.
Fashion ID事件の判決文（C-40/17、ECLI:EU:2018:1039）、第77-79段落。

埋め込むことにより、Fashion IDはそのウェブサイトの訪問者の個人データの収集及びFacebookへの送信を含む業務に関して決定的な影響を及ぼしており、したがって、当該取扱いの手段をFacebookと共同で決定していたと結論付けたFashion IDの事件から導かれる。[30]

68. It is important to underline that the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing).

共通のデータ取扱システム又はインフラの利用が、すべての場合において、関係する当事者の共同管理者としての適格性に繋がるわけではないこと(とりわけ、彼らが実行する取扱いが分離可能であり、他の当事者の介入なしに一方の当事者によって実行が可能な場合、又は、プロバイダが自己の目的がない場合の処理者である場合において。)を強調することは重要である。(関係する当事者に単に商業的利益があるというだけでは、取扱いの目的として適格となるのに十分ではない。)

Example: Travel agency

A travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the travel agency, the airline and the hotel are three different data controllers processing the data for their own and separate purposes and there is no joint controllership.

The travel agency, the hotel chain and the airline then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their

respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internet- based common platform.

例:旅行代理店

旅行代理店は、旅行パッケージの予約を目的として、顧客の個人データを航空会社及びホテルチェーンに送付する。航空会社及びホテルは、依頼された座席及び部屋の空き状況を確認する。旅行代理店は、顧客に旅行の書類及び証票を発行する。 個々の行為主体は、自身の活動を実行し、自身の手段を利用するためにそのデータを取り扱う。この場合、旅行代理店、航空会社及びホテルは、それぞれの目的でデータを取り扱う異なる三者のデータ管理者であり、ここには共同管理は存在しない。

旅行代理店、ホテルチェーン及び航空会社は、次に、パッケージ旅行の取引を提供するという共通の目的で、インターネットベースの共通プラットフォームの構築に共同で参加することを決定する。彼らは、どのデータが保存されるか、予約がどのように割り当てられ確認されるか、そして、誰が保存された情報にアクセスできるかなど、利用される本質的手段について合意する。さらに、彼らは、共同マーケティング活動を実行するため、顧客のデータを共有することを決定する。この場合、旅行代理店、航空会社及びホテルチェーンは、それぞれの顧客の個人データが取り扱われる理由及び方法を共同で決定するため、共通のインターネットベースの予約プラットフォームに関連する取扱業務及び共同マーケティング活動に関して共同管理者となる。ただし、それぞれは、インターネットベースの共通プラットフォーム以外の他の取扱活動に関しては、依然として単独の管理を保持する。

Example: Research project by institutes

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

例：研究機関による研究プロジェクト

複数の研究機関が、特定の共同研究プロジェクトへ参加すること及び、プロジェクトに関与する機関のうちの一つが有する既存のプラットフォームをそのために利用することを決定する。個々の機関は、自己が既に保有する個人データを共同研究の目的のためにプラットフォームに入力し、プラットフォームを通じて他の研究機関から提供されたデータを、研究を遂行するために利用する。この場合、すべての研究機関は、共同して取扱いの目的及び利用手段（既存のプラットフォーム）を決定していることから、このプラットフォームからの情報の保存及び開示によって行われる個人データの取扱いに関して、共同管理者として適格である。しかしながら、個々の研究機関は、それぞれの目的で当該プラットフォームの外で実行される他の取扱いについては、個別の管理者である。

Example: Marketing operation

Companies A and B have launched a co-branded product C and wish to organise an event to promote this product. To that end, they decide to share data from their respective clients and prospects database and decide on the list of invitees to the event on this basis. They also agree on the modalities for sending the invitations to the event, how to collect feedback during the event and follow-up marketing actions. Companies A and B can be considered as joint controllers for the processing of personal data related to the organisation of the promotional event as they decide together on the jointly defined purpose and essential means of the data processing in this context.

例：マーケティング業務

A社とB社は共同ブランドの製品Cを発売しており、この製品を宣伝するイベントを開催したいと考えている。そのため、両者はそれぞれの顧客及び見込顧客のデータベースのデータを共有することを決定し、これに基づいてイベントへの招待者のリストを決定した。彼らは、また、イベントへの招待状を送付する方法、イベント中にフィードバックを収集する方法及びフォローアップ・マーケティング活動についても合意する。A社とB社は、この文脈において共同で定義した目的及び本質的手段を共に決定することから、促進イベントの開催に関連する個人データの取扱いに関し、共同管理者とみなされ得る。

Example: Clinical Trials[31]

[31] The EDPB plans to provide further guidance in relation to clinical trials in the context of its forthcoming

A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.

例:臨床試験[31]

医療提供者(治験責任医師)及び大学(治験依頼者)は、同一の目的で共に臨床試験を開始することを決定する。彼らは、研究プロトコル(すなわち、研究の目的、方法論/設計、収集されるデータ、被験者の除外/包含の基準、データベースの再利用(関連する場合)など)の起草において協働する。彼らは、取扱いに関する同一の目的及び本質的手段を共同で決定し合意することから、この臨床試験に関し共同管理者とみなされ得る。研究を目的とした患者の医療記録からの個人データの収集は、同一のデータの患者治療を目的とした保存及び利用とは区別されることとなり、この場合医療提供者は依然として管理者である。
治験責任医師がプロトコルの起草に参加せず(治験責任医師は治験依頼者により作成済みであるプロトコルを受け入れるのみであり)、プロトコルが治験依頼者によってのみ設計される場合、この臨床試験に関し、治験責任医師は処理者、治験依頼者は管理者とみなされるべきである。

Example: Headhunters

Company X helps Company Y in recruiting new staff- with its famous value-added service "global matchz". Company X looks for suitable candidates both among the CVs received directly by Company Y and those it already has in its own database. Such database is created and managed by Company X on its own. This ensures that Company X enhances the matching between job offers and job seekers, thus increasing its revenues. Even though they have not formally taken a decision together, Companies X and Y jointly participate to the processing with the purpose of finding suitable

Guidelines on processing of personal data for medical and scientific research purposes.
EDPBは、医療および科学研究目的のための個人データの処理に関するガイドラインに沿って、近日中に臨床試験に関連したさらなるガイダンスを提供する予定である。

candidates based on converging decisions: the decision to create and manage the service “global matchz” for Company X and the decision of Company Y to enrich the database with the CVs it directly receives. Such decisions complement each other, are inseparable and necessary for the processing of finding suitable candidates to take place. Therefore, in this particular case they should be considered as joint controllers of such processing. However, Company X is the sole controller of the processing necessary to manage its database and Company Y is the sole controller of the subsequent hiring processing for its own purpose (organisation of interviews, conclusion of the contract and management of HR data).

例：ヘッドハンター

X社は、自社の有名な付加価値サービスである「グローバルマッチ」で、Y社の新しいスタッフの採用を支援する。X社は、Y社が直接受け取った職務経歴書及び自社のデータベースにすでに存在する職務経歴書の双方から適切な候補者を探す。このようなデータベースは、X社が独自に作成及び管理している。これにより、X社は確実に求人と求職者のマッチングを促進し、収益を増やすことができる。X社とY社は、正式には共に決定はしていないが、彼らは、相互補完的決定（X社にとっての「グローバルマッチ」サービスを作成及び管理する決定並びにY社にとっての、自社が直接受け取った職務経歴書でデータベースを充実させる決定）に基づき適切な候補者を見つける目的で、共同してその取扱いに参加する。このような決定は互いに補完し合うものであり、分離不可能であり、適切な候補者を見つける取扱いが発生する為に必要である。したがって、この特定の事案では、彼らはそのような取扱いにおける共同管理者とみなされるべきである。しかしながら、X社はそのデータベースの管理に必要な取扱いにおける唯一の管理者であり、Y社は自己の目的でのその後の採用の取扱い（面接の設定、契約の締結及び人材データの管理）における唯一の管理者である。

Example: Analysis of health data

Company ABC, the developer of a blood pressure monitoring app and Company XYZ, a provider of apps for medical professionals, both wish to examine how blood pressure changes can help predict certain diseases. The companies decide to set up a joint project and reach out to Hospital DEF to become involved as well.

The personal data that will be processed in this project consists of personal data which Company ABC, Hospital DEF and Company XYZ are separately processing as individual controllers. The decision to process this data to assess blood pressure changes is taken jointly by the three actors. Company ABC, Hospital DEF and Company

XYZ have jointly determined the purposes of processing. Company XYZ takes the initiative to propose the essential means of processing. Both Company ABC and the Hospital DEF accept these essential means after they as well were involved in developing some of the features of the app so that the results can be sufficiently used by them. The three organizations thus agree on having a common purpose for the processing which is the assessment of how blood pressure changes can help predict certain diseases. Once the research is completed, Company ABC, Hospital DEF and Company XYZ may benefit from the assessment by using its results in their own activities. For all these reasons, they qualify as joint controllers for this specific joint processing.

If Company XYZ had been simply asked by the others to perform this assessment without having any purpose of their own and merely been processing data on behalf of the others, Company XYZ would qualify as a processor even if it was entrusted with the determination of the non-essential means.

例:健康データの分析

血圧計アプリを開発しているABC社と、医療関係者向けアプリを提供しているXYZ社は、血圧変動が特定の病気の予測にどのように役立つかを調べたいと考えている。両社は共同でプロジェクトを立ち上げ、DEF病院にも参加を呼びかけてみることにした。

このプロジェクトで取扱われる個人データは、ABC社、DEF病院、XYZ社が個々の管理者として個別に取扱う個人データで構成されている。血圧変動を評価するためにデータを取扱う決定は、3つの関係者によって共同で行われる。ABC社、DEF病院、XYZ社は共同で取扱いの目的を決定した。XYZ社は、取扱いの必須手段を率先して提案する。ABC社とDEF病院は、結果を十分に利用できるようにアプリの一部機能の開発に携わった後、これらの必須手段を受け入れる。このようにして、3つの組織は、血圧変動が特定の病気を予測するのに役立つかどうかを評価するという、取扱いの共通の目的を持つことに同意する。研究が完了すると、ABC社、DEF病院、XYZ社は、自分たちの活動にその結果を利用することで、評価から利益を得ることができる。これらの理由により、これらの企業は、特定の共同処理について共同管理者としての資格がある。

仮に、XYZ社が他の企業から、独自の目的を持たずに単にこの評価を行うように依頼され、他の企業に代わってデータを取扱っていたら、たとえ非本質的な手段の決定を委託されていたとしても、XYZ社は処理者としての資格を有することになる。

3.2.3 Situations where there is no joint controllership

共同管理が存在しない状況

69. The fact that several actors are involved in the same processing does not mean that they are necessarily acting as joint controllers of such processing. Not all kind of partnerships, cooperation or collaboration imply qualification of joint controllers as such qualification requires a case-by-case analysis of each processing at stake and the precise role of each entity with respect to each processing. The cases below provide non-exhaustive examples of situations where there is no joint controllership.

複数の行為主体が同一の取扱いに関与しているという事実は、彼らが必ずしもそのような取扱いの共同管理者としてとして行動していることを意味するわけではない。共同管理者としての適格性には、問題とされる個々の取扱いの分析、及び、個々の取扱いに関する個々の主体の正確な役割のケースバイケースによる分析が求められることから、すべての種類のパートナーシップ、協力又は協働が共同管理者としての適格性を意味するわけではない。以下の複数のケースは、共同管理が存在しない状況の非網羅的な例を提供するものである。

70. For example, the exchange of the same data or set of data between two entities without jointly determined purposes or jointly determined means of processing should be considered as a transmission of data between separate controllers.

例えば、共同で決定された目的又は共同で決定された取扱手段なしに二者の主体間で同一のデータ又はデータセットを交換することは、別々の管理者間でのデータの送信とみなされるべきである。

Example: Transmission of employee data to tax authorities

A company collects and processes personal data of its employees with the purpose of managing salaries, health insurances, etc. A law imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control.

In this case, even though both the company and the tax authorities process the same data concerning salaries, the lack of jointly determined purposes and means with regard to this data processing will result in qualifying the two entities as two separate data controllers.

例:従業員データの税務当局への送信

ある会社は、給与や健康保険などの管理を目的として、従業員の個人データを収集し、取り扱う。法律により、同社には、財政管理を強化する目的で、給与に関するすべてのデータを税務当局に送付する義務が課されている。
この場合、同社と税務当局の双方は給与に関する同一のデータを取り扱うが、このデータの取扱いに関して共同で決定された目的及び方法が存在しないため、二者の主体は二つの別個のデータ管理者としての適格性を有することとなる。

71. Joint controllership may also be excluded in a situation where several entities use a shared database or a common infrastructure, if each entity independently determines its own purposes.

共同管理は、個々の主体が自己の目的を単独で決定する場合、複数の主体が共有データベース又は共通のインフラを利用する状況においても、排除され得る。

Example: Marketing operations in a group of companies using a shared database
A group of companies uses the same database for the management of clients and prospects. Such database is hosted on the servers of the mother company who is therefore a processor of the companies with respect to the storage of the data. Each entity of the group enters the data of its own clients and prospects and processes such data for its own purposes only. Also, each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data. They cannot access or use each other's data. The mere fact that these companies use a shared group database does not as such entail joint controllership. Under these circumstances, each company is thus a separate controller.

例:共有データベースを利用する企業グループのマーケティング業務
ある企業グループは、顧客及び見込顧客の管理に同一のデータベースを利用する。このようなデータベースは、データの保存に関して企業グループの処理者である親会社のサーバーでホストされる。企業グループの個々の主体は、自己の顧客及び見込顧客のデータを入力し、自己の目的でのみ当該データを取り扱う。また、個々の主体は、それぞれの顧客及び見込顧客のデータへのアクセス、保存期間、訂正又は削除につき独立して決定する。個々の主体はお互いのデータにアクセス又は利用することはできない。これらの企業が共有グループ・データベースを利用しているという事実だけでは、共同管理が存在するということにならない。したがって、このような状況においては、個々の企業は個別の管理者である。

Example: Independent controllers when using a shared infrastructure

Company XYZ hosts a database and makes it available to other companies to process and host personal data about their employees. Company XYZ is a processor in relation to the processing and storage of other companies' employees as these operations are performed on behalf and according to the instructions of these other companies. In addition, the other companies process the data without any involvement from Company XYZ and for purposes which are not in any way shared by Company XYZ.

例:共有インフラを利用する場合の独立した管理者

XYZ社はデータベースをホスティングし、他の複数の企業がこのデータベースを利用して各企業の従業員に関する個人データの取扱い及びホスティングをできるようにしている。XYZ社は、他の企業の従業員の取扱い及び保存がこれらの他の企業に代わり、彼らの指示に従って行われるため、これらの業務に関して処理者である。さらに、他の企業は、XYZ社に関与されることなく、また、XYZ社と全く共有することのない目的でデータを取り扱う。

72. Also, there can be situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain. In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of operations, joint controllership has to be excluded and the various actors must be regarded as successive independent controllers.

また、様々な行為主体が一連の業務において同一の個人データを連続して取り扱い、個々の行為主体は一連の業務におけるそれぞれの部分で独立した目的及び手段を有する場合があり得る。同一の取扱業務又は一連の業務の目的及び手段の決定に共同参加しない場合は、共同管理は排除されなければならず、様々な行為主体は連続する独立した管理者とみなされなければならない。

Example: Statistical analysis for a task of public interest

A public authority (Authority A) has the legal task of making relevant analysis and statistics on how the country's employment rate develops. To do that, many other public entities are legally bound to disclose specific data to Authority A. Authority A decides to use a specific system to process the data, including collection. This also means that the other units are obligated to use the system for their disclosure of data. In this case, without prejudice to any attribution of roles by law, Authority A will be the only controller

of the processing for the purpose of analysis and statistics of the employment rate processed in the system, because Authority A determines the purpose for the processing, and has decided how the processing will be organised. Of course, the other public entities, as controllers for their own processing activities, are responsible for ensuring the accuracy of the data they previously processed, which they then disclose to Authority A.

例：公共性の高いタスクのための統計分析

公的機関（公的機関A）は、国の雇用率がどのように推移するかに関し、関連する分析及び統計を行う法的職務を有する。そのためには、他の多くの公的事業体は、特定のデータを公的機関Aに開示することを法的に義務付けられている。公的機関Aは、収集を含むデータ取扱いを目的として特定のシステムを利用することを決定する。これは、他の部署がデータの開示にこのシステムを利用することを義務付けられることも意味する。この場合、法律による役割の帰属に影響を与えることなく、公的機関Aは、このシステムにおいて取扱われる雇用率の分析及び統計を目的とした取扱いにおける唯一の管理者となる。その理由は、公的機関Aは、その取扱いの目的を決定し、その取扱いをどのように構成するかを決定したためである。もちろん、他の公的事業体には、自己の取扱活動の管理者として、彼らが以前に取扱い（そのうえで彼らが公共機関Aに開示することとなる）データの正確性を確保する責任がある。

4. DEFINITION OF PROCESSOR

処理者の定義

73. A processor is defined in Article 4 (8) as a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Similar to the definition of controller, the definition of processor envisages a broad range of actors - it can be "*a natural or legal person, public authority, agency or other body*". This means that there is in principle no limitation as to which type of actor might assume the role of a processor. It might be an organisation, but it might also be an individual.

処理者は、第4条第8項において、管理者に代わって個人データを取り扱う自然人又は法人、公的機関、部局又はその他の組織と定義されている。管理者の定義と同様に、処理者の定義は、幅広い行為主体を想定している。それは、「*自然人又は法人、公的機関、部局又はその他の組織*」であり得る。これは、原則として、どの種類の行為主体が処理者

の役割を引き受けるかについて制限がないことを意味する。それは組織かもしれないし、個人かもしれない。

74. The GDPR lays down obligations directly applicable specifically to processors as further specified in Part II section 1 of these guidelines. A processor can be held liable or fined in case of failure to comply with such obligations or in case it acts outside or contrary to the lawful instructions of the controller.

GDPRは、本ガイドラインの第2部のセクション1でさらに特定されているように、特に処理者に直接適用される義務を定めている。処理者は、そのような義務を遵守しなかった場合、又は管理者の適法な指示以外で又はそれに反して行動した場合、責任を問われるか又は制裁金を課せられる可能性がある。

75. Processing of personal data can involve multiple processors. For example, a controller may itself choose to directly engage multiple processors, by involving different processors at separate stages of the processing (multiple processors). A controller might also decide to engage one processor, who in turn - with the authorisation of the controller - engages one or more other processors ("sub processor(s)"). The processing activity entrusted to the processor may be limited to a very specific task or context or may be more general and extended.

個人データの取扱いには、複数の処理者が関わる場合がある。例えば、取扱いにおける別々の段階で異なる処理者（複数の処理者）を関与させることにより、管理者自身が複数の処理者を直接関与させることを選択することができる。管理者は、また、ある処理者を関与させることを決定し、その処理者が、管理者の許可を得て、単一の処理者又は複数の他の処理者（「復処理者」）を関与させる場合がある。処理者に委託された取扱活動は、非常に具体的な職務又は文脈に限定される場合もあれば、より一般的かつ広範囲である場合もある。

76. Two basic conditions for qualifying as processor are:

処理者として適格となるための二つの基本的な条件は、以下のとおりである。

a) being *a separate entity* in relation to the controller and

管理者との関連において*別個の主体*である。

b) processing personal data *on the controller's behalf*.

*管理者に代わって*個人データを取り扱う。

77. *A separate entity* means that the controller decides to delegate all or part of the processing activities to an external organisation. Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot be a processor to another department within the same entity.

*別個の主体*とは、管理者が取扱活動の全て又は一部を外部の組織に委任することを決定することを意味する。企業グループ内においては、双方の会社は別々の主体であることから、ある会社は管理者として行動する別の会社の処理者となることができる。一方、一企業内の部署は、通常、同一の主体内の別の部署の処理者となることはできない。

78. If the controller decides to process data itself, using its own resources within its organisation, for example through its own staff, this is not a processor situation. Employees and other persons that are acting under the direct authority of the controller, such as temporarily employed staff, are not to be seen as processors since they will process personal data as a part of the controller's entity. In accordance with Article 29, they are also bound by the controller's instructions.

