GDPR(一般データ保護規則)の我が国企業への影響について

１　日本企業への影響はあるか

EU で施行された GDPR（General Data Protection Regulation　一般データ保護規則）ですが、EU と取引している我が国の企業や、EU 域内に営業所、駐在員を置いている企業は確実に影響があります。

また、EU 域内から個人データを取得した企業も、ほぼ確実に影響があります。詳細は、後述します。

まず、EU 域内から個人データを取得したい場合には、その情報の数にかかわらず、的確に対応しなければなりません。

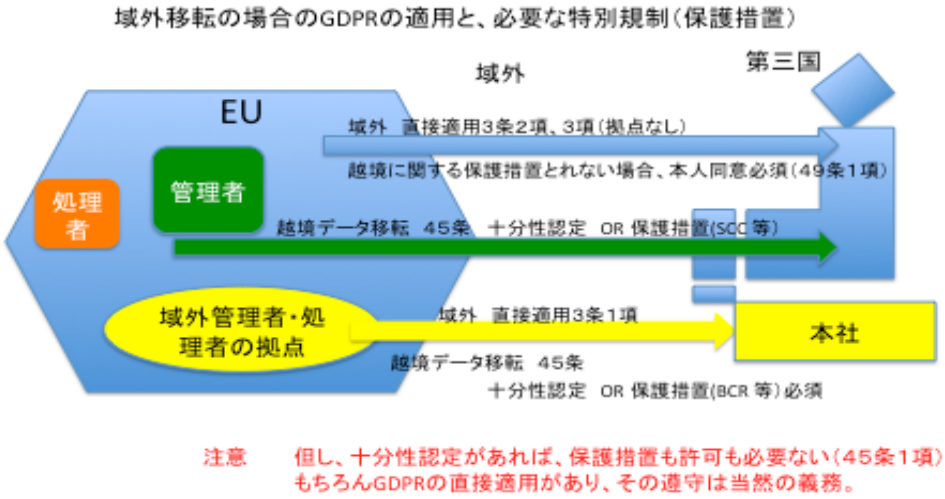
個人データの数（規模）が問題となるのは、代理人を選定すべきか否か、DPO の選任が義務になるか否か、を判断する場合です。比較的大きな規模で個人データを取得、取扱う場合には、EU 域内に拠点を置くか、代理人を置かねばならず、また、いずれの場合にあっても、個人データの取り扱い方について専門的な監督、指導、DPAI（個人データの安全確認の為のリスク、環境評価）を実施する義務があり、そのための専門家としての DPO(Data Protection Officer)の選任の義務があるか否か、を判断する際の要件となるものです。

しかし、こうした事をひとまず置いておいて、先ずは企業内に EU 域内からデータを取得してきたかを検討すべきであり、仮に取得していれば対応を検討しなければなりません。

２　我が国企業、事業への適用について

GDPR は、先ず、EU 域内企業、拠点のある企業に対して、EU 域内での個人データの取扱い（収集、取得など）について、厳しい規制を行った（以下３で述べます）上で、EU 域内での自由な情報流通を保障しようとするものです。

次に、EU 域内から外部への流出（越境データ）、すなわち第三国（third countries）へ移転させる行為は、原則的に禁止しています（GDPR45 条）。EU の企業が収集し、取得した個人データを、我が国企業へ輸出するような形での移転、すなわち域外への情報移転を認める例外的な場合とは、適切な「保護措置」をとる（以下４で述べます）か、本人同意が必要とされ、厳しく規制しています（GDPR 第５章他）。



注意　　但し、十分性認定があれば、保護措置も許可も必要ない（45条1項）。
もちろんGDPRの直接適用があり、その遵守は当然の義務。

３　直接、個人データを取得する場合

日本企業が EU の域内の人々の個人データを取得する場合とはどのような場合か、が問題となります。GDPR では、適用範囲としてその例をあげています。

（１）EU 域内の管理者、処理者の、それらの拠点の活動の過程における個人データの取り扱いに適用されます（３条１項）。

管理者とは、日本法で言うところの個人情報取扱事業者に相当します。また、処理者とは個人情報取扱事業者の委託を受けて個人情報の処理業務を行う事業者です（これも個人情報取扱事業者となります）。

