「EU 一般データ保護規則（GDPR）」
に関わる実務ハンドブック
（第 29 条作業部会ガイドライン編）

・データ保護責任者

2018 年 2 月

日本貿易振興機構（ジェトロ）
ブリュッセル事務所
海外調査部　欧州ロシア CIS 課

2018年5月25日から適用が開始されるEUの「一般データ保護規則（General Data Protection Regulation：GDPR）」は、欧州経済領域（European Economic Area：EEA、EU加盟国28カ国、ノルウェー、アイスランド、リヒテンシュタイン）と個人データをやり取りする日本のほとんどの企業や機関・団体が適用対象となり（外交・防衛・警察などについて例外あり）、同規則への違反行為には高額の制裁金が科されるリスクもある。

ジェトロは2016年11月に、同規則の基本的な構造と基礎的な社内外の対応について概説した「実務ハンドブック（入門編）」[1]を、2017年8月に標準契約条項（Standard Contractual Clauses：SCC）と拘束的企業準則（Binding Corporate Rules：BCR）を中心とする企業のコンプライアンス対応を概説した「実務ハンドブック（実践編）」[2]を公表した。

GDPRに関するガイドラインを解説した本レポートは、同規則に詳しいギブソン・ダン・クラッチャー法律事務所ブリュッセルオフィスに委託し作成した。本レポートでは、「データ保護責任者」に関するガイドラインを2017年12月31日現在の情報を基に解説した。

[1] https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html
[2] https://www.jetro.go.jp/world/reports/2017/01/76b450c94650862a.html

目　次

はじめに

本稿は、第 29 条作業部会[3]が公表している「一般データ保護規則（GDPR）」に関するガイドラインのうち、「データ保護責任者に関するガイドライン（WP243）」（2016 年 12 月 13 日付採択、2017 年 4 月 5 日改訂）[4]の内容を解説することを目的として作成したものである。

第 29 条作業部会 が公表しているガイドラインは、制度の概要について知識を有していない読み手には必ずしも理解しやすい構成になっていないため、各章では、まずガイドラインの構成を示し、その後ガイドラインで説明されている事項のうち重要なものを必要に応じて再構成し、簡潔に概要を記載した。さらに、公表されているガイドラインの内容を概ね記載した上で実務上の論点を含む事項については、「コメント」という形で留意点を追加している。特に、DPO の選任義務は、データ保護に関わるビジネスの観点から、日本本社と欧州拠点の間における意思決定プロセスや組織関係に重要な影響を及ぼす可能性がある問題であるため、コメントとして比較的多くの記述を割くよう心掛けた。ガイドラインの内容を概ね記載することとしたのは、公表されているガイドラインは細部にわたって重要な事項を含む記述が多いことから、内容を省略せずに情報提供する方が読者の GDPR に対するより正確な理解に資すると考えたためである。もっとも、本稿もガイドラインの内容を完全に翻訳した内容ではないため、あくまで GDPR に関するガイドラインを理解するための出発点として活用頂ければ幸いである。

本稿執筆時点（2017 年 12 月 31 日）における第 29 条作業部会による GDPR に関するガイドラインの公表状況は以下の通りである。

・「データ保護影響評価に関するガイドライン（WP248）」（2017 年 4 月 4 日付採択、2017 年 10 月 4 日付改訂）[5]

・「データ侵害通知に関するガイドライン（WP250）」（2017 年 10 月 3 日付採択、2018 年 2 月 6 日採択）[6]

・「自動的決定およびプロファイリングに関するガイドライン（WP251）」（2017 年 10 月 3 日付採択、2018 年 2 月 6 日採択）[7]

・「協調型高度道路交通システム（Cooperative Intelligent Transport Systems：C-ITS）に関連する個人データ処理に関する意見書 03/2017（WP252）」（2017 年 10 月 4 日付採択）[8]

・「制裁金に関するガイドライン（WP253）」（2017 年 10 月 3 日付採択）[9]

・「十分性参照に関する作業文書（WP12 の第 1 章の更新）（WP254）」（2017 年 11 月 28 日付採択、2018 年 2 月 6 日採択）[10]

・「管理者の拘束的企業準則において記載すべき要素および原則の表を定める作業文書（WP256）」（2017 年 11 月 29 日付採択、2018 年 2 月 6 日採択）[11]

---

[3] Article 29 Working Party、EU 加盟各国の監督当局の代表、欧州委員会司法総局データ保護課の代表、欧州データ保護監察機関（EDPS）の代表によって構成される。特定の問題に関して共通の解釈と分析を提供することにより、EU 加盟国のデータ保護法の解釈にある程度の調和をもたらす。

[4] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

[5] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[6] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[7] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[8] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

[9] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

[10] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

[11] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109

「処理者の拘束的企業準則において記載すべき要素および原則の表を定める作業文書（WP257）」（2017年11月29日付採択、2018年2月6日採択）[12]

さらに、以下のガイドラインについてもパブリック・コンサルテーション（公開諮問）の手続きを実施している。

・「同意に関するガイドライン（WP259）」（2017年11月28日付採択、2018年1月23日までパブリック・コンサルテーションを実施）

・「透明性に関するガイドライン（WP260）」（2017年11月28日付採択、2018年1月23日までパブリック・コンサルテーションを実施）

・「規則2016/679（GDPR）第49条に関するガイドライン」（2018年2月6日付採択、2018年3月26日までパブリック・コンサルテーションを実施）[13]

・「認証機関の認定に関するガイドライン」（2018年2月6日付採択、2018年3月30日までパブリック・コンサルテーションを実施）[14]

さらに、第29条作業部会は、GDPRの地理的適用範囲の適用およびGDPR第30条第5項（処理行為の記録義務の例外）の解釈に関してガイドラインを作成中であり、2018年5月までにガイドラインが公表されることも期待される。

なお、本稿において「EU」は特に言及がない限り、EEA（欧州経済領域、EU加盟28カ国とノルウェー、アイスランド、およびリヒテンシュタイン）を意味するものとする。欧州委員会はEEA内のEFTA加盟国であるノルウェー、アイスランド、およびリヒテンシュタインとの間でGDPRをEEA協定書に統合する作業を速やかに行う予定であり、当該作業完了後にこれら3ヵ国においてもGDPRが適用されることとなる。

[12] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110
[13] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614232
[14] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614486

I. データ保護責任者に関するガイドラインの構成

データ保護責任者（Data Protection Officer、以下「DPO」という）に関するガイドラインは、以下の項目によって構成されている。

II. DPO の制度の概要

1. DPO の意義

DPO とは、組織内における GDPR の遵守を監視、および管理者または処理者の GDPR 遵守を支援するために、管理者または処理者によって選任されるデータ保護法およびその実務に関する専門知識を有する者のことをいう。後述する通り、DPO は、GDPR の遵守の監視に関する幅広い権限および高い独立性を有する地位にある。そのため、管理者・処理者としては、DPO の選任義務があるか、DPO を選任する場合には誰をどの拠点で選任するかを慎重に検討する必要がある。

2. DPO の業務

DPOの主たる業務はGDPRの遵守状況を監視することにある（第39条第1項(b)号）。また、DPO は、データ保護影響評価に関して助言し、監視する任務を負い（同項(c)号）、監督当局と協力し、組織における連絡先として活動する（同項(d)、(e)号）。

3. DPOの地位

管理者および処理者は、DPO が個人データの保護に関連する全ての問題において適切かつ適時に関与できる地位を確保しなければならない（第 38 条第 1 項）。DPO は、業務を遂行するにあたり、個人データおよび処理業務にアクセスし、専門知識を維持するために必要なリソース（財源、インフラ、スタッフなど）の提供による支援を受けることができる（第 38 条第 2 項）。また、DPO の地位において重要な点は、DPO が組織内で十分な独立性が確保されなければならず、自らの業務に関して他者から指揮命令を受けない地位にあることである（第 38 条第 3 項）。さらに、DPO は、自らの任務を遂行する際に管理者または処理者から解雇されること、または不利益を受けることがあってはならない（第 38 条第 3 項）。

このように、DPO は組織における個人データの保護に関連する事項について幅広く関与する権限を有すると同時に、組織の指揮命令系統に属さない極めて独立性の高い地位にある。従って、DPO のデータ保護法に関する理解、解釈の姿勢が、DPO を選任する組織の GDPR コンプライアンス体制およびデータ保護に関連するビジネスに非常に大きな影響を及ぼすことになるとともに、仮に組織のビジネスにとって不都合な GDPR の解釈を DPO が主張したとしても、DPO を解任することによって解決することは法的に認められないことになる。以上のような DPO の業務権限、地位の独立性を踏まえると、DPO を選任するか否か、DPO をどの拠点で選任するか、どのような人物を DPO として選任するかは慎重な検討を要する事項であることを理解しておく必要がある。