管理者が、自らの組織内の自己のリソースを利用して、例えば、自社のスタッフを通じてデータを取扱うことを決定する場合、これは処理者の状況ではない。一時的に雇用されたスタッフなど、管理者の直接の権限下で行動する従業員及びその他の者は、管理者の主体の一部として個人データを取扱うため、処理者とはみなされない。また、第29条により、彼らは管理者の指示に拘束される。

79. *Processing personal data on the controller's behalf* firstly requires that the separate entity processes personal data for the benefit of the controller. In Article 4(2), processing is defined as a concept including a wide array of operations ranging from collection, storage and consultation to use, dissemination or otherwise making available and destruction. The concept of "processing" is further described above under 2.1.5.

*管理者に代わって個人データを取扱う*には、まず、別個の主体が当該管理者の利益のために個人データを取扱うことが要求される。第4条第2項では、取扱いは、収集、記録保存、利用の相談、配布、又は、その他利用可能な状態とすること及び破壊までの幅広い業務を含む概念として定義されている。「取扱い」の概念については、上記2.1.5で詳細を説明している。

80. Secondly, the processing must be done on behalf of a controller but otherwise than under its direct authority or control. Acting “on behalf of” means serving someone else’s interest and recalls the legal concept of “delegation”. In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means. The lawfulness of the processing according to Article 6, and if relevant Article 9, of the Regulation will be derived from the controller’s activity and the processor must not process the data otherwise than according to the controller’s instructions. Even so, as described above, the controller’s instructions may still leave a certain degree of discretion about how to best serve the controller’s interests, allowing the processor to choose the most suitable technical and organisational means.[32]

第二に、取扱いは管理者に代わって実行されなければならないが、その直接の権限下又は管理下ではない。「に代わって」行動するとは、他者の利益に資することを意味し、「委任」の法的概念を想起する。データ保護法の場合、処理者は、少なくとも取扱いの目的及び手段の本質的な要素に関して、管理者によって与えられた指示を実装するよう求められる。GDPR第6条及び関連する場合は第9条に準拠した取扱いの適法性は、管理者の活動から生じ、処理者は、管理者の指示に従う以外の方法でデータを取り扱ってはならない。そうであっても、上述したように、管理者の指示は、処理者が最も適切な技術的及び組織的方法を選択できるように、管理者の利益に最適に資する方法についてある程度の裁量をなお残すことができる。[32]

81. Acting “on behalf of” also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller’s instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller’s instructions.

「に代わって」行動するとは、処理者が自己の目的で取扱いを実行できないことも意味する。第28条第10項に規定されているように、処理者は、管理者の指示を超えて、独自の取扱いの目的及び手段の決定を開始する場合、GDPRを侵害する。処理者は、当該取扱いに関し管理者とみなされ、管理者の指示を超えたことにより制裁の対象となり得る。

[32] See section 2.1.4 describing the distinction between essential and non-essential means.
本質的手段と非本質的手段の違いの記述についてはセクション2.1.4を参照。

Example: Service provider referred to as data processor but acting as controller
Service provider MarketinZ provides promotional advertisement and direct marketing services to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for other purposes than advertising for GoodProducts, such as developing their own business activity. The decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this set of processing operations and their processing for this purpose would constitute an infringement of the GDPR.

例:サービス・プロバイダがデータ処理者と呼ばれるが、管理者として機能する場合
サービス・プロバイダのMarketinZは、様々な企業に販促広告及びダイレクトマーケティングサービスを提供している。GoodProductZ社は、MarketinZと契約を結び、それに従って後者の会社はGoodProductZ社の顧客に商業広告を提供し、データ処理者と呼ばれる。しかしながら、MarketinZは、GoodProductZ社の顧客データベースを、自己のビジネス活動の開発など、GoodProductZ社の広告以外の目的にも利用することを決定した。個人データが移転される目的に追加の目的を加えるという決定は、MarketinZをこの一連の取扱業務のデータ管理者に変え、この目的での取扱いはGDPRの侵害を構成することになる。

82. The EDPB recalls that not every service provider that processes personal data in the course of delivering a service is a “processor” within the meaning of the GDPR. The role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as a controller for certain processing operations and as a processor for others, and the qualification as controller or processor has to be assessed with regard to specific sets of data or operations. The nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR. In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the

service provider is to be seen as a separate controller and not as a processor. [33] A case-by-case analysis remains necessary, however, in order to ascertain the degree of influence each entity effectively has in determining the purposes and means of the processing.

EDPBは、サービスの提供中に個人データを取扱うすべてのサービス・プロバイダが、GDPRの意義の範囲内における「処理者」であるとは限らないことを想起する。処理者の役割は、データを取扱っている主体の性質に起因するのではなく、特定の文脈における具体的な活動に起因する。言い換えれば、同一の企業が、特定の取扱い業務については管理者として、その他の業務については処理者として同時に行動することができ、管理者または処理者としての資格は、特定のデータセットまたは業務に関して評価されなければならない。サービスの性質により、その取扱活動がGDPRの意義の範囲内において管理者に代わって個人データを取扱っていることになるかどうかが決まる。実務上は、提供されるサービスが個人データの取扱いを特に対象としていない場合、又は、そのような取扱いがサービスの重要な要素を構成しない場合、サービス・プロバイダは、サービスを提供するために要求される当該取扱いの目的及び手段を、独立して決定する状況にあるかもしれない。そのような状況においては、サービス・プロバイダは処理者ではなく、別個の管理者と見られることとなる。[33] しかしながら、個々の主体が、取扱いの目的及び手段を決定するに当たり実質的に与える影響力の程度を確認するためには、ケースバイケースの分析が依然必要である。

Example: Taxi service

A taxi service offers an online platform which allows companies to book a taxi to transport employees or guests to and from the airport. When booking a taxi, Company ABC specifies the name of the employee that should be picked up from the airport so the driver can confirm the employee's identity at the moment of pick-up. In this case, the taxi service processes personal data of the employee as part of its service to Company ABC, but the processing as such is not the target of the service. The taxi service has designed the online booking platform as part of developing its own business activity to provide transportation services, without any instructions from Company ABC. The taxi

[33] See also Recital 81 of the GDPR, which refers to "entrusting a processor processing activities", indicating that the processing activity as such is an important part of the decision of the controller to ask a processor to process personal data on its behalf.
GDPRの前文第81段落(※)も参照。
※「処理者に対して取扱活動を委託する」が言及され、取扱活動自体が、管理者が自己に代わって個人データを取り扱うよう処理者に依頼する決定における重要な部分であることを示している箇所。

service also independently determines the categories of data it collects and how long it retains. The taxi service therefore acts as a controller in its own right, notwithstanding the fact that the processing takes place following a request for service from Company ABC.

例:タクシーサービス
あるタクシーサービスは、企業が従業員やゲストを空港へ送迎するタクシーを予約できるオンラインプラットフォームを提供しており、このタクシーを予約する際ABC社は、予約時に空港で送迎を受ける従業員名を特定する。これにより、運転手は出迎え時に従業員の身元を確認できる。この場合、タクシーサービスはABC社へのサービスの一環として当該従業員の個人データを取り扱うが、その取扱い自体はサービスの目的ではない。タクシーサービスは、輸送サービスを提供する自らの事業活動を展開する一環として、ABC社からの指示なしに、オンライン予約プラットフォームの設計を行っている。タクシーサービスは、また、収集するデータの類型及び保有期間を独自に決定する。したがって、タクシーサービスは、ABC社からのサービスの要請に従ってその取扱いを行っているという事実にもかかわらず、自らが管理者として行動する。

83. The EDPB notes that a service provider may still be acting as a processor even if the processing of personal data is not the main or primary object of the service, provided that the customer of the service still determines the purposes and means of the processing in practice. When considering whether or not to entrust the processing of personal data to a particular service provider, controllers should carefully assess whether the service provider in question allows them to exercise a sufficient degree of control, taking into account the nature, scope, context and purposes of processing as well as the potential risks for data subjects.

EDPBは、個人データの取扱いがサービスの主目的又は主要目的ではない場合においても、当該サービスの顧客が実際に取扱いの目的及び手段を決定している限り、サービス・プロバイダは依然として処理者として行動している可能性があることに留意する。個人データの取扱いを特定のサービス・プロバイダに委託するかどうかを検討する場合、管理者は、問題のサービス・プロバイダが、取扱いの性質、範囲、文脈及び目的のほか、データ主体の潜在的なリスクを考慮の上、管理者が十分な程度の管理を実行することを許容するかどうかを慎重に評価すべきである。

Example: Call center

Company X outsources its client support to Company Y who provides a call center in order to help Company X's clients with their questions. The client support service means that Company Y has to have access to Company X client data bases. Company Y can only access data in order to provide the support that Company X has procured and they cannot process data for any other purposes than the ones stated by Company X. Company Y is to be seen as a personal data processor and a processor agreement must be concluded between Company X and Y.

例:コールセンター

X社は、顧客のサポートを、X社の顧客からの質問に対応するためのコールセンターを提供するY社に外注する。顧客サポートサービスは、Y社がX社の顧客データベースにアクセスする必要があることを意味する。Y社は、X社が調達したサポートを提供するためにのみデータにアクセスすることができ、X社が述べた目的以外でデータを取り扱うことはできない。Y社は個人データの処理者とみなされ、処理者契約がX社とY社の間で締結されなければならない。

Example: General IT support

Company Z hires an IT service provider to perform general support on its IT systems which include a vast amount of personal data. The access to personal data is not the main object of the support service but it is inevitable that the IT service provider systematically has access to personal data when performing the service. Company Z therefore concludes that the IT service provider - being a separate company and inevitably being required to process personal data even though this is not the main objective of the service – is to be regarded as a processor. A processor agreement is therefore concluded with the IT service provider.

例:一般的なITサポート

Z社は、膨大な量の個人データを含む自社のITシステムの一般的なサポートを実行するためITサービス・プロバイダを雇用する。個人データへのアクセスはサポートサービスの主たる目的ではないが、ITサービス・プロバイダがサービスを実行する際に組織的に個人データへのアクセス権を有することは避けられない。したがって、Z社は、ITサービス・プロバイダは別個の会社であり、サービスの主目的ではないものの必然的に個人データを取り扱う必要があるため、処理者とみなされると結論付ける。したがって、処理者契約がITサービス・プロバイダと締結される。

Example: IT-consultant fixing a software bug

Company ABC hires an IT-specialist from another company to fix a bug in a software that is being used by the company. The IT-consultant is not hired to process personal data, and Company ABC determines that any access to personal data will be purely incidental and therefore very limited in practice. ABC therefore concludes that the IT-specialist is not a processor (nor a controller in its own right) and that Company ABC will take appropriate measures according to Article 32 of the GDPR in order to prevent the IT-consultant from processing personal data in an unauthorised manner.

例：ソフトウェアのバグを修正するITコンサルタント

ABC社は、使用しているソフトウェアのバグを修正するため別の会社からITの専門家（コンサルタント）を雇用する。ITコンサルタントは個人データを取り扱う目的で雇われておらず、ABC社は、個人データへのアクセスは純粋に偶発的なものであり、したがって、実際には非常に限られたものであると判断する。したがって、ABC社は、ITコンサルタントは処理者ではなく（それ自体が管理者でもない）、ITコンサルタントが個人データを無権限の態様で取り扱うことを防ぐため、ABC社がGDPRの第32条に準拠した適切な措置を講じると結論付ける。

84. As stated above, nothing prevents the processor from offering a preliminarily defined service but the controller must make the final decision to actively approve the way the processing is carried out, at least insofar as concerns the essential means of the processing. As stated above, a processor has a margin of manoeuvre as regards non-essential means, see above under sub-section 2.1.4.

上述のように、処理者が事前に定義されたサービスを提供することを妨げるものは何もないが、少なくとも取扱いの本質的な手段に限り、取扱いの実行方法を積極的に承認する最終決定は、管理者が行わなければならに。前述のとおり、処理者は非本質的な手段に関しては操作の余裕がある。上記、サブセクション2.1.4を参照。

Example: Cloud service provider

A municipality has decided to use a cloud service provider for handling information in its school and education services. The cloud service provides messaging services, videoconferences, storage of documents, calendar management, word processing etc. and will entail processing of personal data about school children and teachers. The cloud service provider has offered a standardized service that is offered worldwide. The municipality however must make sure that the agreement in place complies with Article

28(3) of the GDPR, that the personal data of which it is controller are processed for the municipality's purposes only. It must also make sure that their specific instructions on storage periods, deletion of data etc. are respected by the cloud service provider regardless of what is generally offered in the standardized service.

例:クラウド・サービス・プロバイダ

ある地方自治体が、学校及び教育サービスにおいて情報を扱うためにクラウド・サービス・プロバイダを利用することを決定した。クラウド・サービスは、メッセージサービス、ビデオ会議、文書の保存、カレンダーの管理、文書処理などを提供するものであり、学童及び教師に関する個人データの取扱いを伴う。クラウド・サービス・プロバイダは、世界中で提供されている標準化されたサービスを提供する。しかしながら、地方自治体は、締結されている契約がGDPRの第28条第3項に準拠していること、自己が管理者となっている個人データが地方自治体の目的にのみ取扱われることを確保しなければならない。また、標準化されたサービスにおいて一般的に提供されるものに関係なく、保存期間、データの削除などに関する地方自治体による具体的な指示が、クラウド・サービス・プロバイダによって尊重されることも確保されなければならない。

5. DEFINITION OF THIRD PARTY/RECIPIENT

第三者／取得者の定義

85. The Regulation not only defines the concepts of controller and processor but also the concepts of recipient and third party. As opposed to the concepts of controller and processor, the Regulation does not lay down specific obligations or responsibilities for recipients and third parties. These can be said to be relative concepts in the sense that they describe a relation to a controller or processor from a specific perspective, e.g. a controller or processor discloses data to a recipient. A recipient of personal data and a third party may well simultaneously be regarded as a controller or processor from other perspectives. For example, entities that are to be seen as recipients or third parties from one perspective, are controllers for the processing for which they determine the purpose and means.

GDPRは、管理者及び処理者の概念だけでなく、取得者及び第三者の概念も定義している。 管理者及び処理者の概念とは対照的に、GDPRは、取得者及び第三者の具体的な義務又は責任を定めていない。これらは、例えば、管理者又は処理者はデータを取得

者に開示するなどの特定の観点から管理者又は処理者との関係を説明するという意味で、相対的な概念といえる。個人データの取得者及び第三者が、同時に他の観点から管理者又は処理者とみなされる場合がある。例えば、ある観点から取得者又は第三者とみなされる主体は、彼らが目的及び手段を決定する取扱いにおいては管理者である。

Third party

第三者

86. Article 4(10) defines a "*third party*" as a natural or legal person, public authority, agency or body other than

第4条第10条は、「*第三者*」を、下記を除く自然人若しくは法人、公的機関、部局又はその他の組織と定義している。

- the data subject,
  データ主体
- the controller,
  管理者
- the processor and
  処理者
- persons who, under the direct authority of the controller or processor, are authorised to process personal data.
  管理者又は処理者の直接の権限下で、個人データ の取扱いを承認されている者。

87. The definition generally corresponds to the previous definition of "*third party*" in Directive 95/46/EC.

この定義は、指令95/46/ECにおける「*第三者*」の従来の定義と概ね一致している。

88. Whereas the terms "*personal data*", "*data subject*", "*controller*" and "*processor*" are defined in the Regulation, the concept of "*persons who, under the direct authority of the controller or processor, are authorised to process personal data*" is not. It is, however, generally understood as referring to persons that belong to the legal entity of the controller or processor (an employee or a role highly comparable to that of employees, e.g. interim staff provided via a temporary employment agency) but only insofar as they are authorized to process personal data. An employee etc. who obtains access to data that he or she is not authorised to access and for other purposes than that of the employer does not fall within this category. Instead, this

employee should be considered as a third party vis-à-vis the processing undertaken by the employer. Insofar as the employee processes personal data for his or her own purposes, distinct from those of his or her employer, he or she will then be considered a controller and take on all the resulting consequences and liabilities in terms of personal data processing.[34]

「*個人データ*」、「*データ主体*」、「*管理者*」及び「*処理者*」という用語はGDPRで定義されているが、「*管理者又は処理者の直接の権限下で個人データの取扱いを承認されている者*」については定義されていない。しかしながら、一般的には、管理者又は処理者の法人に帰属する者（従業員又は従業員の役割に極めて類似する役割、例えば、派遣会社を通じて提供される暫定的スタッフ）を指すと理解されているが、彼らが個人データの取扱いを承認されている場合に限られる。アクセスする承認を得ていないデータへのアクセスを、雇用者の目的以外の目的で取得する従業員等は、この範疇には含まれない。むしろ、この従業員は、雇用者が行う取扱いに関して第三者とみなされるべきである。従業員が雇用者の目的とは異なる、独自の目的で個人データを取り扱う限りにおいて、この従業員は管理者とみなされ、個人データの取扱いに関して結果として生じるすべての結果及び責任を負う。[34]

89. A third party thus refers to someone who, in the specific situation at hand, is not a data subject, a controller, a processor or an employee. For example, the controller may hire a processor and instruct it to transfer personal data to a third party. This third party will then be considered a controller in its own right for the processing that it carries out for its own purposes. It should be noted that, within a group of companies, a company other than the controller or the processor is a third party, even though it belongs to the same group as the company who acts as controller or processor.

したがって、第三者とは、具体的な状況において、データ主体、管理者、処理者又は従業員ではない者を意味する。例えば、管理者は処理者を雇用し、個人データを第三者に移転するよう指示する場合がある。この第三者は、自らの目的で実行する取扱いについては、自らが管理者であるとみなされる。なお、企業グループ内においては、管理者又は処理者以外の会社は、管理者又は処理者として行動する会社と同一のグループに属していても、第三者であることに留意すべきである。

[34] The employer (as original controller) could nevertheless retain some responsibility in case the new processing occurred because of a lack of adequate security measures.
しかし、適切な安全管理措置がないために新しい取扱いが生じた場合、（当初の管理者である）雇用者は、何らかの責任を負う場合がある。

Example: Cleaning services

Company A concludes a contract with a cleaning service company to clean its offices. The cleaners are not supposed to access or otherwise process personal data. Even though they may occasionally come across such data when moving around in the office, they can carry out their task without accessing data and they are contractually prohibited to access or otherwise process personal data that Company A keeps as controller. The cleaners are not employed by Company A nor are they seen as being under the direct authority of that company. There is no intention to engage the cleaning service company or its employees to process personal data on Company A's behalf. The cleaning service company and its employees are therefore to be seen as a third party and the controller must make sure that there are adequate security measures to prevent that they have access to data and lay down a confidentiality duty in case they should accidentally come across personal data.

例:クリーニングサービス

A社は自社の事務所を清掃するために清掃サービス会社と契約を締結する。清掃人は、個人データにアクセス又はその他の取扱いを行うことは想定されていない。清掃人は、事務所内を動き回る際にこのようなデータを時折見かけることはあるが、データにアクセスすることなく業務を遂行でき、A社が管理者として保有する個人データへのアクセスや、その他の取扱いを行うことは契約上禁止されている。清掃人はA社に雇用されておらず、A社の直接の権限の下にあるともみなされていない。A社に代わって個人データを取り扱うために清掃サービス会社又はその従業員を雇用する意図は存在しない。したがって、清掃サービス会社及びその従業員は第三者とみなされ、管理者は、彼らがデータへアクセスできないよう適切な安全管理措置が講じられていることを確認し、彼らが偶然に個人データに遭遇した場合の守秘義務を定めなければならない。

Example: Company groups – parent company and subsidiaries

Companies X and Y form part of the Group Z. Companies X and Y both process data about their respective employees for employee administration purposes. At one point, the parent company ZZ decides to request employee data from all subsidiaries in order to produce group wide statistics. When transferring data from companies X and Y to ZZ, the latter is to be regarded as a third party regardless of the fact that all companies are part of the same group. Company ZZ will be regarded as controller for its processing of

the data for statistical purposes.