また、DPO は、GDPR で規定される業務以外の業務を行うことも可能であるが、当該業務が GDPR に基づく業務と利益相反を生じさせないことが必要である（第 38 条第 6 項）。従って、DPO は、組織において個人データの処理の目的および手段を決定する地位に就くことはできない。一般論として、いわゆる経営陣（例えば、最高経営責任者、最高執行責任者、最高財務責任者、最高医療責任者、マーケティング部門長、人事部門長または IT 部門長など）は利益相反が生じる地位であると考えられているが、組織構造の中でのより低い役割であってもそのような地位や役割が処理の目的や手段を決定することにつながる可能性があるため、組織構造に応じてケースバイケースで検討する必要がある。

4. DPOの選任

(1) DPOの選任義務

GDPR 第 37 条第 1 項は、以下の場合に DPO の選任義務があると規定している。

（a）処理が公的機関または公的団体によって行われる場合

（b）管理者または処理者の中核的な活動が、データ主体の定期的かつ系統的な監視を必要とする処理業務である場合

（c）管理者または処理者の中核的な活動が、特別カテゴリーの個人データならびに有罪判決および犯罪に関する個人データの大規模な処理である場合

また、EU 法または加盟国法により DPO の選任が義務付けられる場合も、GDPR に基づく DPO の選任義務があることになる（第 37 条第 4 項）。例えば、ドイツにおける新しい連邦データ保護法（2017 年 7 月 5 日成立）では、個人データの自動的処理に関して少なくとも 10 名の従業員を雇用する企業は、DPO の選任義務があると規定されている。

(2) DPO へのアクセスの容易性

事業者グループは、各拠点から容易にアクセス可能である場合には、単一の DPO のみを選任することを認めている（第 37 条第 2 項）。DPO は、必要な場合にはチームからの支援を受けながら、効率的にデータ主体および監督当局とコミュニケーションを取れなければならず、コミュニケーションはデータ主体および監督当局が使用する言語で対応する必要がある。また、DPO ガイドラインは、DPO は基本的に EU 域内に所在することを推奨しているが、管理者または処理者が EU 域内に拠点を有しない一定の状況において、DPO が EU 域外に所在することにより効果的に活動を行うことが可能となる場合があり得るとも述べている。前述の通り、DPO がデータ保護に関するコンプライアンスに関して重要な役割を果たすことに鑑みると、日本企業としては必要な支援体制を整備した上で日本本社で DPO を選任することも検討する必要がある。

5. DPO の専門性および技能

DPO は、専門家としての資質、特にデータ保護法および実務の専門知識ならびに第 39 条で規定される任務を遂行する能力に基づいて選任される必要がある（第 37 条第 5 項）。DPO は、加盟国および EU におけるデータ保護法および実務の専門性を有し、GDPR に対する深い理解を持つことが期待されている。日本企業における実情を踏まえると、日本本社で DPO を選任する場合は、GDPR 対応に関与した社内の責任者を DPO として選任し、適宜チームの支援を受けられるようにすることが考えられる。また、EU 域内の拠点で DPO を選任する場合においても、DPO の地位の重要性に鑑みて、日本本社としても DPO の人選に深く関与して慎重に検討する必要があると考えられる。

Ⅲ. データ保護責任者（DPO）に関するガイドラインの解説

1. はじめに

DPO は、多くの組織にとって GDPR の規定への遵守を促進するための新しい法的枠組みの中心となる。

第 29 条作業部会は、GDPR の採択前に、DPO は説明責任の基礎であり、DPO を選任することで遵守を促進し、さらに企業の競争性を高められると主張していた。説明責任の手段（例えば、データ保護影響評価および監査の促進または実施）の導入による遵守の促進に加え、DPO は関係する利害関係者（例えば、監督当局、データ主体、および組織の中の事業部門）の間における仲介者としての役割を担う。

GDPR は、DPO をデータに関する新たなガバナンス制度の主要な役割として認識し、選任、地位、業務の条件を定めている。当該ガイドラインの目的は、管理者と処理者の GDPR 遵守を援助するとともに、DPO の役割を支援するため、GDPR の関連条項を明確化することである。当該ガイドラインは、一部の EU 加盟国で得た経験を土台にベスト・プラクティスとして推奨すべき事項についても規定している。第 29 条作業部会は、当該ガイドラインの実施を監視し、適切であればさらに詳細な内容を追加する予定である。

2. DPO の選任

(1) 義務的選任

GDPR 第 37 条第 1 項は、以下の 3 つの特定の要件のいずれかを満たす場合に DPO の選任を要求している[15]。

第 37 条第 1 項(a)号　処理が公的機関または公的団体によって行われる場合[16]

第 37 条第 1 項(b)号　管理者または処理者の中核的な活動が、データ主体の定期的かつ系統的な監視が大規模に要求される処理行為である場合

第 37 条第 1 項(c)号　管理者または処理者の中核的な活動が、特別カテゴリーの個人データまたは有罪判決および犯罪に関連する個人データの大規模な処理である場合[17]

コメント 1 ：加盟国法に基づく DPO の選任義務

GDPR 第 37 条第 4 項は EU 加盟国の法律により DPO の選任を義務付けることができることを規定している。そのため、加盟国レベルでは、GDPR を施行するための新しいデータ保護法を制定する動きが起きている。ドイツでは 2017 年 7 月 5 日に、新しい連邦データ保護法（Bundesdatenschutzgesetz）が成立した。DPO の選任に関して、同法律は、第 38 条において、現在のドイツデータ保護法の規定を維持しており、個人データの自動的処理に関して少なくとも 10 名の従業員を雇用する企業は、DPO を選任する義務を負う旨を規定している。GDPR 上は、特定の場合においてのみ、企業に DPO の選任義務が課されている。管理者および処理者は、GDPR 第 35 条に基づくデータ保護影響評価（DPIA）が必要となる処理を行う場合、DPO を選任しなければならない。DPIA が必要となる処理には、個人データの処理が商業上のデータ移転またはマーケティングもしくは市場調査の目的で行われる場合も含まれ

[15] （原文脚注 5）第 37 条第 4 項の下では EU または加盟国の法律により、これら以外の状況でも DPO の選任を義務付けられる場合がある。

[16] （原文脚注 6）裁判所が司法権の行使を行う場合を除く。

[17] （原文脚注 9）第 10 条

る。このドイツ法上の DPO の選任義務は、GDPR 第 37 条第 4 項により GDPR 上の DPO の選任義務があることを意味する。
　このように、各加盟国のデータ保護法毎に DPO の選任義務に関する要件が異なることから、今後、GDPR を実施するための加盟国レベルのデータ保護法において DPO の選任義務がどのように規定されているかを注視しておく必要がある。

第 29 条作業部会では、組織が DPO を選任する必要がないことが明らかでない限りにおいては、関連要因が適切に考慮されたかどうかを立証できるように DPO を選任するか否かを決定する目的で実施する組織内部での分析の過程を、管理者および処理者が文書化することを推奨している[18]。この分析は説明責任の原則に基づく文書化の一部をなすものである。当該文書は監督当局によって提出を求められる場合があり、必要な場合には更新しなければならない（例えば、管理者または処理者が第 37 条第 1 項に列挙される事由に該当する可能性のある新しい活動を行う、または新しいサービスを提供する場合）。
組織が自主的に DPO を選任する場合であっても、選任が義務的である場合と同様に、選任、地位および任務には第 37 条から第 39 条の規定と同じ要件が適用される。

コメント２：DPO の自主的な選任（1）
自主的に選任された DPO についても、GDPR の監視に関する幅広い権限および高い独立性が保証される。従って、DPO の選任義務がない場合には自主的に DPO を選任することのインパクトについてよく認識した上で、DPO の選任を行う必要があり、安易に DPO を選任するべきではない。

上記は、DPO を自主的に選任することを望まず、DPO を選任することを法的に要求されていない組織が、個人データの保護に関連する任務に従事する職員または外部コンサルタントを採用することを妨げるものではない。この場合、当該人物の肩書き、地位、役職、および任務に関して混乱がないことを確認することが重要である。従って、企業内ならびにデータ保護当局、データ主体および一般市民とのやり取りにおいて個人またはコンサルタントの肩書きが「DPO」ではないことが明確にされなければならない。

コメント３：DPO の自主的な選任（2）
個人データの保護に従事する職員や外部コンサルタントを採用する場合は、DPO を任意に選任したものと間違われないよう、GDPR 上の DPO ではないことを明確にする必要がある。

①「公的機関または公的団体」
GDPR は、何が「公的機関または公的団体」の構成要件となるかを定義していない。第 29 条作業部会は、当該概念は加盟国法の下で判断されるべきだと考えている。従って、公的機関および公的団体には、加盟国、地域および地方自治体が含まれるが、適用される加盟国法の下においては、当該概念は通常、公法に基づく一連の他の団体も含まれる。その場合は、DPO の選任は義務となる。

コメント４：公的機関または公的団体の意義

[18] （原文脚注 10）第 24 条第 1 項参照

日本法上で、公的機関、公的団体、または独立行政法人とされる場合でも、加盟国法が定める公的任務を実行する、または公的権限を行使することがない限り、ここでいう「公的機関または公的団体」に該当することはないと思われる。ただし、これは日本法上で、公的機関、公的団体、または独立行政法人とされる団体が、GDPR 上の DPO の選任義務を負わないことを意味しない。GDPR 第 37 条第 1 項(b)・(c)号および同条第 4 項の各要件のいずれかを満たす場合には、これらの団体も GDPR 上の DPO の選任義務を負うことになる。

公的機関または公的団体のみが、公的任務を実行、または公的権限を行使するわけではない。その他の公法または私法に基づく各加盟国法規制に従った公的交通機関、水とエネルギー供給、道路インフラ、公共放送サービス、公営住宅または規制された専門職の自主規制団体などのセクターにおけるその他の自然人または法人も公的任務を実行、または公的権限を行使することがある[19]。

このような場合、データ主体は、データが公的機関または公的団体によって処理される場合と非常によく似た状況に置かれる可能性がある。特に、データは（公的機関または公的団体と）同様の目的のために処理される可能性があり、個人はしばしば自己のデータが処理されるか、またその方法についてほとんど、あるいは全く選択肢がないため、DPO の選任によるさらなる保護が必要となる可能性がある。

このような場合には義務はないものの、第 29 条作業部会はグッド・プラクティスとして次を推奨している。

- 公的任務を実行する、または公的権限を行使する民間団体は DPO を選任する、
- 当該 DPO の活動は公的任務の実行または公務の実行に関連しないもの（例：従業員データベースの管理）を含め実行される全ての処理作業をカバーするべきである。

②「中核的な活動」

GDPR 第 37 条第 1 項(b)号および(c)号は、「管理者または処理者の中核的な活動」に言及している。前文第 97 項は、管理者の中核的な活動は「主要な活動に関連し、補助的な活動としての個人データの処理には関係しない」と規定している。「中核的な活動」は、**管理者または処理者の目標を達成するために必要である重要な作業**と考えることができる。

しかし、「中核的な活動」は、**データの処理が管理者または処理者の活動の不可分な一部を形成している場合の活動**も排除するものとして解釈すべきではない。例えば、病院の中核的な活動は医療を提供することである。しかし、病院は、患者の健康記録などの健康データを処理することなく、安全かつ効果的に医療を提供することはできない。従って、これらのデータを処理することは、病院の中核的な活動の 1 つであると見なされるべきであり、病院は DPO を選任しなければならない。

別の例として、ある民間警備会社は、民間のショッピングセンターと公共スペース数か所の監視をしている。監視は同社の中核的な活動であり、それ自体が個人データの処理と不可分に関連している。従って、同社は DPO を選任する必要がある。

他方、全ての組織は、従業員の給与支払いや標準的な IT サポート活動など、一定の活動を行っている。これらは、組織の中核的な活動または主要事業のための必要なサポート機能である。これらの活動は必要または不可欠であっても、通常は中核的な活動ではなく補助的機能と見なされている。

[19] （原文脚注 13）第 6 条第 1 項(e)号

③「大規模」

GDPR 第 37 条第 1 項(b)号および(c)号は DPO の選任義務が生じるには個人データの処理が「大規模に」行われることを要求している。GDPR は何が大規模を構成するかを定義していないが、前文第 91 項で解釈の指針を提供している[20]。

第 29 条作業部会は**大規模な処理**が行われているかを判断するときに特に次の要因を考慮することを推奨している。

- **関係するデータ主体の人数－具体的な数字としてまたは関連する人口の比率**
- **処理されるデータの量および/または異なる種類のデータの範囲**
- **データ処理行為の期間または永続性**
- **処理行為の地理的範囲**

コメント５：大規模な処理の判断過程の文書化
上記の要因はいずれもどのような考慮がなされるのかが明確ではないため、「大規模な処理」への該当性を判断することは、下記の例にそのまま該当する場合以外、難しいものと考えられる。DPO の選任義務との関係では、「大規模な処理」の要件の該当性の有無についての分析を文書化しておくことが望ましいと考えられる。

コメント６：データ保護影響評価の判断要素としての「大規模な処理」
第 29 条作業部会の「データ保護影響評価に関するガイドライン（WP248）」は、データ保護影響評価の要否に関する判断要素の１つである「大規模な処理」の概念について、DPO ガイドラインにおける説明を参考に判断すべきであると述べている。

大規模な処理の例には次のものが含まれる。

- 病院の通常業務の一環としての患者データの処理
- 市の公共交通機関を利用している個人の移動データの処理（例えば、交通機関カードを通じてのトラッキング）
- データ処理統計目的のための国際ファストフードチェーン店の顧客のリアルタイムの地理位置情報データの専門処理者による処理
- 保険会社または銀行の通常業務の一環としての顧客データの処理
- 検索エンジンによる行動ターゲティング広告のための個人データの処理
- 電話またはインターネットサービスプロバイダによるデータ（内容、閲覧回数、所在地）の処理

[20] （原文脚注 14）前文によると、特に「大規模な処理作業は、かなりの量の個人データを地域、加盟国および超国家レベルで処理することを目的としており、それが多数のデータ主体に影響を及ぼし、高度のリスクをもたらす可能性があるもの」が含まれる。一方、前文では特に「個人データの処理が、個別の医師、その他の医療専門家または弁護士により行われる、患者または依頼者からの個人データに関連する処理の場合は、大規模と考えられるべきではない」と規定されている。前文では基準の両極端の具体例（「個別の医師による処理」と「全国または欧州全体にわたるデータの処理」）が示されているが、理解すべき重要な点は、これらの両極端の間にはグレーな領域があることである。さらに考慮すべきことは、この前文ではデータ保護影響評価を参照していることである。これは一部の要素はデータ保護影響評価に固有のもので、DPO の選任に必ずしも全く同様には適用されないということを示唆している。

大規模な処理と見なされない例には次のものを含む。

- 個々の医師（individual physician）による患者データの処理
- 個々の弁護士（individual lawyer）による有罪判決および犯罪に関する個人データの処理

④ 定期的かつ系統的な監視

データ主体の定期的かつ系統的な監視の概念は GDPR において定義されていない。「データ主体の行動の監視」の概念は、前文第 24 項[21]で言及されており、行動ターゲティング広告を目的とするものも含むインターネット上の全てのトラッキングおよびプロファイリングを明らかに含むとしている。

コメント７：データ保護影響評価の判断要素としての「系統的な監視」 「データ保護影響評価に関するガイドライン（WP248）」は、データ保護影響評価の要否に関する判断要素の１つである「系統的な監視」の概念は、DPO ガイドラインにおける説明を参考に判断すべきであると述べている。

しかし、監視の概念はオンライン環境のみに限らず、オンラインでのトラッキングはデータ主体の行動の単に監視の一例として挙げられているものと考えられるべきである[22]。

第 29 条作業部会は**「定期的」**を次のいずれかを意味すると解釈する。

- **継続している、または特定の期間に特定の間隔で発生する**
- **固定された時間に再び発生する、または繰り返される**
- **常にまたは定期的に発生する**

第 29 条作業部会は**「系統的」**を次のいずれかを意味すると解釈する。

- **システムに従って発生する**
- **事前に準備された、組織化されたまたは秩序がある**
- **データ収集の一般的計画の一部として発生する**
- **戦略の一部として実施される**