例:企業グループ内の親会社及び子会社
X社及びY社はグループZの一部である。X社及びY社はいずれも、従業員の管理目的でそれぞれの従業員に関するデータを取扱う。ある時、親会社であるZZ社が、グループ全体の統計を作成するため、全ての子会社に従業員データを要求することを決定する。X社及びY社からZZ社にデータを移転する状況においては、全ての会社が同一のグループに属しているにもかかわらず、ZZ社は第三者とみなされる。ZZ社は、統計に関する目的のデータの取扱いについては管理者とみなされる。

Recipient
取得者

90. Article 4(9) defines a "*recipient*" 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. Public authorities are however not to be seen as recipients when they receive personal data in the framework of a particular inquiry in accordance with Union or Member State law (e.g. tax and customs authorities, financial investigation units etc.)[35]

第4条第9項は、「*取得者*」を、第三者であるか否かを問わず、個人データの開示を受ける自然人若しくは法人、公的機関、部局又はその他の組織と定義している。ただし、公的機関は、EU法又は加盟国の国内法に従って特別の調査の枠組み内で個人データを取得する場合、取得者とはみなされない(例:税務当局及び税関当局、金融情報部門など)。[35]

91. The definition generally corresponds to the previous definition of "*recipient*" in Directive 95/46/EC.

この定義は、指令95/46/ECの「*取得者*」の従前の定義と概ね一致している。

92. The definition covers anyone who receives personal data, whether they are a third party or not. For example, when a controller sends personal data to another entity, either a processor or a third party, this entity is a recipient. A third party recipient shall

[35] See also Recital 31 of the GDPR
GDPRの前文31参照。

be considered a controller for any processing that it carries out for its own purpose(s) after it receives the data.

この定義は、第三者であるかどうかにかかわらず、個人データを受け取るすべての者を対象とする。例えば、管理者が別の主体（処理者又は第三者）に個人データを移転する場合、この主体は取得者である。第三者である取得者は、当該データを受け取った後に独自の目的で実行する取扱いについては管理者とみなされる。

Example: Disclosure of data between companies

The travel agency ExploreMore arranges travels on request from its individual customers. Within this service, they send the customers' personal data to airlines, hotels and organisations of excursions in order for them to carry out their respective services. ExploreMore, the hotels, airlines and excursion providers are each to be seen as controllers for the processing that they carry out within their respective services. There is no controller- processor relation. However, the airlines, hotels and excursion providers are to be seen as recipients when receiving the personal data from ExploreMore.

例：企業間のデータの開示

旅行代理店ExploreMoreは、個人顧客からの依頼に応じて旅行を手配する。このサービスでは、同代理店は、航空会社、ホテル及びオプショナル・ツアー開催者がそれぞれのサービスを遂行する目的のために、顧客の個人データを各社に送付する。 ExploreMore、ホテル、航空会社及びオプショナル・ツアー開催者それぞれは、各自のサービス内で実行する取扱いの管理者とみなされる。管理者及び処理者の関係は存在しない。しかし、航空会社、ホテル及びオプショナル・ツアー開催者は、ExploreMoreから個人データを受け取る状況において、取得者とみなされる。

PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES

第2部　様々な役割の割り当ての影響

1. RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR

管理者と処理者の関係

93. A distinct new feature in the GDPR are the provisions that impose obligations directly upon processors. For example, a processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality (Article 28(3)); a processor must maintain a record of all categories of processing activities (Article 30(2)) and must implement appropriate technical and organisational measures (Article 32). A processor must also designate a data protection officer under certain conditions (Article 37) and has a duty to notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2)). Furthermore, the rules on transfers of data to third countries (Chapter V) apply to processors as well as controllers. In this regard, the EDPB considers that Article 28(3) GDPR, while mandating a specific content for the necessary contract between controller and processor, imposes direct obligations upon processors, including the duty to assist the controller in ensuring compliance.[36]

GDPRの明確で新しい特徴は、処理者に直接義務を課す規定である。例えば、処理者は、個人データの取扱いを承認された者が自らに守秘義務を課すことを確保しなければならない（第28条第3項）。処理者は、取扱活動の全ての種類の記録を保管しなければならず（第30条第2項）、かつ、適切な技術的措置及び組織的措置を実装しなければならない（第32条）。処理者は、また、特定の条件下でデータ保護オフィサーを指名しなければならず（第37条）、かつ、個人データの侵害に気付いた後、不当な遅滞なく管理者に通知する義務がある（第33条第2項）。さらに、第三国へのデータ移転に関するルール（第5章）は、管理者だけでなく処理者にも適用される。この点に関して、EDPBは、GDPR第28条第3項は、管理者と処理者の間で必要な契約の具体的な内容を義務付けている一方で、処理者には、コンプライアンスを確保するために管理者への支援義務を含め、処理者に直接の義務を課していると考える。[36]

1.1 Choice of the processor
処理者の選択

94. The controller has the **duty to use "only processors providing sufficient guarantees** to implement appropriate technical and organisational measures", so

[36] For instance, the processor should assist the controller, where necessary and upon request, in ensuring compliance with obligations relating to data protection impact assessments (Recital 95 GDPR). This needs to be reflected in the contract between the controller and the processor pursuant to Article 28(3)(f) GDPR.
例えば、処理者は、必要に応じて又は要求に応じて、データ保護影響評価に関する義務の遵守を確保するために、管理者を支援する必要がある（GDPR前文95条）。これは、GDPR第28条第3項(f)に従い、管理者と処理者の間の契約に反映させる必要がある。

that processing meets the requirements of the GDPR - including for the security of processing - and ensures the protection of data subject rights.[37] The controller is therefore responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration.

管理者は、取扱いがGDPRの要件（取扱いの安全管理に関するものを含む）を満たし、データ主体の権利の保護を確保するため、「適切な技術的措置及び組織的措置の実装に**十分な保証を提供する処理者のみ」を使用する義務**がある。[37] したがって、管理者は、処理者によって提供される保証の十分性を評価する責任があり、GDPRで規定された全ての要素を真剣に考慮したことを立証できなければならない。

95. The guarantees “provided” by the processor are those that the processor is able to **demonstrate to the satisfaction of the controller**, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations. Often this will require an exchange of relevant documentation (e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external data protection audits, recognised international certifications, like ISO 27000 series).

処理者によって「提供される」保証は、処理者が**管理者を満足させるために明示できる保証**であり、管理者が義務の遵守を評価する際に効果的に考慮できる唯一のものである。多くの場合、これには関連文書（例：プライバシーポリシー、サービス利用規約、取扱活動の記録、記録管理ポリシー、情報安全管理ポリシー、外部のデータ保護監査の報告書、ISO 27000シリーズのごとき承認された国際認証など）の交換が必要となる。

96. The controller’s assessment of whether the guarantees are sufficient is a form of risk assessment, which will greatly depend on the type of processing entrusted to the processor and needs to be made on a case-by-case basis, taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons. As a consequence, the EDPB cannot provide an exhaustive list of the documents or actions that the processor needs to show or demonstrate in any given scenario, as this largely depends on the specific circumstances of the processing.

[37] Article 28(1) and Recital 81 GDPR.
GDPR第28条第1項及び前文81。

保証が十分であるかどうかについての管理者による評価はリスク評価の一形態である。これは処理者に委託された取扱いの種類に大きく依存し、取扱いの性質、範囲、文脈及び目的のほか、自然人の権利及び自由に対するリスクを考慮の上、ケースバイケースで行う必要がある。そのため、取扱いの具体的な状況に大きく依存するため、EDPBは、処理者がどのようなシナリオでも提示または実証する必要のある文書または行為の完全なリストを提供することはできない。

97. The following elements[38] should be taken into account by the controller in order to assess the sufficiency of the guarantees: the processor's **expert knowledge** (e.g. technical expertise with regard to security measures and data breaches); the processor's **reliability**; the processor's **resources**. The reputation of the processor on the market may also be a relevant factor for controllers to consider.

保証の十分性を評価するため、管理者は次の要素[38]を考慮に入れるべきである。処理者の**専門知識**（例：安全管理措置及びデータ侵害に関する技術的な専門知識）、処理者の**信頼性**、処理者の**リソース**。市場における処理者の評判も、管理者が考慮する関連要素であり得る。

98. Furthermore, the adherence to an approved code of conduct or certification mechanism can be used as an element by which sufficient guarantees can be demonstrated.[39] The processors are therefore advised to inform the controller as to this circumstance, as well as to any change in such adherence.

さらに、承認された行動規範又は認証メカニズムの遵守は、十分な保証を証明できる要素として利用できる。[39] したがって、処理者は、この状況について、及びそのような遵守の変更があった場合にはそれを、管理者に通知することが推奨される。

99. The obligation to use only processors "providing sufficient guarantees" contained in Article 28(1) GDPR is a continuous obligation. It does not end at the moment where the controller and processor conclude a contract or other legal act. Rather the controller should, at appropriate intervals, verify the processor's guarantees, including through audits and inspections where appropriate.[40]

[38] Recital 81 GDPR.
GDPR前文81。
[39] Article 28(5) and Recital 81 GDPR.
GDPR第28条第1項及び前文81
[40] See also Article 28(3)h GDPR.

GDPR第28条第1項に定める「十分な保証を提供する」処理者のみを使用する義務は、継続的な義務である。それは、管理者及び処理者が契約又はその他の法律行為を締結した時点で終了するものではない。むしろ、管理者は、適切な間隔で、必要に応じ監査及び検査によることを含め、処理者の保証を検証すべきである。[40]

1.2 Form of the contract or other legal act
契約又はその他の法律行為の形態

100. Any processing of personal data by a processor must be governed by a contract or other legal act under EU or Member State law between the controller and the processor, as required by Article 28(3) GDPR.

処理者による個人データの取扱いは、GDPR第28条第3項で要求されているように、管理者と処理者の間におけるEU法又は加盟国の国内法に基づく契約又はその他の法律行為により規律されなければならない。

101. Such legal act must be **in writing, including in electronic form**.[41] Therefore, non-written agreements (regardless of how thorough or effective they are) cannot be considered sufficient to meet the requirements laid down by Article 28 GDPR. To avoid any difficulties in demonstrating that the contract or other legal act is actually in force, the EDPB recommends ensuring that the necessary signatures are included in the legal act, in line with applicable law (e.g. contract law).

そのような法律行為は、**電子形式を含め、書面**によらなければならない。[41] したがって、書面によらない合意は、(それらがいかに徹底したものであっても、あるいは効果的なものであっても)GDPR第28条で定められた要件を満たすに十分であるとみなすことはできない。契約又はその他の法律行為が実際に有効であることを証明するに当たっての困難を回避するため、EDPBは、適用される法律に沿って (例:契約法)、必要な署名が法律行為に含まれることを確保するよう勧告する。

GDPR第28条第3項(h)も参照。

[41] Article 28(9) GDPR.

GDPR第28条第9項。

※仮訳者注:
一次法及び二次法について、欧州委員会の資料が次のように説明している。
欧州委員会(https://ec.europa.eu/info/law/law-making-process/types-eu-law_en)
条約はEU法の出発点であり、EUでは一次法と呼ばれる。
条約の原則と目的に基づいて作られた法体系は二次法と呼ばれ、規制、指令、決定、勧告、意見などが含まれる。
一次法及び二次法並びに二次法に含まれる規則(Regulation)、指令(Directive)、決定(Decision)、勧告(Recommendation)、意見(Opinion)についての詳しい説明を国会図書館の下記URLにて読むことができる。
国立国会図書館(https://rnavi.ndl.go.jp/politics/entry/eu-law.php)

102. Furthermore, the contract or the other legal act under Union or Member State law must be **binding on the processor** with regard to the controller, i.e. it must establish obligations on the processor that are binding as a matter of EU or Member State law. Also it must set out the obligations of the controller. In most cases, there will be a contract, but the Regulation also refers to "other legal act", such as a national law (primary or secondary) or other legal instrument. If the legal act does not include all the minimum required content, it must be supplemented with a contract or another legal act that includes the missing elements

さらに、EU法又は加盟国の国内法に基づく契約その他の法律行為は、管理者に関して**処理者を拘束する**ものでなければならい。すなわち、それは、EU法又は加盟国の国内法の問題として、拘束力のある処理者に対する義務を規定しなければならない。また、それは、管理者の義務も定めなければならない。ほとんどの場合、契約が存在することになるであろうが、GDPRは、国内法(一次法又は二次法)※又はその他の法的文書などの「その他の法律行為」にも言及している。法律行為に最低限必要な全ての内容が含まれていない場合は、不足している要素を含む契約又は別の法律行為で補足されなければならない。

103. Since the Regulation establishes a clear obligation to enter into a written contract, where no other relevant legal act is in force, the absence thereof is an infringement of the GDPR.[42] Both the controller and processor are responsible for ensuring that there is a contract or other legal act to govern the processing.[43] Subject to the

[42] The presence (or absence) of a written arrangement, however, is not decisive for the existence of a controller-processor relationship. Where there is reason to believe that the contract does not correspond with reality in terms of actual control, on the basis of a factual analysis of the circumstances surrounding the relationship between the parties and the processing of personal data being carried out, the agreement may be set aside. Conversely, a controller-processor relationship might still be held to exist in absence of a written processing agreement. This would, however, imply a violation of Article 28(3) GDPR. Moreover, in certain circumstances, the absence of a clear definition of the relationship between the controller and the processor may raise the problem of the lack of legal basis on which every processing should be based, e.g. in respect of the communication of data between the controller and the alleged processor.

しかしながら、書面による取決めの存在(又は不存在)は、管理者と処理者の関係の存在を決定付けるものではない。契約が実際の管理に関して現実と一致しないと信じる理由がある場合、その契約は無効とされ得る。逆に、書面による取扱契約がない場合においても、管理者と処理者の関係がなお存在するとされる場合もあるかもしれない。ただし、これはGDPR第28条第3項の違反を意味する。さらに、一定の状況においては、管理者と処理者の関係につき明確な定義がないため、例えば、管理者と処理者とされる者の間のデータのやりとりに関して、全ての取扱いの基礎となるべき法的根拠がないという問題が発生する可能性がある。

[43] Article 28(3) is not only applicable to controllers. In the situation where only the processor is subject to the territorial scope of the GDPR, the obligation shall only be directly applicable to the processor, see also EDPB Guidelines 3/2018 on the territorial scope of the GDPR, p. 12.

provisions of Article 83 of the GDPR, the competent supervisory authority will be able to direct an administrative fine against both the controller and the processor, taking into account the circumstances of each individual case. Contracts that have been entered into before the date of application of the GDPR should have been updated in light of Article 28(3). The absence of such update, in order to bring a previously existing contract in line with the requirements of the GDPR, constitutes an infringement of Article 28(3).

A written contract pursuant to Article 28(3) GDPR may be embedded in a broader contract, such as a service level agreement. In order to facilitate the demonstration of compliance with the GDPR, the EDPB recommends that the elements of the contract that seek to give effect to Article 28 GDPR be clearly identified as such in one place (for example in an annex).

GDPRは、書面による契約を締結する明確な義務を定めているため、他の関連する法律行為が有効でない場合には、それがないことはGDPRの違反となる。[42] 管理者及び処理者の双方には、取扱いを規律する契約又はその他の法律行為の存在を確保する責任がある。[43] GDPRの第83条の規定に準拠して、管轄監督機関は、個々のケースの状況を考慮の上、管理者及び処理者の双方に制裁金を課すことができる。GDPRの適用日前に締結された契約は、第28条第3項に照らして更新されているべきである。既存の契約をGDPRの要件に合わせるため、そのような更新がなされていないことは、第28条第3項の違反となる。

GDPR第28条第3項に準拠した書面による契約は、サービス・レベル・アグリーメントのような、より広範な契約に組み込まれることがある。GDPRを遵守していることの証明を容易にするために、EDPBは、GDPR第28条を有効にしようとする契約の要素を、そのようなものとして同一の箇所で（例えば附属書で）明確に識別することを推奨する。

104. In order to comply with the duty to enter into a contract, **the controller and the processor may choose to negotiate their own contract** including all the compulsory elements **or to rely, in whole or in part, on standard contractual clauses in relation to obligations under Article 28.**[44]

第28条第3条は管理者のみに適用されるわけではない。処理者のみがGDPRの地理的適用範囲の対象となる状況においては、義務は処理者にのみ直接適用される。GDPRの地理的適用範囲（第3条）に関するEDPBガイドライン3/2018 – バージョン2.1　p.12も参照。

[44] Article 28(6) GDPR. The EDPB recalls that standard contractual clauses for the purposes of compliance with Article 28 GDPR are not the same as standard contractual clauses referred to in Article 46(2). While the former further stipulate and clarify how the provisions of Article 28(3) and (4) will be fulfilled, the latter provide appropriate safeguards in case of transfer of personal data to a third country or an international organisation in

契約を締結する義務を遵守するため、**管理者及び処理者は**、全ての強制的要素を含む**独自の契約を交渉するか、又は、第28条が定める義務に関連する標準契約条項に、全体的又は部分的に依拠することを選択できる。**[44]

105. A set of standard contractual clauses (SCCs) may be, alternatively, adopted by the Commission[45] or adopted by a supervisory authority, in accordance with the consistency mechanism.[46] These clauses could be part of a certification granted to the controller or processor pursuant to Articles 42 or 43.[47]

あるいは、一連の標準契約条項（SCC）が、一貫性メカニズムに従って、欧州委員会によって採用される場合[45]、又は、監督機関によって採用される場合がある。[46] これらの条項は、第42条又は第43条に準拠して、管理者又は処理者に与えられた認証の一部であり得る。[47]

106. The EDPB would like to clarify that there is no obligation for controllers and processors to enter into a contract based on SCCs, nor is it to be necessarily preferred over negotiating an individual contract. Both options are viable for the purposes of compliance with data protection law, depending on the specific circumstances, as long as they meet the Article 28(3) requirements.

EDPBは、管理者及び処理者がSCCに基づいて契約を締結する義務はなく、個々の契約を交渉するよりも必ずしも優先されるべきものでもないことを明確にしたい。双方のオプションとも、第28条第3項の要件を満たしている限り、特定の状況に応じ、データ保護法遵守の目的上、実行可能である。

---

the absence of an adequacy decision pursuant to Article 45(3).
GDPR第28条第6項。EDPBは、GDPR第28条を遵守するための標準契約条項は、第46条第2項に言及される標準契約条項と同一ではないことを想起する。前者は、第28条第3項及び第4項の規定がどのように充足されるかをさらに規定し明確化するのに対し、後者は、第45条第3項に準拠した十分性が存在しない場合において、個人データを第三国又は国際機関に移転する場合の適切な保護措置を提供する。

[45] Article 28(7) GDPR.
GDPR第28条第7項。

[46] Article 28(8) GDPR. The Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism, including standard contractual clauses for the purposes of compliance with Art. 28 GDPR, can be accessed here: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions
GDPR第28条第8項。一貫性メカニズムにおいて取り扱われた問題に関して監督機関及び裁判所が下した決定（GDPR第28条の遵守を目的とした標準契約条項を含む）の登録簿は、ここからアクセスできる。
https://edpb.europa.eu/our-work-tools/consistency-findings/register-for- decisions

[47] Article 28(6) GDPR.
GDPR第28条第6項。

107. If the parties wish to take advantage of standard contractual clauses, the data protection clauses of their agreement must be the same as those of the SCCs. The SCCs will often leave some blank spaces to be filled in or options to be selected by the parties. Also, the SCCs will generally be embedded in a larger agreement describing the object of the contract, its financial conditions, and other agreed clauses: it will be possible for the parties to add additional clauses (e.g. applicable law and jurisdiction) as long as they do not contradict, directly or indirectly, the SCCs[48] and they do not undermine the protection afforded by the GDPR and EU or Member State data protection laws.

当事者が標準契約条項の使用を望む場合、その契約のデータ保護条項はSCCの条項と同一でなければならない。SCCは、しばしば、当事者が記入すべき空欄や選択すべきオプションを残している。また、SCCは、通常、契約の目的、その財務条件及びその他の合意条項が記載されるより大きな契約書に組み込まれている。当事者は、SCC[48] に直接的又は間接的に相反せず、かつ、GDPR及び、EU法若しくは加盟国のデータ保護法によって提供される保護を損なわない限り、追加の条項（例：適用法及び管轄）を追加することができる。

108. Contracts between controllers and processors may sometimes be drafted unilaterally by one of the parties. Which party or parties that draft the contract may depend on several factors, including: the parties' position in the market and contractual power, their technical expertise, as well as access to legal services. For instance, some service providers tend to set up standard terms and conditions, which include data processing agreements.

[48] The EDPB recalls that the same degree of flexibility is allowed when the parties choose to use SCCs as appropriate safeguard for transfers to third countries pursuant to Article 46(2)(c) or Article 46(2)(d) GDPR. Recital 109 GDPR clarifies that "*The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses [...] or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses*".