コメント８：「定期的」および「系統的」の判断過程の文書化 組織において「定期的かつ系統的な監視」に該当し得る業務を行っている場合には、上記の作業部会の「定期的」と「系統的」の文言の解釈を踏まえ、同組織が GDPR 上の DPO の選任義務の有無について組織内での分析の結果を文書化しておくことが望ましいと考えられる。

「定期的かつ系統的な監視」の例には次が含まれる。

通信ネットワークの運営、通信サービスの提供、電子メールのリターゲティング、データドリブンマーケティング活動、リスク評価のためのプロファイリングおよびスコアリング（例：信用スコア付け、保険料の設定、不正防止、マネーロンダリングの探知などを目的とするも

---

[21] （原文脚注 15）「処理行為がデータ主体の行動の監視であると見なされ得るか否かを判断するためには、自然人がインターネット上でトラッキングされるか否かを、特に当該個人に関する決定を行なうため、または、当該個人の嗜好、行動および言動の分析または予測のための自然人のプロファイリングからなる個人データ処理技術がその後に使用される可能性を含めて、判断しなければならない。」

[22] （原文脚注 16）前文第 24 項は GDPR の域外適用に焦点を当てていることに注意。さらに、「行動の監視」（第 3 条第 2 項(b)号）と「データ主体の定期的かつ系統的な監視」（第 37 条第 1 項(b)号）との間では文言の違いがあるため、これらは異なる概念を構成すると考えられる可能性がある。

の）、移動体通信機器用のアプリなどによる位置追跡、ポイントサービス、行動ターゲティング広告、ウェアラブル・デバイスによる健康状態、運動および健康データの監視、閉回路テレビ（CCTV）、スマートメーターやスマートカー、ホームオートメーションなどの接続デバイス。

⑤ 特別カテゴリーの個人データならびに有罪判決および犯罪に関するデータ

GDPR 第 37 条第 1 項(c)号は、第 9 条に基づく特別カテゴリーの個人データの処理および第 10 条に規定されている有罪判決および犯罪に関する個人データの処理について規定している。

同条項では「ならびに（and）」という用語を使用しているが、2 つの基準が同時に適用されなければならない政策上の理由はない。従って、この文章は「または（or）」と書いてあるとの理解で読むべきと考えられる。

コメント 9 ：「大規模」の意義 第 37 条第 1 項(c)号「管理者または処理者の中核的な活動が、特別カテゴリーの個人データまたは有罪判決および犯罪に関連する個人データの大規模な処理である場合」の要件のうち、「大規模な処理」の意義については、2.1.3 で挙げられている「大規模な処理」にあたる場合の例を参考に判断することになる。

(2) 処理者の DPO

DPO の選任に関して、GDPR 第 37 条は管理者および処理者の両方に当てはまる。どちらが義務的選任に関する基準を満たすかによって、場合によっては管理者のみまたは処理者のみ、その他の場合は管理者とその処理者の両方が DPO を選任する（そして相互に協力する）必要がある。

強調すべき重要な点は、処理者が義務的選任の基準を満たしていてもその管理者は必ずしも DPO を選任するよう要求されないことである。例として次が挙げられる。

- ある町で家電製品の販売を行う小さな家族経営事業者が、中核的な活動がウェブサイト分析サービスおよびターゲティング広告およびマーケティングの援助を行う処理者のサービスを使用する。少ない顧客数および比較的限定された活動に鑑みると、家族経営事業者およびその顧客の活動から「大規模」なデータ処理は発生しない。しかし、こうした小規模事業者のような顧客を多数有する処理者の活動は、総合すると大規模な処理を行っていることになる。従って、当該処理者は第 37 条第 1 項(b)号に基づき DPO を選任しなければならない。もっとも、家族経営事業者そのものは DPO を選任する義務はない。
- 中規模タイル製造業者が、労働健康サービスを外部の処理者に外注しており、当該処理者は多数の同様の顧客を有している。大規模なデータ処理が行われているのならば、当該処理者は第 37 条第 1 項(c)号に基づき DPO を選任する。しかし、管理者である中規模タイル製造業者は必ずしも DPO を選任する義務はない。

処理者によって選任された DPO は、処理者が自らデータ管理者としての役割（例えば、人事、IT、ロジスティクス）を担っている場合には、処理者の組織が実施する活動も監督する。

(3) 「複数の組織のための単一の DPO の選任」

GDPR 第 37 条第 2 項は、事業者グループが「各拠点から容易にアクセス」できるという条件で、単一の DPO のみを選任することを認めている。DPO の任務の 1 つが「本規則に基づいて管

理者および処理者ならびに義務の処理を行う従業員に対して情報を提供し、助言すること」であることから考えて[23]、アクセスの容易性の考え方は、DPO の任務として、データ主体[24]、監督当局[25]、また組織内部との連絡窓口を務めることを指している。

内部または外部からを問わず、確実に DPO へのアクセスが可能であるようにするために、連絡先詳細が必ず GDPR の要件に従って提供されるようにすることが重要である[26]。

DPO は、必要に応じてチームからの支援を受けながら、効率的に、データ主体[27]と連絡できる立場にあり、かつ関連する監督当局と協力[28]しなければならない。これは、関連する監督当局およびデータ主体によって使用されている言語または複数言語で連絡を行わなければならないことを意味している。DPO のアベイラビリティは（従業員と物理的に同一の場所にいるか、ホットラインその他の確実なコミュニケーションの手段を通じてであるかを問わない）、データ主体が DPO に連絡可能であることを確保するために必要不可欠である。

コメント 10：DPO チームの構成

日本企業としては、DPO チームとしてこれまでデータ保護および GDPR 対応を行ってきた日本本社の法務、またはコンプライアンス、総務担当の執行役員、部長クラスの責任者を DPO として選任し、監督当局やデータ主体とのコミュニケーションを効果的に行うために必要な支援体制（DPO を補助する担当者の配置、社内の連絡系統の整理など）を現地子会社および日本本社で整備することが考えられる（日本本社での DPO の選任の可能性については、後述を参考）。あるいは、欧州には DPO 業務の委託を受けることの多い法律事務所（規模の小さなデータ保護法に特化した専門法律事務所が多い傾向がある）も存在するため、そのような法律事務所に業務委託することも考えられる。

また、日本本社において DPO を選任する場合には、監督当局およびデータ主体との現地語によるコミュニケーションを確保するため、現地子会社または外部の法律事務所もしくはコンサルタントにおいて、DPO チームのメンバー（非 DPO）として、現地語による監督当局およびデータ主体とのコミュニケーションが可能な人材を書面で選任しておくことが必要である。

GDPR 第 37 条第 3 項によれば、その組織の構造および規模を考慮して、数カ所の公的機関または公的団体について、単一の DPO を選任することができる。また、リソースと連絡方法[29]に関する同じ考慮事項が適用される。DPO は様々な任務を担当しているため、管理者または処理者は単一の DPO が数カ所の公的機関および公的団体を担当する場合でも、必要な場合はチームによる支援を受けながら、効率的に任務に従事できるよう保証しなければならない。

(4) DPO のアクセスの容易性および現地化

GDPR 第 IV 章の第 4 節によれば、DPO のアクセスの容易性は実効的である必要がある。

---

[23] （原文脚注 21）第 39 条第 1 項(a)号
[24] （原文脚注 19）第 38 条第 4 項
[25] （原文脚注 20）第 39 条第 1 項(e)号
[26] （原文脚注 22）下記セクション「2.6［DPO の連絡先詳細の公表と連絡］」も参照。
[27] （原文脚注 23）第 12 条第 1 項
[28] （原文脚注 24）第 39 条第 1 項(d)号
[29] リソースについては下記「3.1　個人データ保護に関連する全ての事項への DPO の関与」を、連絡方法については同「2.6　DPO の連絡先詳細の公表と連絡」を参照。

確実にDPOへのアクセスが可能であるようにするために、第29条作業部会は、管理者または処理者が EU 域内に拠点を有するか否かに関わらず（地理的範囲については第 3 条を参照）、DPO を EU 域内に配置することを推奨している。

コメント 11：DPO のアクセスの容易性

DPO に関するガイドラインは、DPO へのアクセスの容易性の観点から DPO が EU 域内に所在することを推奨する旨を記載しているが、そのような措置はアクセスの容易性を満たす方法としての推奨事項に過ぎない。従って、DPO を EU 域内で選任しないとしても、DPO のアクセスの容易性が確保されていれば、GDPR 違反とはならない。