EDPBは、当事者がGDPRの第46条第2項(c)又は第46条第2項(d)に準拠して、第三国への移転に係る適切な保護措置としてSCCを利用することを選択した場合、同程度の柔軟性が認められることを想起する。GDPRの前文109は、次のように明確にしている。「*欧州委員会又は監督機関によって採択された標準データ保護条項を管理者又は処理者が利用することができるということは、[...]標準契約条項と矛盾せず、かつ、データ主体の基本的な権利及び自由を妨げるものでない限り、管理者又は処理者が、処理者と別の処理者との間の契約のような、より広範囲の契約の中に標準データ保護条項を含めることを妨げるものではなく、また、別の条項や保護措置を追加することを妨げるものでもない。管理者及び処理者は、標準保護条項を補完する契約上の約定を介して、追加的な保護措置を提供することが奨励されるべきである*」。

管理者と処理者の間の契約は、しばしば、一方の当事者によって片務的に起草される場合がある。契約を起草する者がいずれの当事者（又は複数の当事者）であるかは、当事者の市場における地位及び契約上の力、技術的な専門知識、法律サービスへのアクセスを含むいくつかの要因に左右される場合がある。例えば、一部のサービス・プロバイダは、データ取扱契約を含む標準的な契約条件を設定する傾向がある。

109. An agreement between the controller and processor must comply with the requirements of Article 28 GDPR in order to ensure that the processor processes personal data in compliance with the GDPR. Any such agreement should take into account the specific responsibilities of controllers and processors. Although Article 28 provides a list of points which must be addressed in any contract governing the relationship between controllers and processors it leaves room for negotiations between the parties to such contracts. In some situations a controller or a processor may be in a weaker negotiation power to customize the data protection agreement. Reliance on the standard contractual clauses adopted pursuant to Article 28 (subparagraphs 7 and 8) may contribute to rebalancing the negotiating positions and to ensure that the contracts respect the GDPR.

管理者と処理者の間の契約は、処理者がGDPRに準拠して個人データを処理することを保証するために、GDPR第28条の要件に準拠する必要がある。そのような契約は、管理者と処理者の特定の責任を考慮する必要がある。第28条は、管理者と処理者の関係を規定するあらゆる契約において対処しなければならないポイントのリストを提供しているが、そのような契約の当事者間の交渉の余地を残している。状況によっては、管理者または処理者がデータ取扱契約をカスタマイズするための交渉力が弱くなることがある。第28条（第7項および第8項）に従って採択された標準的な契約条件に依存することは、交渉の立場を再均衡させ、契約がデータ取扱契約を尊重していることを保証するのに役立つかもしれない

110. The fact that the contract and its detailed terms of business are prepared by the service provider rather than by the controller is not in itself problematic and is not in itself a sufficient basis to conclude that the service provider should be considered as a controller. Also, the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law, nor can it discharge the controller from its data protection

obligations. The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR. Any proposed modification, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller, bearing in mind the degree of leeway that the processor enjoys with respect to non-essential elements of the means (see paragraphs 40-41 above). The mere publication of these modifications on the processor's website is not compliant with Article 28.

契約及びその詳細な取引条件が管理者ではなくサービス・プロバイダによって作成されているという事実自体は問題ではなく、また、それ自体は、サービス提供者を管理者とみなすべきであると結論付けるに十分な根拠ではない。また、大規模なサービス・プロバイダに対する小規模なデータ管理者の契約上の力の不均衡は、データ保護法に準拠していない条項及び契約条件を管理者が受け入れることを正当化するものと見なされるべきではなく、管理者をデータ保護の義務から解放できるものでもない。管理者は条件を評価しなければならず、又、条件を自由に受け入れてサービスを利用する限り、GDPRの遵守に係る全責任も受け入れたことになる。処理者が標準約款に含まれるデータ取扱契約の変更を提案する場合は、処理者が非本質的な手段でない要素について、どの程度の自由度を享受しているかを考慮し、管理者に直接通知し、承認を得る必要がある (上記、第40-41段落を参照)。処理者のウェブサイトでこれらの変更を公開するだけでは、第28条を遵守していることにはならない。

1.3 Content of the contract or other legal act
契約又はその他の法律行為の内容

111. Before focusing on each of the detailed requirements set out by the GDPR as to the content of the contract or other legal act, some general remarks are necessary.

契約又はその他の法律行為の内容に関してGDPRで定められた詳細な個々の要件に焦点を当てる前に、いくつかの一般的な所見が必要である。

112. While the elements laid down by Article 28 of the Regulation constitute its core content, the contract should be a way for the controller and the processor to further clarify how such core elements are going to be implemented with detailed instructions. Therefore, **the processing agreement should not merely restate the provisions of the GDPR**: rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal

data processing that is the object of the processing agreement. Far from being a pro-forma exercise, the negotiation and stipulation of the contract are a chance to specify details regarding the processing.[49] Indeed, the "protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors [...] requires a clear allocation of the responsibilities" under the GDPR.[50]

GDPRの第28条で定められた要素は中核的な内容を構成するが、当該契約は、管理者及び処理者が、そのような中核的な要素がどのように実装されるかを詳細な指示によってさらに明確にする手段であるべきである。したがって、**取扱契約には、GDPRの規定を単に再述する**だけでなく、むしろ、要件がどのように満たされるか、及び、当該取扱契約の目的である、個人データの取扱いに要求される安全性のレベルに関するより明確で具体的な情報を含めるべきである。契約の交渉及び規定は、単なる形式的な作業ではなく、取扱いに関する詳細を特定する機会である。[49] 実際、「データ主体の権利及び自由の保護並びに管理者及び処理者の責任及び義務[...]は、GDPRに準拠した責任の明確な割り当てを必要とする」。[50]

113. At the same time, the contract should **take into account "*the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject*".**[51] Generally speaking, the contract between the parties should be drafted in light of the specific data processing activity. For instance, there is no need to impose particularly stringent protections and procedures on a processor entrusted with a processing activity from which only minor risks arise: while each processor must comply with the requirements set out by the Regulation, the measures and procedures should be tailored to the specific situation. In any event, all elements of Article 28(3) must be covered by the contract. At the same time, the contract should include some elements that may help the processor in understanding the risks to the rights and freedoms of data subjects arising from the processing: because the activity is performed on behalf of the controller, often the controller has a deeper understanding

[49] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), p. 5.
デンマークの監督機関によって提出された標準契約条項の草案に関するEDPB意見書14/2019（GDPR第28条第8項）p.5も参照。
[50] Recital 79 GDPR.
GDPR前文79。
[51] Recital 81 GDPR.
GDPR前文81。

of the risks that the processing entails since the controller is aware of the circumstances in which the processing is embedded.

同時に、契約では、「*行われる取扱いの過程における処理者の特定された職務及び職責並びにデータ主体の権利及び自由に対するリスク*」を考慮に入れるべきである。[51] 一般的にいえば、当事者間の契約は、具体的なデータ取扱活動に照らして作成されるべきである。例えば、軽微なリスクのみが発生する取扱活動を委託された処理者に特に厳格な保護及び手続を課す必要はない。個々の処理者はGDPRで定められた要件を遵守しなければならないが、措置及び手続は具体的な状況に合わせるべきである。いずれにせよ、第28条第3項の全ての要素は契約でカバーされなければならない。同時に、契約には、取扱いから生じるデータ主体の権利及び自由に対するリスクを処理者が理解するのに資するであろういくつかの要素を含めるべきである。その活動は管理者に代わって実行されるので、多くの場合、管理者が、その取扱いが組み込まれている状況を認識しており、その取扱いに伴うリスクをより深く理解している。

114. Moving on to the required content of the contract or other legal act, EDPB interprets Article 28(3) in a way that it needs to set out:

契約又はその他の法律行為に求められている内容に移ると、EDPBは、第28条第3項は(契約又はその他の法律行為では)次のことを定める必要があるとしていると解釈している。

- the **subject-matter** of the processing (for instance, video surveillance recordings of people entering and leaving a high-security facility). While the subject matter of the processing is a broad concept, it needs to be formulated with enough specifications so that it is clear what the main object of the processing is;

  取扱いの**主題**(例えば、高セキュリティ施設に出入りする人々のビデオ監視記録)。取扱いの主題は広い概念であるが、取扱いの主な目的が何であるかが明確になるよう、十分な仕様で策定する必要がある。

- the **duration**[52] of the processing: the exact period of time, or the criteria used to determine it, should be specified; for instance, reference could be made to the duration of the processing agreement;

  取扱いの**期間**[52]:正確な期間、又は、期間を決定するために使用される基準が特定

[52] The duration of the processing is not necessarily equivalent to the duration of the agreement (there may be legal obligations to keep the data longer or shorter).
取扱いの期間は、必ずしも契約の期間と同じではない(データをより長くまたはより短く保持する法的義務がある場合がある)。

されるべきである。例えば、取扱契約の期間に言及することができるであろう。

- the **nature** of the processing: the type of operations performed as part of the processing (for instance: “filming”, “recording”, “archiving of images”, ...) **and purpose** of the processing (for instance: detecting unlawful entry). This description should be as comprehensive as possible, depending on the specific processing activity, so as to allow external parties (e.g. supervisory authorities) to understand the content and the risks of the processing entrusted to the processor.

  取扱いの**性質**：取扱いの一部として実行される業務の種類（「撮影」、「記録」、「画像の保管」など）及び取扱いの**目的**（不法侵入の検出など）。この記述は、外部の当事者（例：監督機関）が処理者に委託された取扱いの内容及びリスクを理解できるよう、具体的な処理活動に応じて、可能な限り包括的であるべきである。

- the **type of personal data**: this should be specified in the most detailed manner as possible (for instance: video images of individuals as they enter and leave the facility). It would not be adequate merely to specify that it is “personal data pursuant to Article 4(1) GDPR” or “special categories of personal data pursuant to Article 9”. In case of special categories of data, the contract or legal act should at least specify which types of data are concerned, for example, “information regarding health records”, or “information as to whether the data subject is a member of a trade union”;

  個人データの種類：これは、可能な限り詳細な態様で特定されるべきである（例、施設に出入りする個人のビデオ画像）。「GDPR第4条第1項に準拠した個人データ」又は「第9条に準拠した特別な類型の個人データ」と特定するだけでは不十分である。特別な類型のデータの場合、契約又は法律行為では、例えば、「健康記録に関する情報」又は「データ主体が労働組合のメンバーであるかどうかに関する情報」など、少なくとも関係するデータの種類を特定すべきである。

- the **categories of data subjects**: this, too, should be indicated in a quite specific way (for instance: “visitors”, “employees”, delivery services etc.);

  データ主体の類型：これも、また、非常に具体的な形（例：「訪問者」、「従業員」、「配達サービス等」）で示されるべきである。

- the **obligations and rights of the controller**: the rights of the controller are further dealt with in the following sections (e.g. with respect to the right of the controller to perform inspections and audits). As regards the obligations of the controller, examples include the controller’s obligation to provide the processor

with the data mentioned in the contract, to provide and document any instruction bearing on the processing of data by the processor, to ensure, before and throughout the processing, compliance with the obligations set out in the GDPR on the processor's part, to supervise the processing, including by conducting audits and inspections with the processor.

管理者の義務及び権利：管理者の権利は、後続のセクションでさらに詳しく説明する（例：検査及び監査の実施に関する管理者の権利に関して）。管理者の義務には、例えば、契約に記載されているデータを処理者に提供する義務、処理者によるデータの取扱いに関係する指示を提供及び文書化する義務、取扱いの前及び取扱い全体を通じて、GDPRに定められた処理者の義務の遵守を確保する義務、取扱いを監督する（処理者に対する監査及び検査の実施を含む）義務がある。

115. While the GDPR lists elements that always need to be included in the agreement, other relevant information may need to be included, depending on the context and the risks of the processing as well as any additional applicable requirement.

GDPRでは契約に常に含める必要のある要素を列挙しているが、取扱いのリスク及び文脈のほか、追加の適用要件によっては、他の関連情報を含める必要がある場合がある。

1.3.1 The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR)

処理者は、管理者からの文書化された指示のみに基づいてデータを取り扱わなければならない（GDPR第28条第3項(a)）。

116. The need to specify this obligation stems from the fact that the processor processes data on behalf of the controller. Controllers must provide its processors with instructions related to each processing activity. Such instructions can include permissible and unacceptable handling of personal data, more detailed procedures, ways of securing data, etc. The processor shall not go beyond what is instructed by the controller. It is however possible for the processor to suggest elements that, if accepted by the controller, become part of the instructions given.

この義務を特定する必要性は、処理者が管理者に代わってデータを取扱うという事実に起因する。管理者は、個々の取扱活動に関連する指示を処理者に提供しなければならない。このような指示には、許容される個人データの取扱い及び許容されない個人データの取り扱い、より詳細な手続、データを保護する方法などを含めることができる。処理者は、管理者から指示された内容を超えてはならない。しかし、処理者が要素を提案し、管理者

がそれを受け入れれば、指示された内容の一部とすることも可能である。

117. When a processor processes data outside or beyond the controller's instructions, and this amounts to a decision determining the purposes and means of processing, the processor will be in breach of its obligations and will even be considered a controller in respect of that processing in accordance with Article 28(10) (see section 1.5 below[53]).

処理者が管理者の指示外又はそれを超えてデータを取扱い、これが取扱いの目的及び手段を決定する決定に相当する場合、処理者はその義務に違反し、さらに第28条第10項に従って、その取扱いに関して管理者とみなされることになる（下記、セクション1.5を参照[53]）。

118. The instructions issued by the controller must be **documented**. For these purposes, it is recommended to include a procedure and a template for giving further instructions in an annex to the contract or other legal act. Alternatively, the instructions can be provided in any written form (e.g. e-mail), as well as in any other documented form as long as it is possible to keep records of such instructions. In any event, to avoid any difficulties in demonstrating that the controller's instructions have been duly documented, the EDPB recommends keeping such instructions together with the contract or other legal act.

このような指示は**文書化**されなければならない。これらの目的のため、契約（又はその他の法律行為）の別紙に、さらに指示を与えるための手続及びテンプレートを含めることが推奨される。あるいは、そのような指示の記録を残すことが可能であれば、電子メールなどの書面でも、その他の文書化された形式でも提供することができる。いずれにせよ、管理者の指示が適切に文書化されていることを証明することが困難にならないように、EDPBは、そのような指示を契約又はその他の法律行為と共に保管するよう勧告する。

119. The duty for the processor to refrain from any processing activity not based on the controller's instructions also applies to **transfers** of personal data to a third country or international organisation. The contract should specify the requirements for transfers to third countries or international organisations, taking into account the provisions of Chapter V of the GDPR.

[53] See Part II, sub-section 1.5 ("Processor determining purposes and means of processing").
第2部サブセクション1.5（「取扱いの目的及び手段を決定する処理者」）を参照。

処理者が管理者の指示に基づかない取扱活動を控える義務は、第三国又は国際機関への個人データの**移転**にも適用される。契約には、GDPRの第5章の規定を考慮の上、第三国又は国際機関への移転の要件を特定すべきである。

120. The EDPB recommends that controller pay due attention to this specific point especially when the processor is going to delegate some processing activities to other processors, and when the processor has divisions or units located in third countries. If the instructions by the controller do not allow for transfers or disclosures to third countries, the processor will not be allowed to assign the processing to a sub-processor in a third country, nor will he be allowed to have the data processed in one of his non-EU divisions.

EDPBは、特に処理者が一部の取扱活動を他の処理者に委任する場合、及び、処理者が第三国に部署又は部門を有する場合、管理者はこの特定の点に十分な注意を払うよう勧告する。管理者の指示が第三国への移転又は開示を許可しない場合、処理者は、第三国の復処理者に取扱いを割り当てることも、自己のEU外の部署の一つにデータを取扱わせることもできない。

121. A processor may process data other than on documented instructions of the controller **when the processor is required to process and/or transfer personal data on the basis of EU law or Member State law to which the processor is subject**. This provision further reveals the importance of carefully negotiating and drafting data processing agreements, as, for example, legal advice may need to be sought by either party as to the existence of any such legal requirement. This needs to be done in a timely fashion, as the processor has an obligation to inform the controller of such requirement before starting the processing. Only when that same (EU or Member State) law forbids the processor to inform the controller on "important grounds of public interest", there is no such information obligation. In any case, any transfer or disclosure may only take place if authorised by Union law, including in accordance with Article 48 of the GDPR.

処理者は、自己が服するEU法又は加盟国法に基づき個人データを取り扱うこと及び/又は移転することを要求されている場合、管理者の文書化された指示に基づくことなくデータを取扱うことができる。この規定は、例えば、そのような法的要件の存在に関して、いずれかの当事者が法的助言を求める必要があり得ることから、データ取扱契約を慎重に交渉して作成することの重要性をさらに明らかにしている。処理者は取扱いを開始する前

にそのような要件を管理者に通知する義務があるため、これは適時に行う必要がある。同一の（EU又は加盟国の）法律が処理者に「公益の重要な理由」に基づき管理者に通知することを禁じている場合にのみ、そのような通知義務は存在しない。いずれの場合も、移転又は開示は、GDPRの第48条に準拠することを含め、EU法によって承認された場合にのみ行うことができる。

1.3.2 The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR)

処理者は、個人データの取扱いを承認された者が自らに守秘義務を課し、又は、適切な法律の守秘義務の下にあることを確保しなければならない（GDPR第28条第3項(b)）。

122. The contract needs to state that the processor must ensure that anyone it allows to process the personal data is committed to confidentiality. This may occur either via a specific contractual agreement, or due to statutory obligations already in place.

契約書には、処理者が個人データの取扱いを許可したものに、守秘義務を課すことを明記する必要がある。これは、特定の契約上の合意を介して、又は、すでに施行されている法定義務により生じ得る。

123. The broad concept of “persons authorised to process the personal data” includes employees and temporary workers. Generally speaking, the processor should make the personal data available only to the employees who actually need them to perform tasks for which the processor was hired by the controller.

広い概念である「個人データの取扱いを承認された者」には、従業者及び臨時従業者が含まれる。一般的にいえば、処理者は、処理者が管理者に雇われた業務を遂行するために実際に個人データを必要とする従業者のみが個人データを利用できるようにすべきである。

124. The commitment or obligation of confidentiality must be “appropriate”, i.e. it must effectively forbid the authorised person from disclosing any confidential information without authorisation, and it must be sufficiently broad so as to encompass all the personal data processed on behalf of the controller as well as the conditions under which the personal data are processed.

機密保持の約束又は義務は「適切」でなければならない。すなわち、それは、承認され

た者が承認を得ることなく秘密情報を開示することを効果的に禁止するものでなければならず、また、それは、管理者に代わって取扱われたすべての個人データや個人データが取扱われる条件を網羅するように、十分に広範でなければならない。

1.3.3 The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR)

処理者は、第32条によって求められる全ての措置を講じなければならない（GDPR第28条第3項(c)）。

125. Article 32 requires the controller and the processor to implement appropriate technical and organisational security measures. While this obligation is already directly imposed on the processor whose processing operations fall within the scope of the GDPR, the duty to take all measures required pursuant to Article 32 still needs to be reflected in the contract concerning the processing activities entrusted by the controller.

第32条は、管理者及び処理者に適切な技術上及び組織上の安全管理措置を実装することを求めている。この義務は、その取扱業務がGDPRの範囲内にある処理者にすでに直接課されているが、第32条によって求められている全ての措置を講じる義務は、管理者から委託された取扱活動に関する契約に依然として反映される必要がある。

126. As indicated earlier, the processing contract should not merely restate the provisions of the GDPR. The contract needs to include or reference information as to the security measures to be adopted, **an obligation on the processor to obtain the controller's approval before making changes**, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR. Moreover, the description is also necessary in order to enable the controller to comply with its accountability duty pursuant to Article 5(2) and Article 24 GDPR as regards the security measures imposed on the processor. A corresponding obligation of the processor to assist the controller and to make available all information necessary to demonstrate compliance can be inferred from Art. 28.3 (f) and (h) GDPR.

前に示したように、取扱契約はGDPRの規定を単に再述するだけではならない。契約には採用される安全管理措置、**処理者が変更を加える前に管理者の承認を得る義務**、及び、

時間の経過とともに進化する可能性があるリスクに関する適切性を確保するための安全管理措置の定期的な見直しに関する情報を含める又は参照する必要がある。契約に含められる安全管理措置に関する情報の詳細度は、管理者がGDPR第32条第1項に準拠した措置の適切性を評価できるものでなければならない。さらに、その記述は、管理者が処理者に課せられた安全管理措置に関してGDPR第5条第2項及び第24条に定めるアカウンタビリティの義務を遵守できるようにするためにも必要である。管理者を支援し、遵守を証明するために必要な全ての情報を利用可能にするという処理者の対応すべき義務は、GDPRの第28条第3項(f)及び(h)から推測できる。

127. The level of instructions provided by the controller to the processor as to the measures to be implemented will depend on the specific circumstances. In some cases, the controller may provide a clear and detailed description of the security measures to be implemented. In other cases, the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures. In any event, the controller must provide the processor with a description of the processing activities and security objectives (based on the controller's risk assessment), as well as approve the measures proposed by the processor. This could be included in an annex to the contract. The controller exercises its decision-making power over the main features of the security measures, be it by explicitly listing the measures or by approving those proposed by the processor.