多くの日本企業は、重大なコンプライアンス事項である GDPR への対応について、日本本社主導で行っている。このような場合に、日本本社において GDPR の遵守プロジェクトを推進する人物（後述の利益相反がないことを前提）を DPO として選任することは、当該日本企業グループにおいて GDPR へのコンプライアンスを高めることにとってプラスにこそなれ、マイナスになることはないと考えられる。GDPR の本質的な要請は、監督当局およびデータ主体から DPO へのアクセスの容易性を確保することであり、DPO が物理的に所在する場所ではないと考える。そして、監督当局およびデータ主体から DPO へのアクセスの容易性は、上述の通り、現地子会社において、DPO チームのメンバー（非 DPO）として、現地語による監督当局およびデータ主体とのコミュニケーションが可能な人材を書面で選任しておき、監督当局やデータ主体から、当該 DPO チームのメンバーに連絡があった際には、速やかに日本本社の DPO に当該連絡の内容を取り次ぐとともに、当該 DPO から監督当局やデータ主体への連絡が円滑に行われることを確保することが重要である。

以上の措置は、一見すると容易ではなく感じられるかもしれないが、結局は、GDPR 上の管理者の他の義務への対応として、日本本社―現地子会社―監督当局および/またはデータ主体への迅速な連絡が必要となるということを意味する。例えば、GDPR 第 33 条の個人データ侵害（例：サイバー攻撃による EU 所在者の個人データの漏えい）の場合の遅滞なき、可能な場合には、当該個人データ侵害に気付いてから 72 時間以内の監督当局の報告義務への対応が挙げられる。当該報告義務は、当該個人データ侵害が自然人の権利および自由に対するリスクを生じさせる可能性がない場合を除いて、生じることになる。日本企業としては、当該報告義務が存在するか否かについて微妙な判断を求められるケースも当然のことながらあり得る。その際に、日本企業が考慮することを求められる事項は、EU の GDPR の解釈もさることながら、日本国内におけるマスメディアへの対応、米国・中国などの他の法域の監督当局への対応など多岐にわたることになる。このように、EU 域外にグローバル本社機能を持つ日本企業にとって、GDPR 上の DPO が物理的に日本本社に存在することは、サイバー攻撃による個人データの漏えいのような一大事への対応を、EU 以外の重要な法域の監督当局への対応も視野に入れながらバランスの取れた対応を行う上では、都合が良いと考えられる。

しかしながら、管理者または処理者が EU 域内に拠点を有しない場合[30]一定の状況においては、DPO は EU 域外に所在するときに、より効果的に活動を行い得る可能性は排除されない。

コメント 12：DPO のアクセスの容易性（2）

[30] （原文脚注 25）GDPR 第 3 条（地理的範囲）参照

前コメントと同様、DPO を EU 域内で選任することは推奨事項として述べられているに過ぎないため、管理者または処理者が EU 域内に拠点を有している場合においても、EU 域外で DPO を選任することも可能である。

コメント 13：DPO の選任に関するリスクと対応策

DPO は、データ保護に関して幅広い権限を有するとともに、高い独立性が確保される地位にある。例えば、ある管理者が推進しようとするビジネスが EU の個人データに関連する場合、当該管理者の DPO は当該ビジネスにおける GDPR に関する問題について監視、助言などを行うことになるが、DPO によるリスク評価の内容や GDPR の解釈次第では当該ビジネスの実施が不合理に遅滞し、頓挫するといった事態が発生し得る。もっとも、DPO は、管理者からの高い独立性を有し、何人からも指揮命令を受けないことから DPO は管理者の見解に服せずに自由に見解を示すことが可能であり、仮に管理者が当該ビジネスにおけるリスク評価に関する DPO の見解が管理者の見解と整合しないことを理由に DPO を解任した場合、明白な GDPR 違反となる。

DPO の選任ミスは DPO の地位に関して DPO との紛争につながるリスクがあるが、これは単なる従業員との紛争ではなく、GDPR 違反の有無に直結して高額な制裁金が課される可能性を伴う紛争であるため、どのような人物をどの拠点で選任するかには、慎重な検討が求められる。

上記のような DPO の選任に関するリスクを考慮して、日本企業の中には、まずは日本本社において DPO を選任しておき、2018 年 5 月の GDPR 適用開始後に DPO に関する動向を踏まえながら次の対応を検討するケースが数多く存在する。また、例えば、個人データの処理に関わるビジネスの研究開発を行う場合（欧州で収集した顧客データのビッグデータ活用）やタレントマネジメント（従業員が持つタレント（英語で「能力・資質・才能を意味する）やスキル、経験値などの情報を人事管理の一部として一元管理することによって組織横断的に戦略的な人事配置や人材開発を行うこと）の IT システムを欧州を含む全世界の従業員を対象として日本本社で導入する場合には、日本本社で DPO を選任することがデータ保護影響評価の実施との関係で効率的であるとも考えられる。

また、EU 拠点内で DPO を選任するとしても、DPO の人選は現地子会社に委ねず、日本本社も関与して慎重に検討することが必要である。

(5) DPO の専門性および技能

GDPR 第 37 条第 5 項は、DPO は「専門家としての資質、特にデータ保護法およびプラクティスの専門知識ならびに第 39 条に述べられている任務を遂行する能力に基づいて選任されること」と規定している。前文第 97 項は、必要とされる専門的知識は実行するデータ処理業務および処理する個人データに必要な保護に基づいて判断されるべきと規定している。

① 専門性のレベル

必要な専門性のレベルは厳密には定義されていないが、組織が処理するデータの機密性、複雑性および量に見合うものでなければならない。例えば、データ処理行為が特に複雑な場合、または大量のセンシティブデータを処理する場合、DPO はより高度な専門性とサポートを必要とし得る。また、組織が個人データを系統的に EU 域外に移転するかどうか、またはそのような移転は稀であるかによっても違ってくる。従って、組織内部で発生するデータ保護問題を十分考慮した上で DPO を慎重に選出する必要がある。

② 専門家としての資質

GDPR 第 37 条第 5 項は DPO を選任する際に、考慮すべき専門家としての資質について規定していないが、DPO が加盟国ならびに EU のデータ保護法およびプラクティスの専門性を有し、GDPR に対する深い理解を持たなければならないことは重要な点である。また、監督当局が DPO のための十分かつ定期的な訓練を促進することが有効である。

コメント 14：DPO の専門家としての資質の確保 データ保護法およびプラクティスの専門知識については、客観的に評価可能な経歴や資格を有することが望ましい。例えば、非営利組織であるプライバシー専門職国際協会（International Association of Privacy Professionals：IAPP）[31]（データ保護・プライバシーに関する国際団体であり、多くの国際的企業が参画し、支援を行っている）の CIPP/E（Certified Information Privacy Professional/Europe）[32]の資格を取得していることは、データ保護に関する一定の知識・理解を有することを証するのに有効な手段といえる。このような資格の取得が時間的制約などの事情から困難な場合には、データ保護に関する専門性を有する法律事務所、コンサルティング会社あるいはその他の専門家によるトレーニング・プログラムを受けることも考えられる。CIPP/E の言語は英語であるため、CIPP/E のトレーニングを英語で受講することが困難である場合には、次善の策として、日本語で GDPR に関するトレーニングを受講することが考えられる。

事業分野と管理者の組織に関する知識も役に立つ。DPO は、実行される処理業務ならびに管理者の情報システム、データセキュリティおよびデータ保護に関するニーズについて良く理解しているべきである。公的機関または公的団体の場合、DPO はその組織の行政上のルールおよび手続きに関して十分な知識を備えるべきである。

③ 業務を遂行する能力

DPO が果たすべき任務を遂行する能力とは、個人的資質と知識に加え組織の中の地位も指していると解釈されるべきである。

個人的資質には、例えば誠実さおよび高度な職業倫理などが含まれるべきである。DPO の主たる関心事は、GDPR の遵守を可能にすることである。DPO は、組織の中でデータ保護の文化を醸成する上で主たる役割を果たし、GDPR の不可欠な要素であるデータ処理の原則[33]、データ主体の権利[34]、設計および初期設定によるデータ保護[35]、処理行為の記録[36]、処理のセキュリティ[37]および個人データの侵害通知および連絡[38]などを実行するための支援を行う。

④ サービス契約に基づく DPO

DPO の役割は、管理者・処理者の組織外の個人または組織と締結されたサービス契約に基づいて果たすこともできる。後者の場合は、DPO の役割を果たす組織の各メンバーが GDPR 第 IV