実装される措置に関して管理者から処理者に提供される指示のレベルは、具体的な状況によって異なる。ある場合には、管理者は、実装される安全管理措置の明確で詳細な説明を提供する場合がある。別の場合には、管理者は、達成すべき最小の安全管理目的を説明し、一方で特定の安全管理措置の実装を提案するよう処理者に要求する場合がある。いずれにせよ、管理者は、取扱活動及び安全管理目的の説明(管理者のリスク評価に基づくもの)を処理者に提供するほか、処理者によって提案された措置を承認しなければならない。これは、契約書の別紙に含めることができる。管理者は、措置を明示的に掲示するか、処理者によって提案されたものを承認することにより、安全管理措置の主たる特性に対して意思決定権を行使する。

1.3.4 The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR).

処理者は、別の処理者を従事させることに関し第28条第2項及び第28条第4項

が規定する条件を尊重しなければならない(GDPR第28条第3項(d))。

128. The agreement must specify that the processor may not engage another processor without the controller's prior written authorisation and whether this authorisation will be specific or general. In case of general authorisation, the processor has to inform the controller of any change of sub- processors under a written authorisation, and give the controller the opportunity to object. It is recommended that the contract set out the process for this. It should be noted that the processor's duty to inform the controller of any change of sub-processors implies that the processor actively indicates or flags such changes toward the controller.[54] Also, where specific authorisation is required, the contract should set out the process for obtaining such authorisation.

契約には、管理者の事前の書面による承認なしに、処理者は別の処理者を従事させることはできないこと、及び、この承認が特定的なものか全般的なものかを明記しなければならない。全般的な承認の場合、処理者は、書面による承認の下で復処理者の変更をした場合、管理者に通知し、管理者に異議を唱える機会を与えなければならない。契約にこのためのプロセスを規定することが推奨される。復処理者の変更を管理者に通知する処理者の義務は、処理者がそのような変更を管理者に対して積極的に示すか警告することを意味していることに留意すべきである。[54] また、特定的な承認が求められている場合、契約にそのような承認を得るプロセスを規定すべきである。

129. When the processor engages another processor, a contract must be put in place between them, imposing the same data protection obligations as those imposed on the original processor or these obligations must be imposed by another legal act under Union or Member State law (see also below paragraph 160). This includes the obligation under Article 28(3)(h) to allow for and contribute to audits by the controller or another auditor mandated by the controller.[55] The processor is liable to the

[54] In this regard it is, by contrast, e.g. not sufficient for the processor to merely provide the controller with a generalized access to a list of the sub-processors which might be updated from time to time, without pointing to each new sub-processor envisaged. In other words, the processor must actively inform the controller of any change to the list (i.e. in particular of each new envisaged sub-processor).

この点で、対照的に、例えば、処理者が、想定される個々の新しい復処理者を示すことなく、随時更新されるかもしれない復処理者のリストへの全般的なアクセスを管理者に提供するだけでは十分ではないと考えられる。言い換えると、処理者は、リストの変更を管理者に積極的に通知しなければならない(すなわち、特に、新たに想定される個々の復処理者について)。

[55] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 44.

2019年7月9日、デンマークの監督機関によって提出された標準契約条項草案(GDPR第28条第8項)に関する

controller for the other processors' compliance with data protection obligations (for further details on the recommended content of the agreement see sub-section 1.6 below[56]).

処理者が別の処理者を従事させる場合、最初の処理者に課せられるものと同等のデータ保護義務を課す契約を両者の間で締結するか、これらの義務をEU法又は加盟国の法律に基づく別の法律行為によって課さなければならない (下記、第160段落を参照)。これには、第28条第3項(h)に定める、管理者又は管理者から委任された別の監査人による監査を受け入れ、それに貢献する義務が含まれる。[55] 処理者は、他の処理者がデータ保護義務を遵守することにつき、管理者に対して責任を負う(勧告される契約内容の詳細については、下記サブセクション1.6を参照[56])。

1.3.5 The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the data subject's rights (Article 28(3) (e) GDPR).

処理者は、データ主体の権利を行使する要求に対処すべき管理者の義務の履行のため、管理者を支援しなければならない(GDPR第28条第3項(e))。

130. While ensuring that data subjects requests are dealt with is up to the controller, the contract must stipulate that the processor has an obligation to provide assistance "by appropriate technical and organisational measures, insofar as this is possible". The nature of this assistance may vary greatly "taking into account the nature of the processing" and depending on the type of activity entrusted to the processor. The details concerning the assistance to be provided by the processor should be included in the contract or in an annex thereto.

データ主体の要求が対処されることの確保は管理者次第であるが、契約には、処理者は「可能である限り、適切な技術的及び組織上の措置によって」支援を提供する義務があることを定めなければならない。この支援の性質は、「取扱いの性質を考慮して」、また、処理者に委託された活動の種類によって、大きく異なり得る。処理者が提供する支援に関する詳細は、契約又はその別紙に含めるべきである。

131. While the assistance may simply consist in promptly forwarding any request received and/or enabling the controller to directly extract and manage the relevant

---

EDPB意見書14/2019、第44段落も参照。

[56] See Part II, sub-section 1.6 ("Sub-processors").
第2部サブセクション1.6 (「復処理者」)を参照。

personal data, in some circumstances the processor will be given more specific, technical duties, especially when it is in the position of extracting and managing the personal data.

支援は単に受け取った要求を速やかに転送したり、管理者が関連する個人データを直接抽出・管理できるようにするだけの場合もあるが、状況によっては、処理者は、特に個人データを抽出・管理する立場にある場合、より具体的、技術的な職務が与えられることとなろう。

132. It is crucial to bear in mind that, although the practical management of individual requests can be outsourced to the processor, the controller bears the responsibility for complying with such requests. Therefore, the assessment as to whether requests by data subjects are admissible and/or the requirements set by the GDPR are met should be performed by the controller, either on a case-by-case basis or through clear instructions provided to the processor in the contract before the start of the processing. Also, the deadlines set out by Chapter III cannot be extended by the controller based on the fact that the necessary information must be provided by the processor.

個々の要求の実際の管理は処理者に外注できるが、管理者はそのような要求に応じる責任があることを念頭に置くことが極めて重要である。したがって、データ主体による要求が受入可能であるかどうか、及び/又は、GDPRに定められた要件が満たされているかどうかに関する評価は、ケースバイケースで、又は取扱い開始前に契約において処理者に提供される明確な指示を通じて、管理者が行うべきである。また、第3章で定められた期限は、必要な情報は処理者が提供しなければならないということを根拠に、管理者が延長することはできない。

1.3.6 The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR).
処理者は、第32条から第36条に定める義務の遵守の確保に当たり、管理者を支援しなければならない(GDPR第28条第3項(f))。

133. It is necessary for the contract to avoid merely restating these duties of assistance: **the agreement should contain details as to how the processor is asked to help the controller meet the listed obligations.** For example, procedures and template forms may be added in the annexes to the agreement, allowing the processor to provide the controller with all the necessary information.

契約では、これらの支援義務を単に再述することは避ける必要がある。**契約には、処理者が管理者が掲示された義務を果たすことをどのように支援するかに関する詳細を含めるべきである。**例えば、処理者が管理者に全ての必要な情報を提供できるように手続及びテンプレート・フォームを契約の別紙に追加することができる。

134. The type and degree of assistance to be provided by the processor may vary widely "*taking into account the nature of processing and the information available to the processor".* The controller must adequately inform the processor as to the risk involved in the processing and as to any other circumstance that may help the processor meet its duty.

処理者が提供する支援の種類及び程度は、「*取扱いの性質及び処理者が利用できる情報を考慮して*」大きく異なり得る。管理者は、取扱いに伴うリスク及び処理者がその義務を果たすのに役立ち得るその他の状況につき、処理者に適切に通知しなければならない。

135. Moving on to the specific obligations, the processor has, first, a duty to assist the controller in meeting the obligation to adopt adequate technical and organisational measures to ensure security of processing.[57] While this may overlap, to some extent, with the requirement that the processor itself adopts adequate security measures, where the processing operations of the processor fall within the scope of the GDPR, they remain two distinct obligations, since one refers to the processor's own measures and the other refers to the controller's.

具体的な義務に話を移すと、処理者は、まず、取扱いの安全管理を確保するための適切な技術上及び組織上の措置を採用する義務を充足するに当たり、管理者を支援する義務を負う。[57] これは、ある程度、処理者自身が適切な安全管理措置を採用する要件と重複し得るが、処理者の取扱業務がGDPRの範囲内にある場合は、一つは処理者自身の措置を意味し、もう一つは管理者の措置を意味するため、安全管理措置は二つの異なる義務のままである。

136. Secondly, the processor must assist the controller in meeting the obligation to notify personal data breaches to the supervisory authority and to data subjects. The processor must notify the controller whenever it discovers a personal data breach

[57] Article 32 GDPR.
GDPR第32条。

affecting the processor's or a sub-processor's facilities / IT systems and help the controller in obtaining the information that need to be stated in the report to the supervisory authority.[58] The GDPR requires that the controller notify a breach without undue delay in order to minimize the harm for individuals and to maximize the possibility to address the breach in an adequate manner. Thus, the processor's notification to the data controller should also take place without undue delay.[59] Depending on the specific features of the processing entrusted to the processor, it may be appropriate for the parties to include in the contract a specific timeframe (e.g. number of hours) by which the processor should notify the controller, as well as the point of contact for such notifications, the modality and the minimum content expected by the controller.[60] The contractual arrangement between the controller and the processor may also include an authorisation and a requirement for the processor to directly notify a data breach in accordance with Articles 33 and 34, but the legal responsibility for the notification remains with the controller.[61] If the processor does notify a data breach directly to the supervisory authority, and inform data subjects in accordance with Article 33 and 34, the processor must also inform the controller and provide the controller with copies of the notification and information to data subjects.

次に、処理者は、監督機関及びデータ主体に個人データの侵害を通知する義務の充足に当たり、管理者を支援しなければならない。処理者は、処理者又は復処理者の施設/ITシステムに影響を与える個人データの侵害を発見した場合は常に管理者に通知し、監督機関への報告に記載する必要のある情報を管理者が取得するに当たり支援しなければならない。[58] GDPRでは、データ主体の被害を最小限に抑え、適切な方法で違反に対処する可能性を最大限に高めるために、管理者がデータ侵害を不当に遅延することなく通知することが求められている。したがって、処理者から管理者への通知も、不当に遅延することなく行われる必要がある。[59] 処理者に委託された取扱いの具体的な特徴に応じて、

[58] Article 33(3) GDPR.
GDPR第33条第3項。

[59] For more information, see the Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 13-14.
詳細については、規則2016/679に定める個人データ侵害の通知に関するガイドライン、WP250rev.01（2018年2月6日）、p.13-14を参照。

[60] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 40.
2019年7月9日、デンマークの監督機関によって提出された標準契約条項草案（GDPR第28条第8項）に関するEDPB意見書14/2019、第44段落も参照。

[61] Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 14.
規則2016/679に定める個人データ侵害の通知に関するガイドライン、WP250rev.01（2018年2月6日）、p.14。

処理者が管理者に通知すべき特定の時間枠（時間数など）、そのような通知のための連絡先、方法、管理者が期待する最低限の内容を契約に含めることが当事者にとって適切な場合がある。[60] 管理者と処理者の間の契約上の取り決めには、処理者が第33条および第34条に従ってデータ違反を直接通知するための権限および要件を含めることも可能だが、当該通知の法的責任は管理者にある。[61] 処理者がデータ侵害を監督機関へ直接通知し、第33条および第34条に従ってデータ主体に通知する場合、処理者は管理者にも通知し、データ主体への通知および情報のコピーを管理者に提供しなければならない。

137. Furthermore, the processor must also assist the controller in carrying out data protection impact assessments when required, and in consulting the supervisory authority when the outcome reveals that there is a high risk that cannot be mitigated.

さらに、処理者は、必要に応じ、データ保護影響評価の実行に当たり、また、その結果が軽減できない高いリスクがあることを明らかにした場合における監督機関への相談に当たり、管理者を支援しなければならない。

138. The duty of assistance does not consist in a shift of responsibility, as those obligations are imposed on the controller. For instance, although the data protection impact assessment can in practice be carried out by a processor, the controller remains accountable for the duty to carry out the assessment[62] and the processor is only required to assist the controller "where necessary and upon request."[63] As a result, the controller is the one that must take the initiative to perform the data protection impact assessment, not the processor.

支援の義務は、責任の転嫁を構成しない。これらの義務が管理者に課せられるためである。例えば、データ保護影響評価は実際には処理者が実行できるが、管理者は、その評価を実行する義務につき引き続き責任を負い[62]、処理者に求められているのは、「必要に応じ、かつ、要求に応じて」管理者を支援することのみである。[63] その結果、データ保護影響評価を実行するために主導権を握らなければならないのは、処理者ではなく管理者である。

---

[62] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, p. 14

第29条データ保護作業部会、データ保護影響評価（DPIA）及び規則2016/679の適用上取扱いが「高リスクをもたらす可能性が高い」かどうかの判断に関するガイドライン、WP 248 rev.01、p.14。

[63] Recital 95 GDPR.

GDPR前文95。

1.3.7 On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Art. 28(3)(g) GDPR).
取扱活動の終了時には、処理者は、管理者の選択により、全ての個人データを消去又は管理者に返却し、既存の複製物を消去しなければならない(GDPR第28条第3項(g))。

139. The contractual terms are meant to ensure that the personal data are subject to appropriate protection after the end of the "provision of services related to the processing": it is therefore up to the controller to decide what the processor should do with regard to the personal data.

契約条件は、「取扱いに関連するサービスの提供」の終了後に個人データが適切に保護されることを確保するためのものである。したがって、処理者が個人データに関して何をすべきかを決定するのは管理者である。

140. The controller can decide at the beginning whether personal data shall be deleted or returned by specifying it in the contract, through a written communication to be timely sent to the processor. The contract or other legal act should reflect the possibility for the data controller to change the choice made before the end of the provision of services related to the processing. The contract should specify the process for providing such instructions.

管理者は、個人データを消去しなければならないか返却しなければならないかを契約書に明記し、処理者に適時に送付される書面により、最初に決定できる。契約又はその他の法律行為は、取扱いに関連するサービスの提供が終了する前にデータ管理者が行った選択を変更する可能性を反映すべきである。契約では、そのような指示の提供に関するプロセスを明記すべきである。

141. If the controller chooses that the personal data be deleted, the processor should ensure that the deletion is performed in a secure manner, also in order to comply with Article 32 GDPR. The processor should confirm to the controller that the deletion has been completed within an agreed timescale and in an agreed manner.

管理者が個人データの消去を選択した場合、処理者は、GDPR第32条を遵守するためにも、安全な態様で消去が実行されることを確保すべきである。処理者は、消去が合意された時間枠内に、かつ、合意された態様により完了したことを管理者に確認すべきである。

142. The processor must delete all existing copies of the data, unless EU or Member State law requires further storage. If the processor or controller is aware of any such legal requirement, it should inform the other party as soon as possible.

処理者は、全ての既存のデータ複製物を消去しなければならないが、EU又は加盟国の法律が更なる保存を求めている場合は例外とされる。処理者又は管理者がそのような法的要件を認識している場合は、できるだけ早期に相手方に通知すべきである。

1.3.8 The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR).

処理者は、第28条に定められた義務の遵守を証明するため、及び、管理者によって行われる検査若しくは管理者から委任された別の監査人によって行われる検査を含め、監査を受け入れ、また、監査に資するようにするために必要な全ての情報を、管理者が利用できるようにしなければならない(GDPR第28条第3項(h))。

143. The contract shall include details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing that are relevant to demonstrate compliance with the obligations laid down in Article 28 GDPR. For instance, the relevant portions of the processor's records of processing activities may be shared with the controller. The processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on the functioning of the systems used, security measures, how the data retention requirements are met, data location, transfers of data, who has access to data and who are the recipients of data, sub-processors used, etc.

契約には、GDPR第28条に定められた義務の遵守を証明するために関連する処理の詳細について、管理者が十分に情報提供されるように、処理者と管理者の間の情報の流れが発生する頻度及び方法に関する詳細が含まれていなければならない。例えば、処理者の取扱活動に係る記録の関連部分は、管理者と共有され得る。処理者は、管理者に代わって、取扱活動がどのように行われるかに関する全ての情報を提供すべきである。そのような情報には、利用するシステムの機能、安全管理措置、データ保持要件を満たす根拠、

データの所在地、データの移転、データへのアクセス及びデータの取得者、使用する復処理者などに関する情報を含めるべきである。

144. Further details shall also be set out in the contract regarding the ability to carry out and the duty to contribute to inspections and audits by the controller or another auditor mandated by the controller.

The GDPR specifies the inspections and audits are carried out by the controller or by a third party mandated by the controller. The goal of such audit is ensuring that the controller has all information concerning the processing activity performed on its behalf and the guarantees provided by the processor. The processor may suggest the choice of a specific auditor, but the final decision has to be left to the controller according to Article 28(3)(h) of the GDPR.[64] Additionally, even where the inspection is performed by an auditor proposed by the processor, the controller retains the right to contest the scope, methodology and results of the inspection. [65]

The parties should cooperate in good faith and assess whether and when there is a need to perform audits on the processor's premises,, as well as which type of audit or inspection (remote / on-site / other way to gather the necessary information) would be needed and appropriate in the specific case also taking into account security concerns; the final choice on this is to be taken by the controller. Following the results of the inspection, the controller should be able to request the processor to take subsequent measures, e.g. to remedy shortcomings and gaps identified.[66] Likewise, specific procedures should be established regarding the processor's and the controller's inspection of sub-processors (see sub-section 1.6 below[67]).

管理者または管理者に委任された別の監査人による検査および監査を実施する能力やそれに貢献する義務について、さらに詳細を契約書に定めるものとする。

---

[64] See EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, paragraph 43.
管理者と処理者間の標準契約条項に関するEDPBとEDPSの共同意見書01/2021、第43段落を参照。

[65] See Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), paragraph 43.
デンマークの監督機関によって提出された標準契約条項の草案に関するEDPB意見書14/2019(GDPR第28条第8項)を参照。

[66] See Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), paragraph 43.
デンマークの監督機関によって提出された標準契約条項の草案に関するEDPB意見書14/2019(GDPR第28条第8項)を参照。

[67] See Part II, sub-section 1.6 ("Sub-processors").
第2部サブセクション1.6(「復処理者」)を参照。

GDPRでは、管理者または管理者に委任された第三者による検査および監査を実施することが規定されている。このような監査の目的は、管理者が自分のために行われた処理活動および処理者が提供する保証に関するすべての情報を確実に把握することである。処理者は、特定の監査人を選択するよう提案ができるが、GDPR第28条第3項(h)に従い、最終的な決定は管理者に委ねられる。[64] また、処理者が提案した監査人によって検査が行われた場合でも、管理者は検査の範囲、方法、結果について異議を唱える権利を保持する。[65]

両者は誠意をもって協力し、処理者の施設で監査を行う必要性があるかどうか、また、セキュリティ上の懸念を考慮した上で、特定のケースではどのタイプの監査または検査（リモート／オンサイト／必要な情報を収集する他の方法）が必要かつ適切であるかどうかを評価しなければならない。検査の結果を受けて、管理者は処理者に対して、識別された欠陥やギャップを是正するなどの後続措置を講じることを要求できるようにする必要がある。[66] 同様に、処理者および管理者による下位処理者の検査に関して、特定の手順を確立する必要がある（下記、サブセクション1.6を参照[67]）。

145. The issue of the allocation of costs between a controller and a processor concerning audits is not covered by the GDPR and is subject to commercial considerations. However, Article 28 (3)(h) requires that the contract include an obligation for the processor to make available all information necessary to the controller and an obligation to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. This means in practice that parties should not insert in the contract clauses envisaging the payment of costs or fees that would be clearly disproportionate or excessive, thus having a dissuasive effect on one of the parties. Such clauses would indeed imply that the rights and obligations set out in Article 28(3)(h) would never be exercised in practice and would become purely theoretical whereas they form an integral part of the data protection safeguards envisaged under Article 28 GDPR.