[31] https://iapp.org/
[32] https://iapp.org/certify/cippe/
[33] （原文脚注 26）GDPR 第 II 章
[34] （原文脚注 27）同第 III 章
[35] （原文脚注 28）第 25 条
[36] （原文脚注 29）第 30 条
[37] （原文脚注 30）第 32 条
[38] （原文脚注 31）第 33 条および第 34 条

章の第 4 節の全ての適用される関連する要件を満たすことが不可欠である（例えば、誰も利益相反がないことが不可欠である）。各メンバーが GDPR の規定に基づき保護されることも、同様に重要である（例えば、DPO の活動のサービス契約を不当に終了させないことに加え、DPO としての業務を行う組織の個人メンバーを不当に解雇しない）。同時に、個々のスキルと特長を組み合わせることにより、チーム体制で作業する複数の個人がより効果的に顧客にサービスを提供することができる。

コメント 15：組織外の組織とのサービス契約に基づく DPO 組織外の組織とのサービス契約に基づく DPO を選任した場合、DPO の役割を果たす組織の各メンバーがどの程度の資質を具備する必要があるかは、各メンバーの役割によるものと考えられる。DPO としての役割を担う者は当然のことながら、GDPR に規定される専門家としての資質が求められるが、DPO をサポートするチームの一員としての役割を担う者は必ずしも DPO と同等の資質が求められるわけではないと考えられる。

法的な明確性および良い組織体制のために、かつ、チームメンバーの利益相反を防ぐために、DPO チーム内で明確な作業分担を割り当て、各依頼者ごとに特定の個人を連絡担当者かつ責任者に選任することが推奨される。また、一般的に、サービス契約中にこれらの事項を規定しておくことも重要である。

(6) DPO の連絡先詳細の公表と連絡

GDPR 第 37 条第 7 項は、管理者または処理者に次を要求している。

- DPO の連絡先詳細を公表する
- 関連する監督当局に DPO の連絡先詳細を連絡する

これらの要件の目的は、データ主体（組織の内外の両方）および監督当局が組織の別の者に連絡する必要なく内密に、容易かつ直接 DPO に連絡できるようにすることである。機密性は同様に重要である。例えば、DPO とのコミュニケーション内容の機密性が保証されない場合、従業員は DPO に対して申立てを行うことを躊躇する可能性がある。DPO は EU 法および加盟国法に従って業務に関する秘密または機密の守秘義務を負う（第 38 条第 5 項）。

DPO の連絡先詳細にはデータ主体と監督当局が DPO に容易に連絡できるような情報（住所、専用電話番号および専用電子メールアドレス）が含まれなければならない。必要な場合、公衆との連絡の目的のために他の連絡手段、例えば専用ホットラインまたは組織のウェブサイト上の DPO 宛の専用連絡フォームなどを提供することもできる。

GDPR 第 37 条第 7 項は公表された連絡先詳細に DPO の氏名を含むことは要求していない。DPO の氏名の公表を行うのがグッド・プラクティスともなり得るが、個別の状況でこれが必要または役に立つかは管理者または処理者および DPO が決めることである[39]。

しかしながら、DPO の氏名を監督当局に連絡することは、DPO が組織と監督当局の間における連絡先を務めるために非常に重要である（第 39 条第 1 項(e)号）。

[39] （原文脚注 32）注目すべき点は、個人データ侵害が起こった場合に監督当局およびデータ主体に提供されなければならない情報を規定している第 33 条第 3 項(b)号は、第 37 条第 7 項と違い、具体的に連絡を取る DPO の氏名（連絡先詳細だけでなく）も要求していることである。

グッド・プラクティスとして、第29条作業部会は組織が監督当局および従業員にDPOの氏名と連絡先詳細を知らせることを推奨している。例えば、DPO の氏名と連絡先詳細は組織のイントラネット、内線電話帳および組織図において内部で公表することが考えられる。

3. DPOの地位

(1) 個人データ保護に関連する全ての事項へのDPOの関与

GDPR 第 38 条は、管理者および処理者は DPO が「個人データの保護に関連する全ての問題に適切かつ適時に関与すること」を保証することを定めている。

DPOまたはDPOのチームがデータ保護に関連する全ての問題に、可能な限り早い段階から関与することが不可欠である。データ保護影響評価に関連して、GDPR は DPO の早期の関与を明示的に規定しており、そのような影響評価を行う場合には管理者が DPO に助言を求めるよう定めている[40]。DPO が最初の時点から情報を与えられ、相談を受けることで GDPR への遵守が促進され、設計によるプライバシーのアプローチを確保されることから、それを組織内のガバナンスの標準的な手続きとすべきである。さらに、DPO は、組織内の相談相手と見なされること、および組織内のデータ処理行為に関わる作業グループの一員であることが重要である。

そのため、組織としては、例えば次の点を保証すべきである。

- DPOが経営陣および中間管理職の会議に定期的に参加するよう要請されること。
- DPOの出席は、データ保護に密接な関係のある決定がなされる場合に推奨される。DPOが適切な助言を提供できるようにするために、全ての関連情報は適時にDPOに提供されなければならない。

コメント16：DPOの会議への出席 言うまでもなく、DPO は経営陣および中間管理職の会議に、常に出席しなければならないわけではない。また、データ保護に密接な関係のある決定がなされる会議について出席が推奨されるが、電話会議などを通じて出席することも可能である。

- DPO の意見は常に重視されなければならない。意見の相違がある場合、第 29 条作業部会はグッド・プラクティスとして、DPO の助言に従わない理由を文書化することを推奨している。
- データ侵害やその他の事件が発生した場合、速やかにDPOに相談しなければならない。
- 適切な場合、管理者または処理者はDPOにどういうときに相談が必要かを規定するデータ保護ガイドラインまたはプログラムを作成することができる。

(2) 必要なリソース

GDPR第38条第2項は組織に対して、「［DPOの］任務を遂行し、個人データおよび処理業務にアクセスし、専門知識を維持するために必要なリソースを提供すること」により DPO を支援することを要求している。特に次の事項を考慮する必要がある。

- 経営陣（取締役会レベルなど）によるDPOの役割の積極的支援。
- DPO が任務を完遂するのに十分な時間。これは、組織内の DPO がパートタイムで選任されている場合や組織外のDPOが他の任務に加えてデータ保護を行う場合に特に重要である。そうでなければ、相反する優先項目により DPO の任務がおろそかにされ得る。

[40] （原文脚注 33）第35条第2項

DPO の任務に専念するのに十分な時間があることが最も重要である。DPO の役割がフルタイムで行われていない場合、それに割く時間の割合を設定することがグッド・プラクティスである。また、役割を遂行するのに必要な時間、DPO の任務に対する適切な優先度のレベルを判断し、そして DPO（または組織）が作業計画を立てることはグッド・プラクティスである。

- 財源、インフラ（敷地、施設、設備）、および必要に応じてスタッフの十分な支援。

コメント 17：DPO を支援するためのリソース
DPO を選任する拠点によっては、財源や設備の観点からリソースの拡充に制約が生じざるを得ない場合もあり得る。DPO を支援するためには合理的な内容のリソースが必要であるが、DPO を支援可能な範囲について、DPO との間で事前に共通理解を得ておくことが望ましい。

- DPO の選任をスタッフ全員に正式に伝え、組織の中でその存在および役割が確実に知られているようにする。
- 人事、法務、IT、セキュリティなど他のサービスから、DPO が不可欠な支援およびインプット、情報が得られるようにするために必要なアクセス。
- 継続的訓練。DPO はデータ保護に関する最新の動向を常に把握できる機会を与えられなければならない。その目的は DPO の専門性を常に高めることで、DPO はデータ保護のトレーニング・コースやプライバシー・フォーラム、ワークショップなどへの参加を含むその他の専門性育成に参加するよう奨励されるべきである。
- 組織の規模と構造によっては、DPO のチーム（DPO とそのスタッフ）を設置する必要が生じる可能性がある。そのような場合、チームの内部構成および各メンバーの任務と責任を明確に規定しなければならない。同様に、DPO の役割が外部のサービス提供者によって行われる場合、依頼者のために選任された主たる窓口担当者が責任者となることで、その事業体で働く個人からなるチームが一丸となって DPO の任務を効果的に遂行する可能性もある。

一般的に、処理作業が複雑および/またはセンシティブであればあるほど、より多くのリソースを DPO に与える必要がある。データ保護に関する役割は実行されるデータ処理に関連して効果的かつ十分にリソースが確保されていなければならない。