監査に関する管理者と処理者の間の費用配分の問題は、GDPRでは言及されていないため、商業的な考慮が必要となりる。しかし、第28条第3項(h)では、処理者が管理者に必要なすべての情報を提供する義務と、管理者または管理者が委任した別の監査人が行う検査を含む監査を許容し、それに貢献する義務を契約に含めることを求めている。これは実際には、明らかに不釣り合いまたは過剰であるために当事者の一方に抑制的な効果をもたらす費用または手数料の支払いを想定した条項を当事者が契約書に挿入すべきではないことを意味する。このような条項は、第28条第3項(h)に定められた権利および義務

が実際には行使されず、純粋に理論的なものになることを意味するが、これらはGDPR第28条で想定されているデータ保護の保護手段の不可欠な部分を形成している。

1.4 Instructions infringing data protection law
データ保護法を侵害する指示

146. According to Article 28(3), the processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

第28条第3項によれば、処理者は、指示がGDPR又は他のEU又は加盟国のデータ保護規定に違反していると判断した場合、直ちに管理者に通知しなければならない。

147. Indeed, the processor has a duty to comply with the controller's instructions, but it also has a general obligation to comply with the law. An instruction that infringes data protection law seems to cause a conflict between the aforementioned two obligations.

実際に、処理者には管理者の指示に従う義務があるが、法律を遵守する一般的な義務もある。データ保護法に違反する指示は、前述の二つの義務の間に矛盾を生じさせるように思われる。

148. Once informed that one of its instructions may be in breach of data protection law, the controller will have to assess the situation and determine whether the instruction actually violates data protection law.

指示の一つがデータ保護法に違反している可能性があると通知された場合、管理者は状況を評価し、その指示が実際にデータ保護法に違反しているかどうかを判断しなければならないこととなる。

149. The EDPB recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction sent by the processor and in case of inaction from the controller in this context. One example would be to insert a clause on the termination of the contract if the controller persists with an unlawful instruction. Another example would be a clause on the possibility for the processor to suspend the implementation of the affected instruction until the controller confirms, amends or withdraws its instruction.[68]

[68] See EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, paragraph 39.

EDPBは、当事者に対し、処理者から送付された侵害する指示の通知によって生じる結果、及び、この文脈における管理者の不作為の場合について交渉し、契約において合意することを勧告する。一例としては、管理者が違法な指示に固執した場合、契約の終了に関する条項を挿入することである。他の例としては、管理者がその命令を確認、修正、または撤回するまで、処理者が影響を受ける命令の実施を中断する可能性に関する条項が挙げられる。[68]

1.5 Processor determining purposes and means of processing
取扱いの目的及び手段を決定する処理者

150. If the processor infringes the Regulation by determining the purposes and means of processing, it shall be considered as a controller in respect of that processing (Article 28(10) GDPR).

処理者が取扱いの目的及び手段を決定することによりGDPRに違反する場合、処理者は、当該取扱いとの関係においては、管理者とみなされる（GDPR第28条第10項）。

1.6 Sub-processors
復処理者

151. Data processing activities are often carried out by a great number of actors, and the chains of subcontracting are becoming increasingly complex. The GDPR introduces specific obligations that are triggered when a (sub-)processor intends to engage another player, thereby adding another link to the chain, by entrusting to it activities requiring the processing of personal data. The analysis of whether the service provider acts as a sub-processor should be carried out in line with what described above on the concept of processor (see above paragraph 83).

データ取扱活動は、しばしば、多数の行為者によって実行され、委託の連鎖はますます複雑になっている。GDPRは、(復)処理者が別のプレーヤーを業務に従事させようとしそれによって当該連鎖に別のリンクを追加しようとするときに発動される特定の義務を導入している。サービス・プロバイダーが、復処理者としてみなされるかどうかは、処理者のの概念について上述した内容に沿って分析する必要がある（上記、第83段落を参照）。

152. Although the chain may be quite long, the controller retains its pivotal role in determining the purpose and means of processing. Article 28(2) GDPR stipulates that

[68] 管理者と処理者間の標準契約条項に関するEDPBとEDPSの共同意見書01/2021、第39段落を参照。

the processor shall not engage another processor without prior specific or general written authorisation of the controller (including in electronic form). In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In both cases, the processor must obtain the controller's authorisation in writing before any personal data processing is entrusted to the sub-processor. In order to make the assessment and the decision whether to authorise subcontracting, a list of intended sub-processors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor.[69]

その連鎖は非常に長い場合があるが、管理者は、取扱いの目的及び手段の決定において極めて重要な役割を保持している。GDPR第28条第2項は、管理者から事前に書面による特定の承認又は書面 (電子形式を含む)による全般的な承認のない状況で、別の処理者を業務に従事させてはならないと規定している。書面による全般的な承認の場合、処理者は、管理者に対し、別の処理者の追加又は交代に関する変更の予定がある場合これを通知し、それによって、管理者に、そのような変更に対して異議を唱える機会が与えなければならない。いずれの場合も、処理者は、個人データの取扱いが復処理者に委託される前に、管理者の書面による承認を得なければならない。再委託を承認するかどうかの評価及び決定を行うため、処理者はデータ管理者に、予定された復処理者のリスト(各復処理者の場所、彼らが行う内容及びどのような保護措置が講じられているかの証明を含む)を提供しなければならない。[69]

153. The prior written authorisation may be specific, i.e. referring to a specific sub-processor for a specific processing activity and at a specific time, or general. This should be specified in the contract or other legal act that governs the processing.

事前の書面による承認は、特定的である場合(すなわち、特定の取扱活動のための特定の復処理者及び特定の時間に言及する場合)も、あるいは、全般的である場合もある。これは、取扱いを規律する契約又はその他の法律行為に明記する必要がある。[69]

---

[69] This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.

この情報は、管理者がGDPRの第24条のアカウンタビリティの原則並びに第28条第1項、第32条及び第5章の規定を遵守できるようにするために必要である。

154. In cases where the controller decides to accept certain sub-processors at the time of the signature of the contract, a list of approved sub-processors should be included in the contract or an annex thereto. The list should then be kept up to date, in accordance with the general or specific authorisation given by the controller.

契約の締結時に管理者が一定の復処理者を受け入れることを決定した場合、承認された復処理者のリストを契約又はその別紙に含めるべきである。そのリストは、管理者によって与えられた全般的な承認又は特定的な承認に従って、最新の状態に保たれるべきである。

155. If the controller chooses to give its **specific authorisation**, it should specify in writing which sub- processor and what processing activity it refers to. Any subsequent change will need to be further authorised by the controller before it is put in place. If the processor's request for a specific authorisation is not answered to within the set timeframe, it should be held as denied. The controller should make its decision to grant or withhold authorisation taking into account its obligation to only use processors providing "sufficient guarantees" (see sub-section 1.1 above[70]).

管理者が**特定的な承認**を与えることを選択した場合、いずれの復処理者及び取扱活動を意味しているかを、書面により明記すべきである。その後の変更は、それが実施される前に管理者による更なる承認が必要となろう。特定的な承認に係る処理者の要請が設定された時間枠内に応答されない場合、それは拒否されたものとされるべきである。管理者は、「十分な保証」を提供する処理者のみを使用するという義務を考慮の上、承認を与えるか保留するかを決定すべきである(上記、サブセクション1.1を参照[70])。

156. Alternatively, the controller may provide its **general authorisation** to the use of sub-processors (in the contract, including a list with such sub-processors in an annex thereto), which should be supplemented with criteria to guide the processor's choice (e.g., guarantees in terms of technical and organisational measures, expert knowledge, reliability and resources).[71] In this scenario, the processor needs to inform the controller in due time of any intended addition or replacement of sub-

[70] See Part II –sub–section 1.1 ("Choice of the processor").
第2部サブセクション1.1 (「処理者の選択」)を参照。

[71] This duty of the controller stems from the accountability principle in Article 24 and from the obligation to comply with provisions of Articles 28(1), 32 and Chapter V of the GDPR.
管理者のこの義務は、GDPRの第24条のアカウンタビリティの原則並びに第28条第1項、第32条及び第5章の規定を遵守する義務に起因する。

processor(s) so as to provide the controller with the opportunity to object.

あるいは、管理者は、復処理者の使用に対する**全般的な承認**を（契約において、契約の別紙にそのような復処理者のリストを記載することにより）提供することができる。これは、処理者の選択の指針となる基準（例：技術的及び組織的措置、専門家の知識、信頼性及びリソースに関する保証）により補完されるべきである。[71] このシナリオでは、処理者は、異議を唱える機会を管理者に提供するため、復処理者の追加又は交代の予定がある場合これを適時に管理者に通知する必要がある。

157. Therefore, the main difference between the specific authorisation and the general authorisation scenarios lies in the meaning given to the controller's silence: in the general authorisation situation, the controller's failure to object within the set timeframe can be interpreted as authorisation.

したがって、特定的な承認と全般的な承認のシナリオの主な違いは、管理者の沈黙に与えられた意味にある。全般的な承認の状況においては、管理者が設定された時間枠内に異議を唱えなかった場合、承認と解釈され得る。

158. In both scenarios, the contract should include details as to the timeframe for the controller's approval or objection and as to how the parties intend to communicate regarding this topic (e.g. templates). Such timeframe needs to be reasonable in light of the type of processing, the complexity of the activities entrusted to the processor (and the sub-processors) and the relationship between the parties. In addition, the contract should include details as to the practical steps following the controller's objection (e.g. by specifying time frame within which the controller and processor should decide whether the processing shall be terminated).

いずれのシナリオにおいても、契約には、管理者の承認又は異議申立ての時間枠、及び、この議題に関する当事者による意思疎通方法（テンプレートなど）に関する詳細を含める必要がある。このような時間枠は、取扱いの種類、処理者（及び復処理者）に委託された活動の複雑さ及び当事者間の関係に照らして合理的である必要がある。更に、契約書には、管理者の異議申し立て後の具体的な手順を記載する必要がある （例えば、管理者と処理者が処理を中止するかどうかを決定する期間を指定する等）。

159. Regardless of the criteria suggested by the controller to choose providers, the processor remains fully liable to the controller for the performance of the sub-processors' obligations (Article 28(4) GDPR). Therefore, the processor should ensure

it proposes sub-processors providing sufficient guarantees.

管理者がプロバイダを選択するために提案した基準に関わらず、処理者は、復処理者による義務の履行につき管理者に対して責任を全面的に負う（GDPR第28条第4項）。そのため、処理者は十分な保証を提供する復処理者を提案することを保証する必要がある。

160. Furthermore, when a processor intends to employ an (authorised) sub-processor, it must enter into a contract with it that imposes the same obligations as those imposed on the first processor by the controller or the obligations must be imposed by another legal act under EU or Member State law. The whole chain of processing activities needs to be regulated by written agreements. Imposing the “same” obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same. This also means that if the processor entrusts the sub-processor with a specific part of the processing, to which some of the obligations cannot apply, such obligations should not be included “by default” in the contract with the sub-processor, as this would only generate uncertainty. As an example, as to assistance with data breach related obligations, notification of a data breach by a sub-processor directly to the controller could be done if all three agree. However, in the case of such direct notification the processor should be informed and get a copy of the notification.

さらに、処理者が（承認された）復処理者を雇用する意向である場合、処理者が、管理者が最初の処理者に課した義務と同様の義務を課す契約を復処理者と締結するか、または、当該義務は、EU又は加盟国の法律に基づく別の法律行為によって課されなければならない。取扱活動の連鎖の全体は、書面による合意によって規制される必要がある。「同様の」義務を課すことは、形式的にではなく機能的に解釈されるべきである。契約に、管理者と処理者の間の契約で使用されているものとまったく同一の文言を含める必要はないが、その義務が実質的に同様であることを確保すべきである。これは、また、処理者が、取扱いの特定の部分を復処理者に委託し、これに一部の義務が適用できない場合、そのような義務を復処理者との契約に「デフォルトで」含めるべきでないことも意味する。不確実性を生み出すのみであるからである。例として、データ違反関連の義務の支援については、3者が合意すれば、復処理者が管理者に直接データ違反を通知することができる。ただし、そのような通知は、処理者にも通知し、通知のコピーを入手する必要がある。

2. CONSEQUENCES OF JOINT CONTROLLERSHIP

共同管理により生じる影響

2.1 Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR

GDPRに定める義務を遵守するための共同管理者のそれぞれの責任を透明性のある態様で決定

161. Article 26(1) of the GDPR provides that joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the Regulation.

GDPRの第26条第1項は、共同管理者は、GDPRに定める義務を遵守するためのそれぞれの責任を透明性のある態様で決定し、合意しなければならないと規定している。

162. Joint controllers thus need to set "who does what" by deciding between themselves who will have to carry out which tasks in order to make sure that the processing complies with the applicable obligations under the GDPR in relation to the joint processing at stake. In other words, a distribution of responsibilities for compliance is to be made as resulting from the use of the term "*respective*" in Article 26(1). This does not preclude the fact that EU or Member State law may already set out certain responsibilities of each joint controller. Where this is the case, the joint controller arrangement should also address any additional responsibilities necessary to ensure compliance with the GDPR that are not addressed by the legal provisions.[72]

したがって、共同管理者は、その取扱いが、問題となっている共同取扱いに関連してGDPRが定める適用義務を遵守していることを確保するため、誰がどの業務を行うかを管理者間で決定することにより、「誰が何をするか」を設定する必要がある。言い換えれば、遵守に係る責任の分配は、第26条第1項の「*それぞれの*」という用語が使用されていることにより行われることになる。 これは、EU法又は加盟国の国内法が、共同管理者の特定の責任を定めている場合があることを排除するものではない。このような場合、共同管理者の

[72] "In any event, the joint controller arrangement should comprehensively address all of the responsibilities of the joint controllers, including those which may have already been set out in the relevant EU or Member State law and without prejudice to the obligation of joint controllers to make available the essence of the joint controller arrangement in accordance with Article 26(2) GDPR."
「いずれにしても、共同管理者の取り決めは、関連するEU又は加盟国の国内法で既に定められている可能性があるものも含めて、共同管理者の全ての責任を包括的に取扱うべきであり、GDPR第26条第2項に従って共同管理者の取り決めの要素を公開する共同管理者の義務を損なうものではない。」

取り決めでは、法律上の規定では対処できないGDPRの遵守を確保するために必要な追加の責任についても対処する必要がある。[72]

163. The objective of these rules is to ensure that where multiple actors are involved, especially in complex data processing environments, responsibility for compliance with data protection rules is clearly allocated in order to avoid that the protection of personal data is reduced, or that a negative conflict of competence lead to loopholes whereby some obligations are not complied with by any of the parties involved in the processing. It should be made clear here that all responsibilities have to be allocated according to the factual circumstances in order to achieve an operative agreement. The EDPB observes that there are situations occurring in which the influence of one joint controller and its factual influence complicate the achievement of an agreement. However, those circumstances do not negate the joint controllership and cannot serve to exempt either party from its obligations under the GDPR.

これらのルールの目的は、とりわけ、複雑なデータが取り扱われる環境下で複数の行為者が関与する場合において、個人データの保護が低下することを回避するため、又は、否定的な権限の対立が抜け穴につながり一部の義務が取扱いに関与する当事者のいずれによっても遵守されなくなることを回避するため、データ保護ルールの遵守に係る責任が明確に割り当てられることを確保することである。ここで明確にしておかなければならないのは、運用上の合意を達成するため、全ての責任を実際の状況に応じて割り当てなければならいということである。EDPBは、共同管理者の影響力とその事実上の影響力によって、合意の達成が複雑になる状況が発生していることを認めている。しかし、そのような状況は共同管理を行っていることを否定するものではなく、一方の当事者がGDPRに基づく義務を免除する役割を果たすことはできない。

164. More specifically, Article 26(1) specifies that the determination of their respective responsibilities (i.e. tasks) for compliance with the obligations under the GDPR is to be carried out by joint controllers "*in particular*" as regards the exercising of the rights of the data subject and the duties to provide information referred in Articles 13 and 14, unless and in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

より具体的には、第26条第1項は、GDPRに定める義務の遵守に係る管理者のそれぞれの責任（例：職務）の決定は、管理者のそれぞれの責任が、管理者が服するEU法又は加盟国の国内法により決定されない場合に、またその限りにおいて、「*とりわけ*」データ主

体の権利の行使、並びに、第13条及び第14条に規定する情報提供の義務に関しては、共同管理者によって履行されるべきことを明記している。

165. It is clear from this provision that joint controllers need to define who respectively will be in charge of answering to requests when data subjects exercise their rights granted by the GDPR and of providing information to them as required by Articles 13 and 14 of the GDPR. This only refers to defining in their internal relationship which of the parties is obligated to respond to which data subjects' requests. . Regardless of any such arrangement, the data subject may contact either of the joint controllers in accordance with Article 26 (3) GPDR. However, the use of the terms "*in particular*" indicates that the obligations subject to the allocation of responsibilities for compliance by each party involved as referred in this provision are non-exhaustive. It follows that the distribution of the responsibilities for compliance among joint controllers is not limited to the topics referred in Article 26(1) but extends to other controller's obligations under the GDPR. Indeed, joint controllers need to ensure that the whole joint processing fully complies with the GDPR.

共同管理者は、データ主体がGDPRによって付与された権利を行使する際の要求への回答や、GDPRの第13条及び第14条で要求される彼らへの情報提供をそれぞれ誰が担当するか、を定める必要があることがこの規定から明らかである。これは、内部の関係において、誰がデータ主体の要求に対応する義務があるかを定義することを意味する。このような取り決めに関わらず、データ主体は、GDPR第26条第3項に基づいて共同管理者のいずれかに連絡することができる。しかしながら、「*とりわけ*」という用語の使用は、この条項で言及されている、関係する個々の当事者の遵守に係る責任の割り当ての対象となる義務が網羅的ではないことを示している。したがって、共同管理者間における遵守に係る責任の分配は、第26条第1項で規定されている議題に限定されず、GDPRに定める他の管理者の義務にも及ぶ。実際、共同管理者は、共同取扱い全体がGDPRを完全に遵守することを確保する必要がある。

166. In this perspective, the compliance measures and related obligations joint controllers should consider when determining their respective responsibilities, in addition to those specifically referred in Article 26(1), include amongst others without limitation:

この観点から、共同管理者がそれぞれの責任を決定する際に考慮すべき遵守措置及び関連する義務には、第26条第1項で具体的に言及されているものに加え、以下のもの

が含まれるが、これらに限定されない。

- Implementation of general data protection principles (Article 5)
  一般データ保護原則の実施（第5条）
- Legal basis of the processing[73] (Article 6)
  取扱いの法的根拠[73]（第6条）
- Security measures (Article 32)
  安全管理措置（第32条）
- Notification of a personal data breach to the supervisory authority and to the data subject[74] (Articles 33 and 34)
  監督機関及びデータ主体に対する個人データ侵害の通知[74]（第33条及び第34条）
- Data Protection Impact Assessments (Articles 35 and 36)[75]
  データ保護影響評価（第35条及び36条）[75]
- The use of a processor (Article 28)
  処理者の使用（第28条）
- Transfers of data to third countries (Chapter V)
  第三国へのデータの移転（第5章）
- Organisation of contact with data subjects and supervisory authorities
  データ主体及び監督機関との連絡の整理

---

[73] Although the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal basis for a particular purpose.
GDPRは、共同管理者が実行する取扱業務ごとに異なる法的根拠を使用することを排除していないが、可能な場合は、常に、特定の目的には同一の法的根拠を使用することが推奨される。

[74] Please also see EDPB guidelines on Personal data breach notification under Regulation 2016/679, WP250.rev.01 which provide that joint controllership will include "*determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations*"(p.13).
共同管理者による決定には「*第33条及び第34条に定める義務の遵守に係る責任をどの当事者が負うかを決定することが含まれ、第29条作業部会は、共同管理者間の契約上の取決めには、GDPRの侵害通知義務の遵守を主導するか、又は責任を負う管理者を決定する規定を含めることを推奨する*」とする「*規則2016/679に定める個人データ侵害通知に関するEDPBガイドライン*」、WP250.rev.01（p.13）も参照。

[75] Please also see EDPB guidelines on DPIAs, WP248.rev01 which provide the following: "*When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities*" (p.7).
DPIAに関するEDPBのガイドライン、WP248.rev01は次のように定めているので参照されたい。「*取扱業務に共同管理者が関与する場合、彼らはそれぞれの義務を正確に定義する必要がある。彼らのDPIAは、リスクを処理し、データ主体の権利及び自由を保護するために設計された様々な措置に責任を負う当事者を定めるべきである。各データ管理者は、秘密を損なうことなく（例：企業秘密、知的財産、機密の事業情報の保護）、又は、脆弱性を開示することなく、自らの必要性を表明し、有用な情報を共有すべきである*」（p.7）。

167. Other topics that could be considered depending on the processing at stake and the intention of the parties are for instance the limitations on the use of personal data for another purpose by one of the joint controllers. In this respect, both controllers always have a duty to ensure that they both have a legal basis for the processing. Sometimes, in the context of joint controllership, personal data are shared by one controller to another. As a matter of accountability, each controller has the duty to ensure that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.[76]

問題となっている取扱い及び当事者の意図に応じて検討され得る他の議題は、例えば、共同管理者のうちの1人による、別の目的での個人データの利用の制限である。この点において、双方の管理者には、常に、双方が取扱いの法的根拠を有していることを確保する義務がある。時には、共同管理の文脈において、個人データが一の管理者から別の管理者に共有される。アカウンタビリティの問題として、個々の管理者には、データを共有する管理者によって当初に収集された目的と矛盾する態様でデータが更に取り扱われないよう確保する義務がある。[76]

168. Joint controllers can have a certain degree of flexibility in distributing and allocating obligations among them as long as they ensure full compliance with the GDPR with respect of the given processing. The allocation should take into account factors such as, who is competent and in a position to effectively ensure data subject's rights as well as to comply with the relevant obligations under the GDPR. The EDPB recommends documenting the relevant factors and the internal analysis carried out in order to allocate the different obligations. This analysis is part of the documentation under the accountability principle.