(3) 指示ならびに「独立して義務および職務を履行すること」

GDPR 第 38 条第 3 項は、DPO が組織内で十分なレベルの自律性に基づいて任務遂行できることを確実にする上で有益な、基本的な保証事項をいくつか設定している。具体的には、管理者・処理者は、DPO が「自分の任務の実行に関して全く指示を受けない」よう要求されている。前文第 97 項では、DPO は「管理者下の従業員であるかどうかに関わらず、独立した立場で自らの任務、職責を行える立場にあるべきである」と付け加えている。

第 39 条の下で任務を遂行するにあたり、DPO は、例えば、どのような結果を達成すべきか、また、苦情をどのように調査するか、監督当局に相談するかなど、問題への対処方法について指示されてはならない。さらに、データ保護法に関連する問題、例えば法の特定の解釈などに関して特定の見解を受け入れるように指示されてはならない。

コメント 18：欧州子会社の管理と DPO の独立性

欧州子会社を有する日本本社が、欧州子会社におけるデータ保護に関するコンプライアンスを監督したいと考えたとしても、DPO に対して日本本社が採用する特定の解釈に賛同するように指示することは、GDPR に違反し認められない。そのため、日本本社による欧州子会社に対するガバナンス強化と DPO の地位の独立性という要請の間には、上記の意味における緊張関係がある。

しかし、DPO の自律性は、GDPR 第 39 条に基づき、DPO がその任務を超えた意思決定権限を有することを意味しない。

管理者または処理者は、DPO 選任後もデータ保護法を遵守する義務を負い、遵守を立証できなければならない[41]。管理者または処理者が GDPR および DPO の助言と相容れない決定をした場合、DPO は、自らの反対意見を最高経営者レベルおよび決定者に対して明確にすることが許されなければならない。この点について、第 38 条第 3 項は、DPO は「管理者または処理者の最高経営者レベルに報告するものとする」と規定している。このように直接報告を行うことは、管理者または処理者への情報提供および助言という DPO の職務の一環としての DPO による助言および勧告を、上級経営陣（例えば、取締役会）が確実に認識できるようにするものである。直接報告を行うもう 1 つの例として、最高経営者レベルに提供される DPO の年間活動報告の作成が挙げられる。

コメント 19：DPO の最高経営者レベルへの報告

GDPR 第 38 条第 3 項は、DPO は、管理者または処理者の最高経営者レベルに報告を行うものと規定している。ここでの DPO の報告先は、どの拠点における DPO として選任されたかによって異なる。例えば、ドイツ拠点において DPO の選任義務が発生した結果として日本本社で DPO を選任した場合、当該 DPO はあくまでドイツ拠点のための DPO であるから、当該 DPO は日本本社ではなくドイツ拠点の最高経営者レベルに対して報告を行うことになる。

(4) DPO の任務の遂行による解雇または不利益

GDPR 第 38 条第 3 項は、DPO が「自らの任務を行うことにより、管理者または処理者に解雇され、また、不利益を被ってはならない」と規定している。

この要件は DPO の自律性を強化し、彼らがデータ保護任務を遂行するに当たり、独立して行動し、十分な保護を得られることを保証する上で有益である。

GDPR の下では、DPO が DPO としての任務を遂行した結果として不利益を被る場合にのみ、DPO に不利益を及ぼすことが禁止されている。例えば、DPO が特定の処理によって高度のリスクが発生すると判断し、管理者または処理者にデータ保護影響評価を行うよう助言しても、管理者または処理者が評価に同意しないこともあり得る。このような状況では、DPO は当該助言を行ったことにより解雇されてはならない。

不利益には様々な形態があり、直接的または間接的であり得る。例えば、昇進の機会の欠落や先延ばし、昇進の妨害、他の従業員が受け取っている福利厚生の拒絶などが考えられる。これらのペナルティは実際に実施される必要はなく、DPO の自らの活動に関連する理由から DPO に不利益を課すために使用される限り、単なる脅しでも DPO に対する不利益となる。

41 （原文脚注 34）第 5 条第 2 項

コメント 20：DPO に対する不利益な取扱

DPO に対する間接的な不利益には様々な形態があり得ると同時に、DPO の処遇に関する主観的な受け止めによっては思わぬ紛争に発展する可能性がある。特に、DPO との職業文化や法文化の違いによって特定の処遇が不利益的取扱であると解釈される可能性に十分留意して、対応を行う必要がある。

通常の管理規則として、または、適用される EU 加盟国の契約法または労働法、刑法の下にあり、また、その適用を受ける他の従業員や請負人の場合と同様に、DPO は、DPO としての自らの任務を遂行する以外の理由（例えば、盗難、身体的、心理的、性的嫌がらせまたは同様の重大な違法行為）に基づく場合、適法に解雇され得る。

GDPR では、どのようにして、いつ DPO が解雇され、または、別の人と交代させられるかについて規定していない。しかし、DPO の契約がより安定しており、不当解雇に対してより多くの保証が存在するほど、彼らは独立性を持って行動できる可能性が高い。従って、第 29 条作業部会は、組織がこの方針に沿って取り組むことを歓迎している。

コメント 21：DPO の任期

DPO は、その独立性を確保するために、DPO の意見が組織の意見と異なることなどを根拠として解任されてはならない。また、不用意に DPO を変更することは、DPO の地位に関して DPO との間で紛争を生じさせるリスクがある。このように DPO を変更することは容易ではないことを考慮すると、当初は比較的短い任期を設定しておくことが望ましい（1 年程度が想定される）。あまりに短期な任期を設定すると DPO の独立性に疑義を生じさせる要素になり得るが、組織によっては事情に応じて 6 カ月の期間を設定することも考えられる。GDPR 適用開始直後に監督当局が DPO の任期を問題として執行活動を行うことは、執行の優先順位や限定された執行のためのリソースの関係で想像し難い（すなわち、組織が DPO の選任義務を履行している場合よりも、当該義務を履行していない組織に執行のリソースが振り向けられることになると予想される）。ただし、GDPR 適用開始後、数年後の段階で、どの程度まで短期間の DPO の任期が許容されるかについて監督当局が一定の指針を公表することも考えられるため、この点を注視して対応することが求められる。

(5) 利益相反

第 38 条第 6 項では DPO が「その他の作業および義務を遂行すること」が認められている。しかし、組織が「そのような作業および義務が利益相反をもたらさないこと」を保証することが義務付けられている。

利益相反がないことは、独立性を持って行動するという要件と密接に関連している。DPO は他の役割を持つことは認められているが、DPO は他の業務および義務によって利益相反が生じないという条件の下でのみ、これらの業務などを担当することができる。これは特に、DPO が組織の中で個人データの処理の目的および手段を決定するような地位に就けないことを意味している。各組織の特定の組織構造により、これはケースバイケースで検討されなければならない。

目安として、相反する地位には、経営陣（例えば、最高経営責任者、最高執行責任者、最高財務責任者、最高医療責任者、マーケティング部門長、人事部門長または IT 部門長など）が含まれるが、その他の組織構造の中におけるより低い役割であっても、そのような地位や役割が処理の目的や手段を決定することにつながる場合も含まれる。

組織の活動、規模および構成によって、管理者や処理者のグッド・プラクティスとして次が挙げられる。

- DPO の役割と両立しない地位を特定する
- 利益相反を避けるため、その趣旨を盛り込んだ内部規則を作成する
- 利益相反に関するより一般的な説明を含める
- 本要件の認知度を高める方法として、DPO は、その DPO としての役割に関して利益相反がないことを宣言する
- 組織の内部規則に保護措置を組み込むとともに、利益相反を避けるために、DPO の職の求人情報、またはサービス契約が十分に正確で詳細に規定されているように確実にする。また、この観点においては、DPO が内部から起用されたのか外部から雇用されたのかによって、様々な利益相反の形態があり得ることも留意する必要がある

4. DPO の任務

(1) GDPR の遵守の監視

GDPR 第 39 条第 1 項(b)号は DPO に、任務の中でも特に GDPR の遵守状況を監視する任務を課している。前文第 97 項ではさらに、DPO は「本規則の組織内部での遵守を監視するのに管理者または処理者を支援するべきである」と規定している。

これらの遵守を監視する任務の一環として、DPO は特に次を実施し得る。

- 処理行為を特定するための情報収集
- 処理行為の遵守の分析ならびに確認
- 管理者または処理者に情報を与え、助言し、提言を提供する

遵守の監視は、遵守不履行の事例がある場合に DPO が個人的にその責任を負うということを意味するものではない。GDPR では「本規則に従って処理が行われていることを保証し、立証するための適切な技術的および組織的な対策を講じること」（第 24 条第 1 項）は DPO ではなく、管理者が行うことが要求されていることを明確にしている。データ保護遵守は DPO ではなくデータ管理者の企業責任である。

コメント 22：GDPR の違反があった場合における DPO の責任
DPO ガイドラインが記載する通り、組織が GDPR に違反したとしても、DPO は当該違反について個人として責任を負うものではない。

コメント 23：DPO の基本的な業務
GDPR 第 39 条第 1 項は DPO が「少なくとも」行うべき任務を規定している。従って、管理者が DPO に対して第 39 条第 1 項に明示的に規定されている任務以外の任務を割り当てること、またそれらの任務をより詳細に特定することは可能である。ただし、DPO が多くの業務を兼務する場合、業務内容によっては利益相反や独立性の観点から問題が生じる可能性があることに留意する必要がある。

(2) データ保護影響評価における DPO の役割

GDPR 第 35 条第 1 項によれば、必要に応じてデータ保護影響評価を行うのは DPO ではなく管理者の任務である。ただし、DPO は、管理者を支援する上で大変重要かつ有用な役割を担い得る。第 35 条第 2 項は、設計によるデータ保護の原則に則り、管理者がデータ保護影響評価を

行う際には DPO の「助言を求める」ことを明確に要求している。そして、第 39 条第 1 項(c)号は DPO に対して「第 35 条に基づき［データ保護影響評価］に関して要求に応じて助言を提供し、その履行を監視する」任務を負わせている。

第 29 条作業部会は、管理者に次の問題などについて DPO の助言を求めることを推奨している。

- データ保護影響評価を実行するかどうか
- データ保護影響評価を実行する場合にどのような方法をとるか
- データ保護影響評価を組織内で実行するか、それとも外部委託するか
- データ主体の権利と利益に対するリスクを軽減するためにどのような保護措置（技術的および組織的対策を含む）を適用すべきか
- データ保護影響評価が正しく行われたかどうか、およびその結論（処理を進めるかどうか、またどの保護措置を適用すべきか）が GDPR を遵守しているかどうか

管理者が DPO により提供された助言に同意しない場合、データ保護影響評価に関する文書において、助言を考慮に入れなかった理由の正当性を書面で具体的に示す必要がある。

コメント 24：データ保護影響評価に関する DPO の助言がビジネスに与える影響

データ保護影響評価は、データ主体の権利および自由に対して高いリスクをもたらす可能性がある場合に必要とされる（第 35 条第 1 項）。第 29 条作業部会は、当該リスクを判断する基準のうちの 1 つとして、技術または組織的なソリューションの革新的な使用または適用を挙げている（「データ保護影響評価に関するガイドライン（WP248）」）。例えば、高速道路における運転行為を監視するためのカメラ・システムの使用は、技術または組織的なソリューションの革新的な使用または適用に該当するとともに、系統的監視に該当することから、データ保護影響評価が必要となるものと考えられる。ここで重要なことは、企業による革新的な技術によるビジネスの展開が EU 域内の個人データに影響する場合は、「技術または組織的なソリューションの革新的な使用または適用」に該当し、データ保護影響評価が必要となる可能性がある点である。その場合、DPO がデータ保護影響評価に関連して GDPR の遵守に関してどのような意見を述べるかによって、当該企業のビジネスの内容やスケジュールが影響を受ける可能性がある。このように、DPO の意見は、企業のイノベーションのスピードにも影響し得るため、GDPR の合理的な解釈に基づく見解を示すことのできる DPO を選任することは、企業のデータ保護コンプライアンスとビジネスのバランスを保つ観点から重要である。

第 29 条作業部会は、例えば DPO の契約に加えて、従業員や経営陣（関連があれば、その他利害関係者）に提供される情報においても、特にデータ保護影響評価の実行に関して、DPO が行う正確な作業およびその範囲の骨子を管理者が明確に示すことを推奨している。

(3) 監督当局との協力および連絡先としての活動

GDPR 第 39 条第 1 項(d)号および(e)号によれば、DPO は「監督当局と協力し」、「第 36 条で定める事前協議、および適切な場合にはその他の事項に関する協議を含む処理に関連する事項について、監督当局の連絡先として活動」しなければならない。

これらの業務は、本ガイドラインの序文において言及されている DPO の「［コンプライアンスの］推進役」としての役割を意味している。DPO は、第 58 条で言及される調査、是正措置、

認可および勧告を行う権限の行使のためのみならず、第 57 条で言及される職務を行うために、監督当局による文書および情報へのアクセスを促進するための連絡先として活動を行う。前述の通り、DPO は EU 法または加盟国法に従って職務の遂行に関して秘密または機密を保持する義務を負う（第 38 条第 5 項）。もっとも、秘密保持義務・機密保持義務は、DPO が監督当局に接触して助言を得ることを禁止していない。第 39 条第 1 項(e)号は、適切な場合は、DPO が監督当局といかなる事項に関しても相談することが可能であると規定している。

コメント 25：DPO による監督当局との相談 DPO は、監督当局と独自に相談することも可能であり、選任された組織におけるデータ保護上の問題を内部告発することも可能である。

(4) リスクベースの取り組み

GDPR 第 39 条第 2 項は DPO が「処理の性質、範囲、背景および目的を考慮して処理業務に伴うリスクを適切に考慮すること」を要求している。

この条文は、一般的で常識的な原則について規定しており、これは DPO の日常業務の多くの側面に関連する可能性がある。本質的に、DPO に対して自己の活動に優先順位を付け、データ保護に関してより高いリスクをもたらす問題に注力することを要求している。これは比較的レベルの低いリスクのデータ処理業務の遵守の監視を怠るべきだという意味ではないが、しかし主に高度のリスクのある分野に注力すべきであることを示している。

この選択的かつ実用的なアプローチは、DPO がデータ保護影響評価を実行する際にどの方法を用いるべきか、どの分野が内部または外部のデータ保護監査の対象となるべきか、どの内部訓練活動をデータ保護活動の責任を担うスタッフまたは経営者に提供するか、そして自分の時間とリソースをどの処理業務により多く時間を費やすかを管理者に助言する上で有益であると考えられる。

コメント 26：DPO のリスクベースでの業務 DPO ガイドラインが記載する通り、DPO の業務にも時間およびリソースの観点から限界があるため、DPO は、組織におけるデータ保護におけるリスクの所在を適切に見極め、プライオリティを合理的に配分して監視業務を行うことが求められる。

(5) 記録管理における DPO の役割

GDPR 第 30 条第 1 項および第 2 項は、DPO ではなく管理者または処理者に対して「その責任の下で処理作業の記録を保管すること」また「管理者に代わって実行された全ての処理行為の種類の記録を保管する」ことを義務付けている。

実務においては、DPO はしばしば、個人データ処理を担当する組織内の様々な部署から提供された情報に基づき、一覧表を作成し、処理作業の登録簿を保持することがある。このプラクティスは、多くの現行の国内法および EU 機関および団体に適用されるデータ保護ルールの下で確立されている[42]。

第 39 条第 1 項は、DPO が最低限担当すべき任務のリストを規定している。従って、管理者の責任の下で、管理者または処理者が DPO に処理業務の記録を保管する任務を割り当てることを

[42] （原文脚注 37）規則（EC）45/2001 第 24 条第 1 項(d)号

妨げるものは何もない。そのような記録は、DPO が遵守を監視する任務を行い、管理者または処理者に情報を与え、助言することを可能にする手段の１つと見なされるべきである。

いずれにしても、第 30 条の下で保管することが要求されている記録は、要求に応じて管理者および監督当局が、ある組織が実行している全ての個人データの処理行為の概要を把握できるための手段と考えるべきである。従って、これは遵守のための前提条件であり、説明責任に関する効果的な対策である。

レポートをご覧いただいた後、アンケート（所要時間：約１分）にご協力ください。

https://www.jetro.go.jp/form5/pub/ora2/20170094

「EU 一般データ保護規則(GDPR)」

（第 29 条作業部会ガイドライン編）

データ保護責任者

作成者　日本貿易振興機構（ジェトロ）海外調査部 欧州ロシア CIS 課

〒107-6006　東京都港区赤坂 1- 12-32

Tel.03-3582-5569

2018.2