共同管理者は、所与の取扱いに関してGDPRへの完全な遵守を確保する限り、彼らの間での義務の分配及び割り当てに、ある程度の柔軟性を持つことができる。割り当てにお

[76] Each disclosure by a controller requires a lawful basis and assessment of compatibility, regardless of whether the recipient is a separate controller or a joint controller. In other words, the existence of a joint controller relationship does not automatically mean that the joint controller receiving the data can also lawfully process the data for additional purposes which are beyond the scope of joint control.
管理者による個々の開示には、取得者が別個の管理者であるか共同管理者の一方であるかに関係なく、適法な根拠及び適合整合性の評価が要求される。言い換えれば、共同管理者の関係が存在するからといって、データを受け取る共同管理者が、共同管理の範囲を超える追加の目的でデータを適法に取り扱うこともできることを自動的に意味するわけではない。

いては、誰がデータ主体の権利を効果的に確保するほか、GDPRに定める関連する義務を遵守する能力を有し、かつ、その立場にあるかなどの要素を考慮に入れるべきである。EDPBは、関連する要素及び様々な義務を割り当てるために実行された内部分析を文書化することを勧告する。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。

169. The obligations do not need to be equally distributed among the joint controllers. In this respect, the CJEU has recently stated that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*".[77] However, there may be cases where not all of the obligations can be distributed and all joint controllers may need to comply with the same requirements arising from the GDPR, taking into account the nature and context of the joint processing. For instance, joint controllers using shared data processing tools or systems both need to ensure compliance with notably the purpose limitation principle and implement appropriate measures to ensure the security of personal data processed under the shared tools.

義務は、共同管理者間で均等に配分される必要はない。この点につき、CJEUは、最近、「*共同責任の存在は、必ずしも個人データの取扱いに関与する様々な行為者の同等の責任を意味しない*」と述べている。[77] しかしながら、共同取扱いの性質及び文脈を考慮して、全ての義務を配分できず、共同管理者全員が、GDPRから生じる同様の要件を遵守する必要がある場合がありうる。例えば、共有データ取扱ツール又はシステムを利用する共同管理者は、双方とも、特に目的制限の原則を遵守することを確保し、共有ツールで取り扱われる個人データの安全管理を確保するための適切な措置を講じる必要がある。

170. Another example is the requirement for each joint controller to maintain a record of processing activities or to designate a Data Protection Officer (DPO) if the conditions of Article 37(1) are met. Such requirements are not related to the joint processing but are applicable to them as controllers.

別の例としては、個々の共同管理者が取扱活動の記録を維持するか、第37条第1項の条件が満たされた場合にデータ保護オフィサー（DPO）を指名するという要件がある。このような要件は、共同取扱いとは関係しないが、管理者として彼らに適用される。

[77] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 43.
Wirtschaftsakademie（C-210/16、ECLI:EU:C:2018:388）の判決文、C-210/16、ECLI:EU:C:2018:388、第43段落。

2.2 Allocation of responsibilities needs to be done by way of an arrangement
責任の割り当ては、取決めによって行う必要がある。

2.2.1 Form of the arrangement
取決めの形式

171. Article 26(1) of the GDPR provides as a new obligation for joint controllers that they should determine their respective responsibilities "*by means of an arrangement between them*". The legal form of such arrangement is not specified by the GDPR. Therefore, joint controllers are free to agree on the form of the arrangement.

GDPRの第26条第1項は、共同管理者の新しい義務として、「両者間での取決めによって」それぞれの責任を決定すべきであると規定している。このような取決めの法的形式は、GDPRによって定められていない。したがって、共同管理者は、取決めの形式について自由に合意することができる。

172. In addition, the arrangement on the allocation of responsibilities is binding upon each of the joint controllers. They each agree and commit *vis-à-vis* each other on being responsible for complying with the respective obligations stated in their arrangement as their responsibility.

さらに、責任の割り当てに関する取決めは、個々の共同管理者を拘束する。各共同管理者はそれぞれ、彼らの責任として、彼らの取決めに規定されているそれぞれの義務を遵守する責任があることにつき、お互いに同意し、確約する。

173. Therefore, for the sake of legal certainty, even if there is no legal requirement in the GDPR for a contract or other legal act, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject. This would provide certainty and could be used to evidence transparency and accountability. Indeed, in case of non-compliance with the agreed allocation provided in the arrangement, its binding nature allows one controller to seek the liability of the other for what was stated in the agreement as falling under its responsibility. Also, in line with the accountability principle, the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR.

したがって、法的確実性のため、GDPRが契約又はその他の法律行為に関する法的要

件を定めていない場合においても、EDPBは、そのような取決めを、管理者が服するEU法又は加盟国の国内法の下での契約又はその他の法的拘束力のある行為などの法的拘束力のある文書の形式で行うことを勧告する。これは確実性を提供するであろうし、透明性及びアカウンタビリティを証明するために利用できるであろう。実際、取決めに規定される、合意された割り当てを遵守しなかった場合、その拘束性により、一方の管理者は、その責任に該当すると合意に記載されていることについて、他方の管理者の責任を追及することができる。また、アカウンタビリティの原則に沿って、契約又はその他の法律行為を利用することで、共同管理者はGDPRによって課せられた義務を遵守していることを証明できる。

174. The way responsibilities, i.e. the tasks, are allocated between each joint controller has to be stated in a clear and plain language in the arrangement.[78] This requirement is important as it ensures legal certainty and avoid possible conflicts not only in the relation between the joint controllers but also vis- à-vis the data subjects and the data protection authorities.

責任、すなわち職務、が個々の共同管理者間で割り当てられる方法は、取決めにおいて明確かつ分かりやすい言葉で規定されなければならない。[78] この要件は、法的確実性を確保し、共同管理者間の関係のみならず、データ主体及びデータ保護機関との関係において生じ得る対立を回避することから、この要件は重要である。

175. To better frame the allocation of responsibilities between the parties, the EDPB recommends that the arrangement also provide general information on the joint processing by notably specifying the subject matter and purpose of the processing, the type of personal data, and the categories of data subjects.

当事者間の責任の割り当てをより適切に構成するため、EDPBは、取決めにおいて、特に、取扱いの主題及び目的、個人データの種類及びデータ主体の類型を特定することにより、共同取扱いに関する一般的な情報も規定することを勧告する。

2.2.2. Obligations towards data subjects
データ主体に対する義務

[78] As stated in Recital 79 of the GDPR "*(...) the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers*".
GDPRの前文79で述べられているように、「*(...)管理者及び処理者の義務及び法的責任は、管理者が他の管理者と共同で取扱いの目的及び手段を決定する場合を含め、監督機関による監視及び監督機関の措置との関係においても、GDPRに基づく責任の明確な割り当てを必要とする*」。

176. The GDPR provides several obligations of joint controllers towards data subjects:
GDPRは、データ主体に対する共同管理者のいくつかの義務を規定している。

The arrangement shall duly reflect the respective roles and relationships of the joint controllers *vis-à- vis* the data subjects
取決めは、データ主体に対する共同管理者のそれぞれの役割及び関係を適切に反映しなければならない。

177. As a complement to what is explained above in section 2.1 of the present guidelines, it is important that the joint controllers clarify in the arrangement their respective role, "*in particular*" as regards the exercise of the rights of the data subject and their duties to provide the information referred to in Articles 13 and 14. Article 26 of the GDPR stresses the importance of these specific obligations. The joint controllers must therefore organise and agree on how and by whom the information will be provided and how and by whom the answers to the data subject's requests will be provided. Irrespective of the content of the arrangement on this specific point, the data subject may contact either of the joint controllers to exercise his or her rights in accordance with Article 26(3) as further explained below.
本ガイドラインのセクション2.1における前述を補足するものとして、共同管理者は、「*とりわけ*」データ主体の権利の行使並びにデータ主体が第13条及び第14条に規定されている情報を提供すべき義務に関し、それぞれの役割を取決めにおいて明確にすることが重要である。GDPRの第26条は、これらの特定の義務の重要性を強調している。したがって、共同管理者は、情報がどのように、また、誰によって提供されるか、及び、データ主体の要請に対する回答がどのように、また、誰によって提供されるかを整理し、合意しなければならない。この特定の点に関する取決めの内容に関わらず、以下に詳述するように、データ主体は、第26条第3項に従って、自己の権利を行使するため共同管理者のいずれかに連絡することができる。

178. The way these obligations are organised in the arrangement should "*duly*", i.e. accurately, reflect the reality of the underlying joint processing. For example, if only one of the joint controllers communicates with the data subjects for the purpose of the joint processing, such controller could be in a better position to inform the data subjects and possibly to answer their requests.
取決めにおいてこれらの義務を体系化する方法は、「*適正に*」、すなわち、正確に、基本的な共同取扱いの現実を反映すべきである。例えば、共同取扱いの目的で共同管理

者の一人のみがデータ主体と連絡を取っている場合、そのような管理者は、データ主体に通知し、場合によっては、その要求に応答することにおいて、より有利な立場にあり得る。

The essence of the arrangement shall be made available to the data subject
取決めの要点は、データ主体が利用できるようにされなければならない。

179. This provision is aimed to ensure that the data subject is aware of the "*essence of the arrangement*". For example, it must be completely clear to a data subject which data controller serves as a point of contact for the exercise of data subject rights (notwithstanding the fact that he or she can exercise his or her rights in respect of and against each joint controller). The obligation to make the essence of the arrangement available to data subjects is important in case of joint controllership in order for the data subject to know which of the controllers is responsible for what.

この規定は、データ主体が「*取決めの要点*」を認識していることを確実にすることを目的としている。例えば、(データ主体が個々の共同管理者に関して、又共同管理者に対してその権利を行使できるという事実にもかかわらず)いずれのデータ管理者がデータ主体の権利の行使において連絡先となるかが、データ主体にとって完全に明確でなければならない。共同管理の場合、取決めの要点をデータ主体が利用できるようにする義務は、データ主体がいずれの管理者が何に責任を有するかを知るために、重要である。

180. What should be covered by the notion of "*essence of the arrangement*" is not specified by the GDPR. The EDPB recommends that the essence cover at least all the elements of the information referred to in Articles 13 and 14 that should already be accessible to the data subject, and for each of these elements, the arrangement should specify which joint controller is responsible for ensuring compliance with these elements. The essence of the arrangement must also indicate the contact point, if designated.

「*取決めの要点*」の概念で何がカバーされるべきかは、GDPRでは特定されていない。EDPBは、要点は、少なくとも、データ主体がすでにアクセスできるはずである第13条及び第14条において規定されている情報の全ての要素をカバーすべきことを勧告する。また、これらの要素のそれぞれにつき、取決めは、いずれの共同管理者がこれらの要素の遵守の確保に責任を有するかを特定すべきである。取決めの要点は、指定されている場合は連絡先も示さなければならない。

181. The way such information shall be made available to the data subject is not specified.

Contrary to other provisions of the GDPR (such as Article 30(4) for the record of processing or Article 40(11) for the register of approved codes of conduct), Article 26 does not indicate that the availability should be "*upon request*" nor "*publicly available by way of appropriate means*". Therefore, it is up to the joint controllers to decide the most effective way to make the essence of the arrangement available to the data subjects (e.g. together with the information in Article 13 or 14, in the privacy policy or upon request to the data protection officer, if any, or to the contact point that may have been designated). Joint controllers should respectively ensure that the information is provided in a consistent manner.

そのような情報をデータ主体が利用できるようにする方法は特定されていない。GDPRの他の規定(取扱いの記録に関する第30条第4項又は承認された行動規範の登録簿に関する第40条第11項など)とは異なり、第26条は、利用可用性が「*要求に応じて*」であるべきことも、「*適切な手段により公に利用可能*」であるべきことも示していない。したがって、データ主体が取決めの要点を利用できるよう最も効果的な方法(例:第13条又は第14条の情報とともに、プライバシーポリシーにおいて、又は要請に応じてデータ保護オフィサーへ(存在する場合)、若しくは指定されている場合の連絡先へ)を決定するのは共同管理者である。共同管理者は、それぞれ、情報が一貫した態様で提供されることを確保すべきである。

The arrangement may designate a contact point for data subjects

取決めにより、データ主体のための連絡先を指定することができる。

182. Article 26(1) provides the possibility for joint controllers to designate in the arrangement a contact point for data subjects. Such designation is not mandatory.

第26条第1項は、共同管理者がデータ主体のための連絡先を取決めにより指定できると規定している。このような指定は必須ではない。

183. Being informed of a single way to contact possible multiple joint controllers enables data subjects to know who they can contact with regard to all issues related to the processing of their personal data. In addition, it allows multiple joint controllers to coordinate in a more efficient manner their relations and communications *vis-à-vis* data subjects.

複数の共同管理者への統一された連絡方法を通知されることで、データ主体は、自分の個人データの取扱いに関連する全ての問題に関して、誰に連絡できるかを知ることができる。さらに、それにより、複数の共同管理者が、データ主体との関係及び連絡をより効率

的に調整できる。

184. For these reasons, in order to facilitate the exercise of data subjects' rights under the GDPR, the EDPB recommends joint controllers to designate such contact point.

これらの理由から、GDPRに定めるデータ主体の権利の行使を容易にするため、EDPBは、共同管理者にそのような連絡先を指定することを勧告する。

185. The contact point can be the DPO, if any, the representative in the Union (for joint controllers not established in the Union) or any other contact point where information can be obtained.

連絡先は、存在する場合はDPO、EU域内の代理人（EU域内に拠点のない共同管理者の場合）、又は、情報が入手できるその他の連絡先とすることができる。

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers.

取決めの条件にかかわらず、データ主体は、個々の共同管理者に関して、及び、個々の共同管理者に対して、その権利を行使できる。

186. Under Article 26(3), a data subject is not bound by the terms of the arrangement and may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.

第26条第3項の規定により、データ主体は、取決めの条件に拘束されず、個々の共同データ管理者に関して、及び、個々の共同管理者に対して、GDPRに定める自らの権利を行使できる。

187. For example, in case of joint controllers established in different Member States, or if only one of the joint controllers is established in the Union, the data subject may contact, at his or her choice, either the controller established in the Member State of his or her habitual residence or place of work, or the controller established elsewhere in the EU or in the EEA.

例えば、共同管理者が異なる加盟国に拠点を有する場合、又は、共同管理者のうち一者のみがEU域内に拠点を有する場合、データ主体は、自らの選択により、自らの常居所若しくは職場がある加盟国に拠点を有する管理者、又は、EU又はEEA域内の他の場所に拠点を有する管理者に連絡することができる。

188. Even if the arrangement and the available essence of it indicate a contact point to receive and handle all data subjects' requests, the data subjects themselves may still choose otherwise.

取決め及び利用可能なその要点に、全てのデータ主体の要請を受け取り、かつ、取り扱う連絡先が示されている場合においても、データ主体自身が別の方法を選択することができる。

189. Therefore, it is important that joint controllers organise in advance in their arrangement how they will manage answers to requests they could receive from data subjects. In this respect, it is recommended that joint controllers communicate to the other controllers in charge or to the designated contact point, the requests received in order to be effectively handled. Requiring data subjects to contact the designated contact point or the controller in charge would impose an excessive burden on the data subject that would be contrary to the objective of facilitating the exercise of their rights under the GDPR.

したがって、共同管理者が、データ主体から受け取り得る要求への回答をどのように管理するかを共同管理者間の取決めにおいて事前に整理することは重要である。この点において、共同管理者は、効果的に対処するため、受け取った要求を担当の他の管理者又は指定された連絡先に連絡することが推奨される。データ主体に対して指定された連絡先又は担当の管理者に連絡することを求めることは、データ主体に過度の負担をかけることとなり、GDPRに定める彼らの権利の行使を促進するという目的に反することとなろう。

2.3 Obligations towards data protection authorities
データ保護機関に対する義務

190. Joint controllers should organise in the arrangement the way they will communicate with the competent supervisory data protection authorities. Such communication could cover possible consultation under Article 36 of the GDPR, notification of a personal data breach, designation of a data protection officer.

共同管理者は、管轄の監督データ保護機関との連絡方法を取決めにおいて整理すべきである。このような連絡には、GDPRの第36条に基づいて可能な協議に加え、個人データ侵害の通知、データ保護オフィサーの指名が含まれ得る。

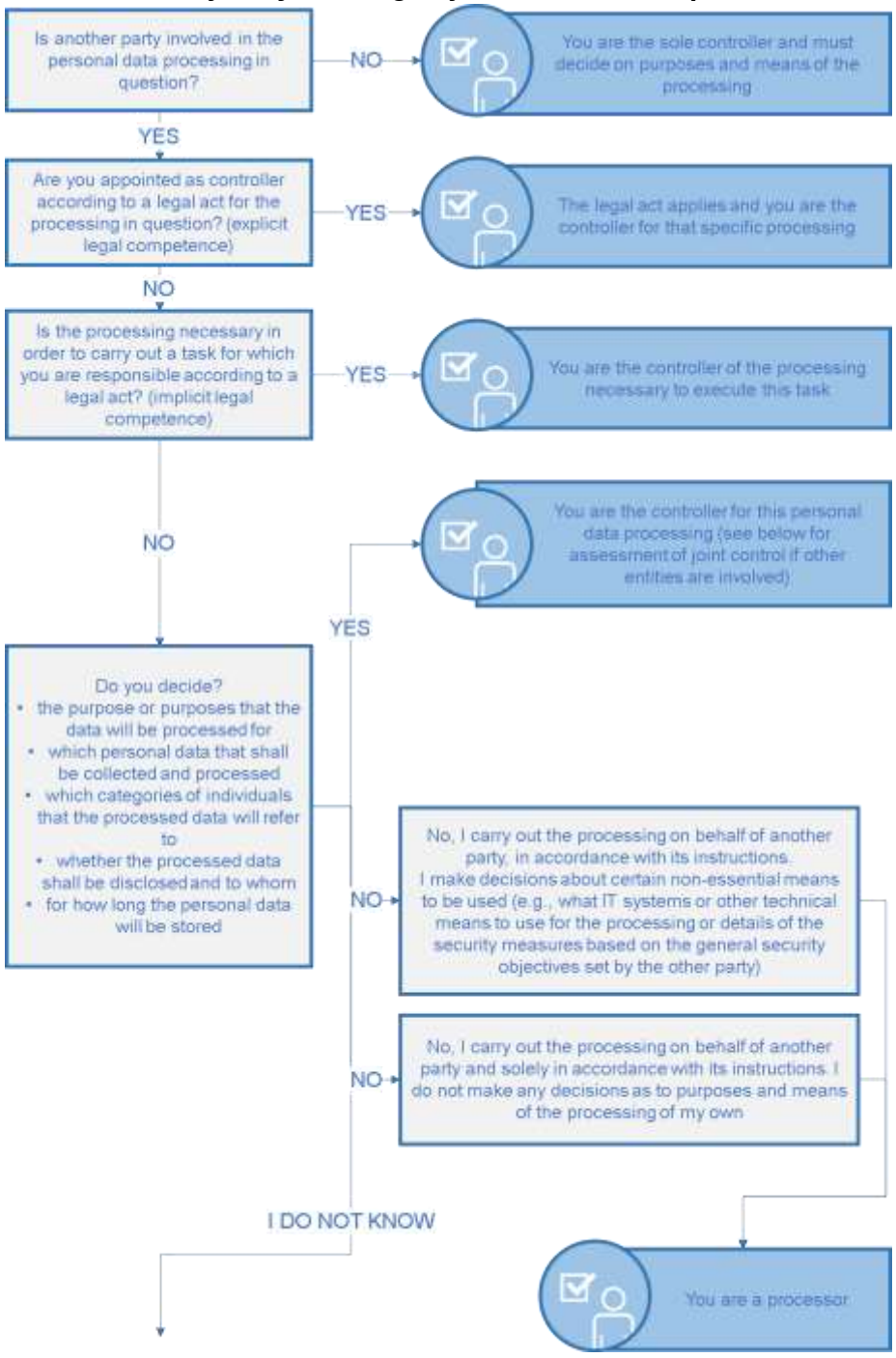
191. It should be recalled that data protection authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint

controllers or the designated contact point. Therefore, the authorities can contact any of the joint controllers to exercise their powers under Article 58 with respect to the joint processing.

データ保護機関は、共同管理者としての当事者の適格性の問題であれ、指定された連絡先の問題であれ、取決めの条件には拘束されないことを想起すべきである。したがって、当該機関は、共同取扱いに関して第58条に定める権限の行使に当たり、いずれの共同管理者にも連絡することができる。

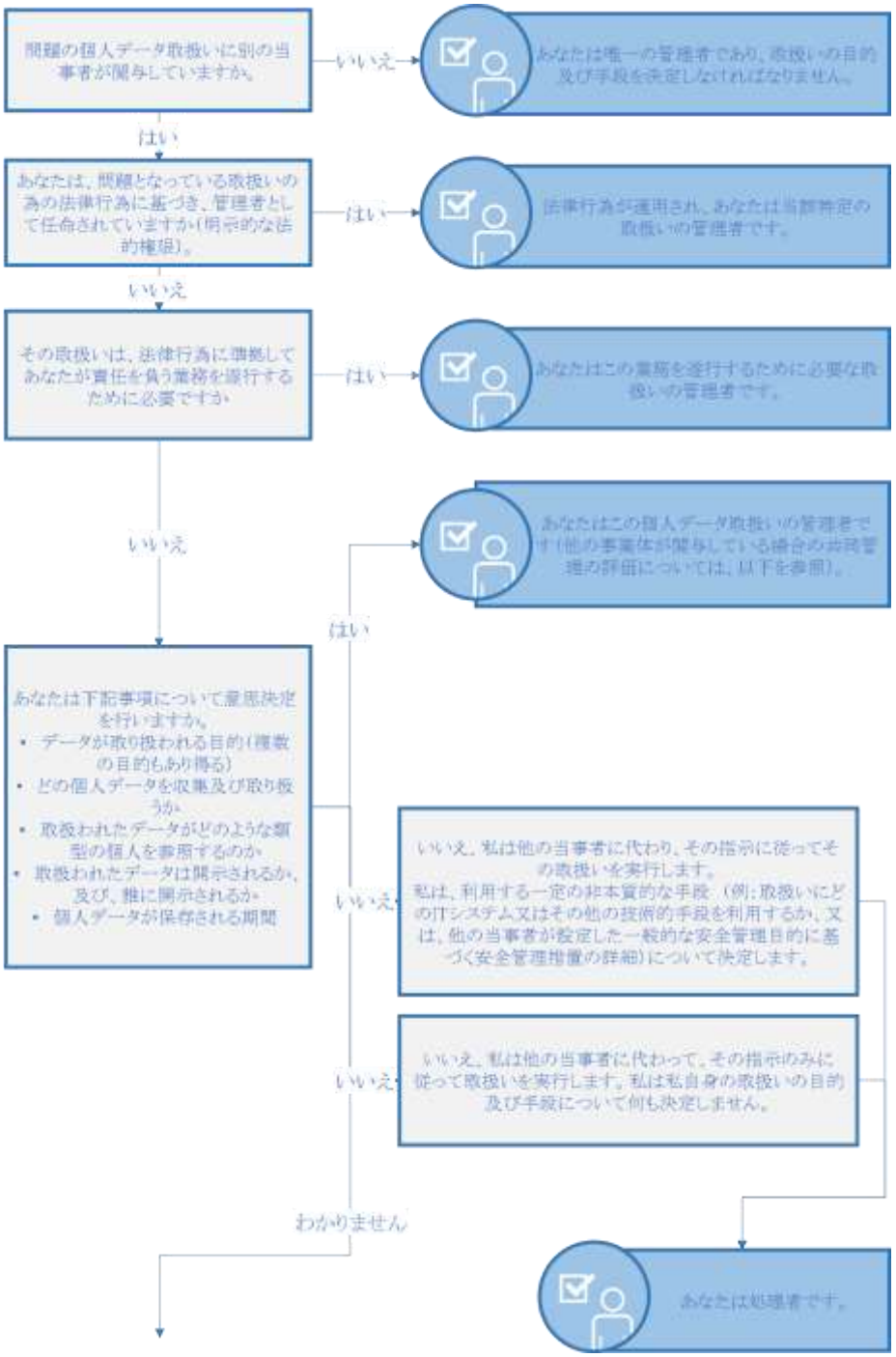
Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice

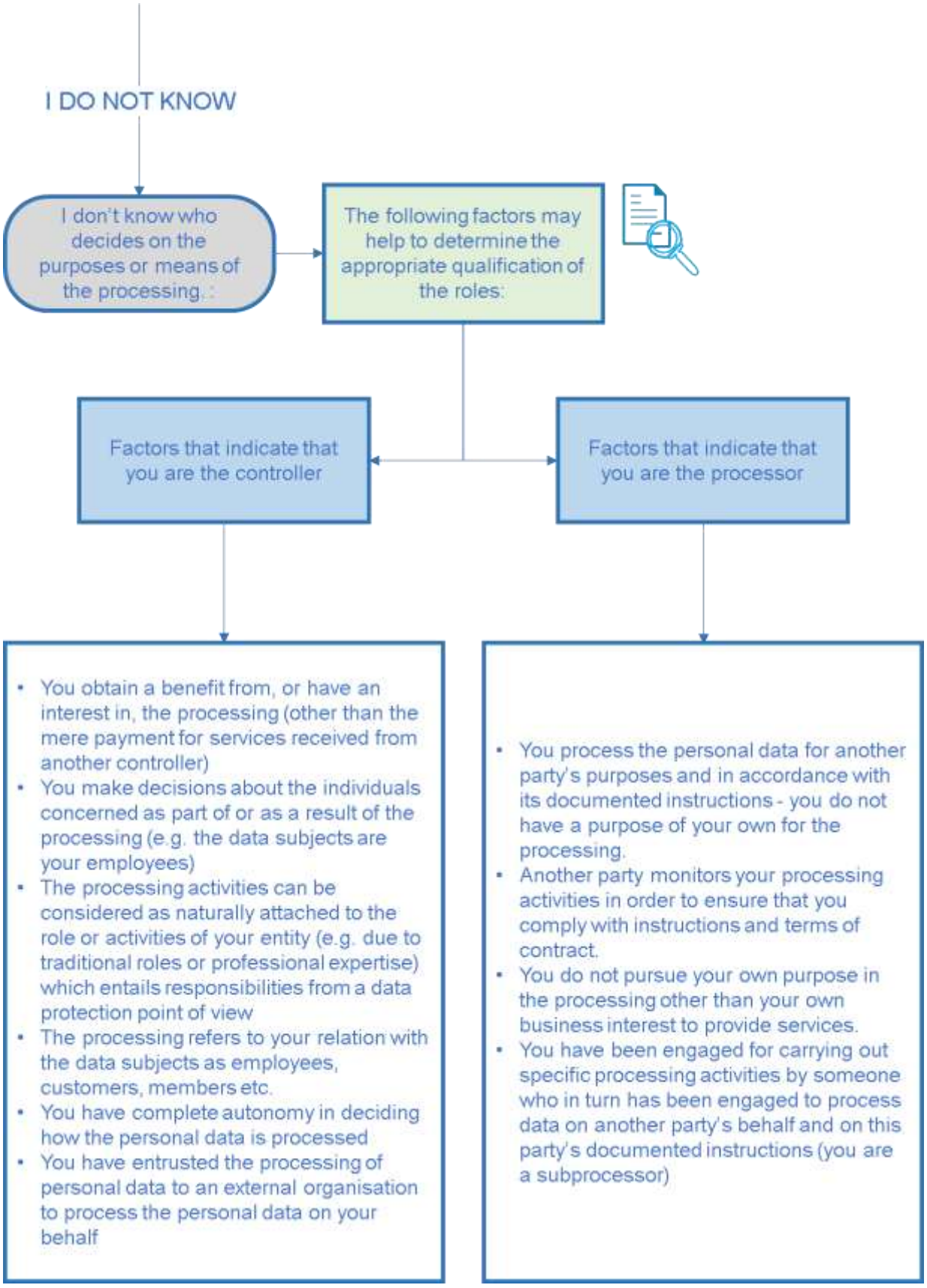
Note: in order to properly assess the role of each entity involved, one must first identify the specific personal data processing at stake and its exact purpose. If multiple entities are involved, it is necessary to assess whether the purposes and means are determined jointly, leading to joint controllership.

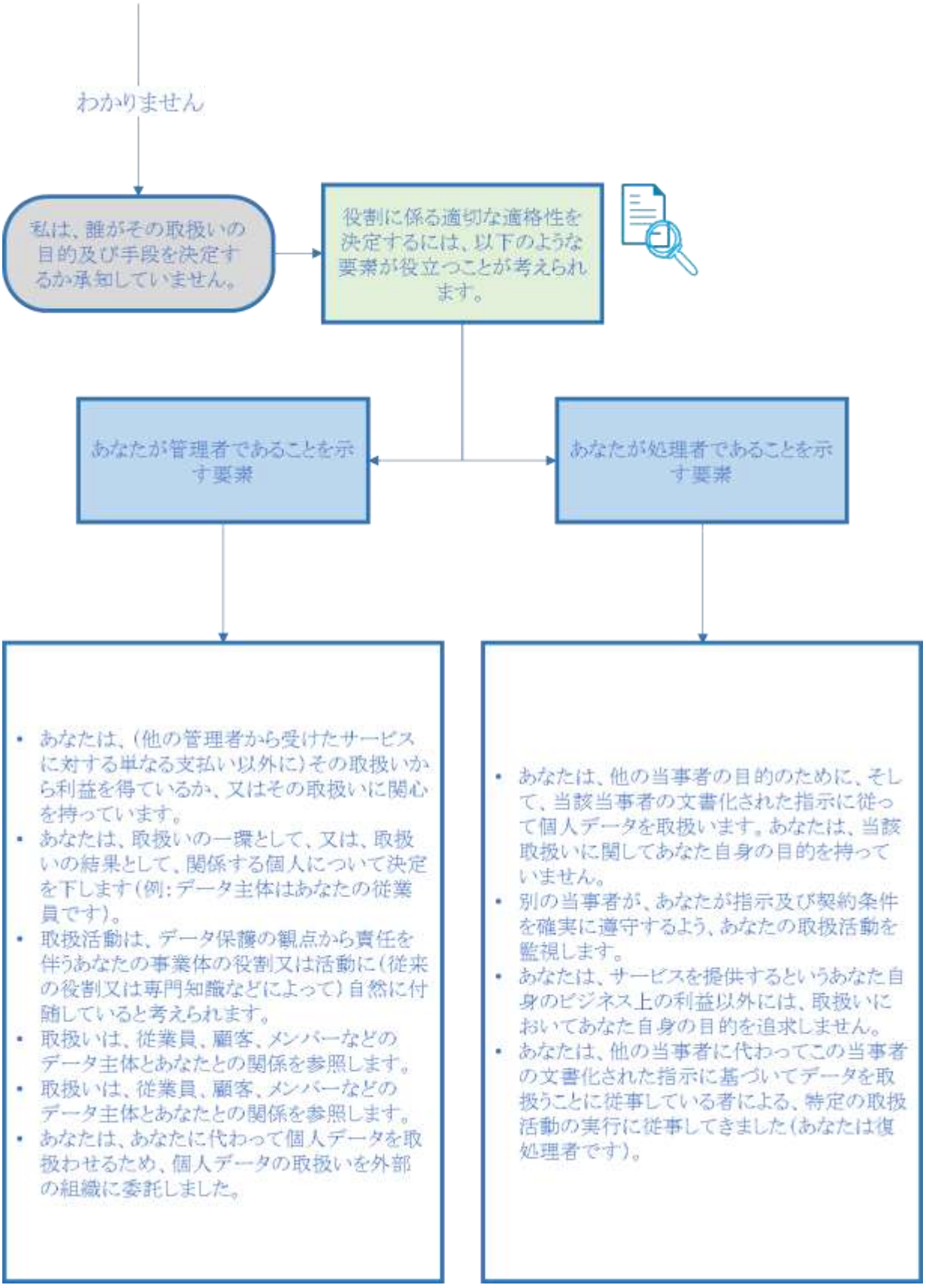


別紙 I – 管理者、処理者及び共同管理者の概念を実務に適用するためのフローチャート

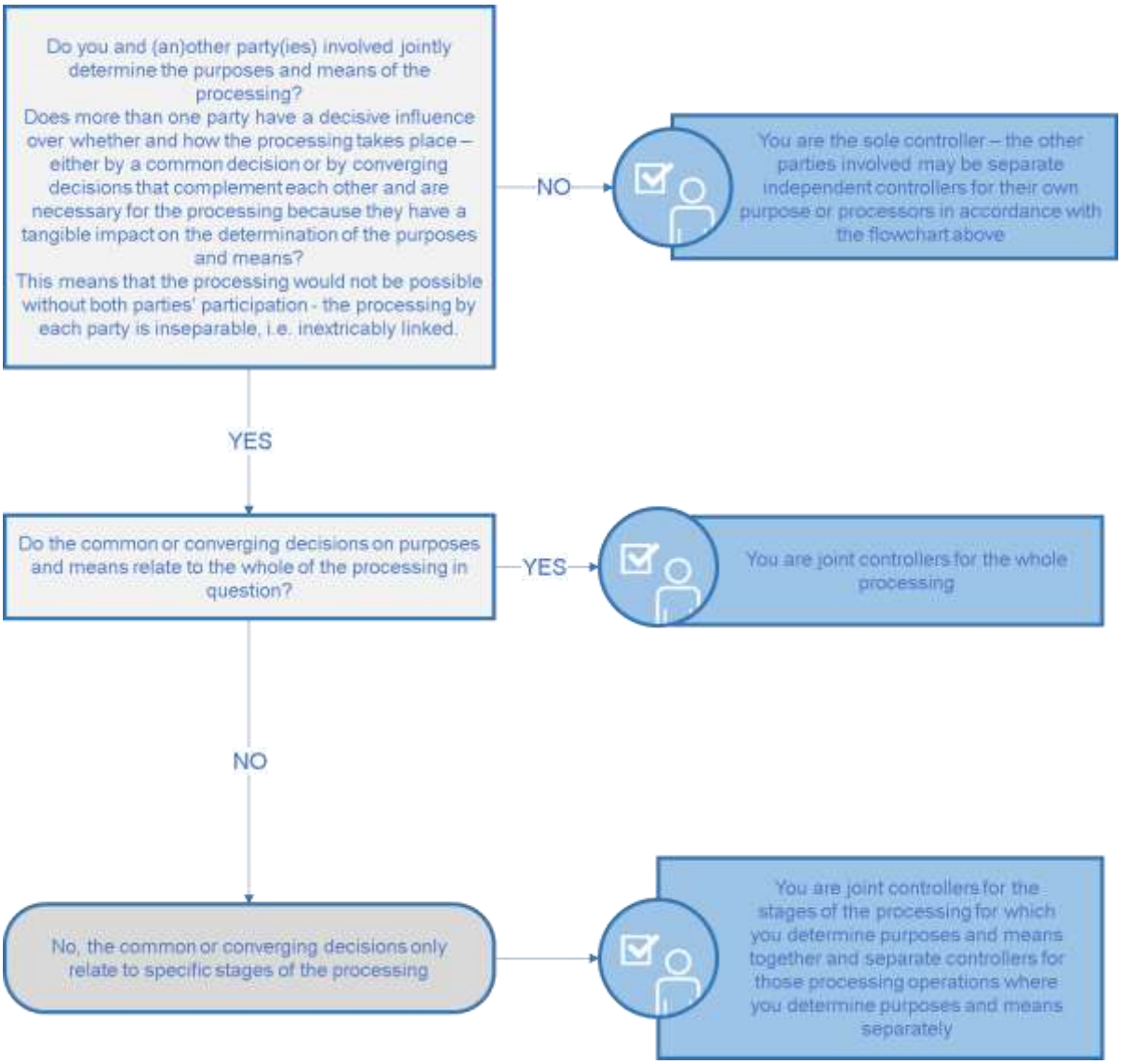
注:関係する個々の主体の役割を適切に評価するため、まず、問題となっている特定の個人データ取扱い及びその正確な目的を識別しなければならない。複数の主体が関与している場合は、共同管理につながる目的及び手段が共同で決定されているかどうかを評価する必要がある。




I DO NOT KNOW
I don't know who decides on the purposes or means of the processing. :
The following factors may help to determine the appropriate qualification of the roles:
Factors that indicate that you are the controller
Factors that indicate that you are the processor
• You obtain a benefit from, or have an interest in, the processing (other than the mere payment for services received from another controller)
• You make decisions about the individuals concerned as part of or as a result of the processing (e.g. the data subjects are your employees)
• The processing activities can be considered as naturally attached to the role or activities of your entity (e.g. due to traditional roles or professional expertise) which entails responsibilities from a data protection point of view
• The processing refers to your relation with the data subjects as employees, customers, members etc.
• You have complete autonomy in deciding how the personal data is processed
• You have entrusted the processing of personal data to an external organisation to process the personal data on your behalf
• You process the personal data for another party's purposes and in accordance with its documented instructions - you do not have a purpose of your own for the processing.
• Another party monitors your processing activities in order to ensure that you comply with instructions and terms of contract.
• You do not pursue your own purpose in the processing other than your own business interest to provide services.
• You have been engaged for carrying out specific processing activities by someone who in turn has been engaged to process data on another party's behalf and on this party's documented instructions (you are a subprocessor)


わかりません
私は、誰がその取扱いの目的及び手段を決定するか承知していません。
役割に係る適切な適格性を決定するには、以下のような要素が役立つことが考えられます。
あなたが管理者であることを示す要素
あなたが処理者であることを示す要素
• あなたは、(他の管理者から受けたサービスに対する単なる支払い以外に)その取扱いから利益を得ているか、又はその取扱いに関心を持っています。
• あなたは、取扱いの一環として、又は、取扱いの結果として、関係する個人について決定を下します(例:データ主体はあなたの従業員です)。
• 取扱活動は、データ保護の観点から責任を伴うあなたの事業体の役割又は活動に(従来の役割又は専門知識などによって)自然に付随していると考えられます。
• 取扱いは、従業員、顧客、メンバーなどのデータ主体とあなたとの関係を参照します。
• 取扱いは、従業員、顧客、メンバーなどのデータ主体とあなたとの関係を参照します。
• あなたは、あなたに代わって個人データを取扱わせるため、個人データの取扱いを外部の組織に委託しました。
• あなたは、他の当事者の目的のために、そして、当該当事者の文書化された指示に従って個人データを取扱います。あなたは、当該取扱いに関してあなた自身の目的を持っていません。
• 別の当事者が、あなたが指示及び契約条件を確実に遵守するよう、あなたの取扱活動を監視します。
• あなたは、サービスを提供するというあなた自身のビジネス上の利益以外には、取扱いにおいてあなた自身の目的を追求しません。
• あなたは、他の当事者に代わってこの当事者の文書化された指示に基づいてデータを取扱うことに従事している者による、特定の取扱活動の実行に従事してきました(あなたは復処理者です)。

Joint controllership - If you are the controller and other parties are involved in the personal data processing:



共同管理-あなたが管理者であり、他の当事者が個人データの取扱いに関与している場合：