加えて、これらの拠点の活動がある場合に、適用となります。拠点とは、主たる拠点と言う概念（GDPR４条１６項）の統括管理部門や主な取扱活動を行う機関である必要はありません。あくまでも管理者や、処理者の業務を支援し、一体として事業活動を行う関係にあれば足りるとされています。

GDPR3 条１項は、管理者、処理者の「拠点」（an establishment）における「活動の過程(関連)における」（in the context of the activities）個人情報の処理とされており、「拠点」の活動に関連していることであって、拠点自身が個人情報処理をしている必要はありません。

この点、GDPR 前文２２項では、「拠点とは、安定的な仕組みを通じて行われる実効的かつ現実の活動の実施を意味する」としており、この点を確認している点も考慮すべきこととなります。

こうした規定、前文の考え方を踏まえた上で、次の事案において明確な判断をしています。

Google.inc は全世界に検索サービスを提供しており、各国にはその業務を支援する為に支店が設立されていますが、これら支店は検索エンジン及びその情報処理に関しては一切の権限がなく、すべて米国本社が掌握しています。EU にもそうした支店がありますが、中でも Google Spain が拠点であるかが争われた事案で、Google.inc は、Google Spain は個人データを処理しないし、重要なこと業務を行うものでもないから、拠点ではないと主張しました。これに対して 欧州司法裁判所の判断は、「忘れられる権利」（削除請求権）の判断の前提として、Google Spain　が、Google.inc の「拠点」であることを明確に認めました（　Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)　A decision by the Court of Justice of the European Union (CJEU).）。

この結果、米国 Google.inc は、EU に拠点（Google Spain）を持ち、その拠点を利用して、EU 域内（EEA）の個人データを収集し、取り扱っていることから、当然に GDPR の適用を受けることになります。

以上を踏まえますと、EU の域内に、支社、支店、営業所、出張所などがあるか、駐在員がいる場合には、拠点があるという判断となり、３条１項の適用により、当然に GDPR の適用があると言う結論となります。日本本社は従業者、その他の関係者情報を現地からの報告を受けるなどして個人データを含む各種の情報を取得するので、日常的な越境データの取得になります。

念のため付け加えますと、多くの日本企業は、駐在員は日本人であって EU の人間ではないのだから、日本法の適用があるのであって、GDPR の適用はない、と考えがちですが、これは大きな間違いです。日本人従業者のデータの取得であっても、その従業者が EU 域内で稼働している以上は、その情報取得は EU 域内の個人データの取得となるわけです。EU 域内の情報という場合には、国籍や住所は関係ありません。EU 域内に所在していることが唯一の条件となります。したがって、日本人の従業者であっても、EU 加盟国に住民登録しているかに関わらず、GDPR の適用を受けることになります。

つまり、EU 域内に日本の企業の拠点がある場合には、GDPR の適用があり、これには例外がないということです。

（２）EU 域内に拠点を持たないが、自ら情報を取得する場合

① EU 域内のデータ主体に対する物品、またはサービスの提供を行い、それに伴って個人データが日本企業に移動する場合（３条２項(a)）

EU 域内に事業所などがない場合でも、日本から WEB を通して、あるいは現地企業を経由して商品やサービスを提供し、その後保証などのため WEB 登録を勧めるような場合には、日本企業が消費者、購入者の個人データを取得することになります。通信販売に留まらず、マンガの発行やソフトウエア販売、各種のデータのダウンロードサービスなどもこれに該当することが多いでしょう。

日本企業が、こうした物品販売やサービス提供を、EU 域内のデータ主体を対象として行なっているのかどうかの判断はどのようにするのでしょうか。

日本企業のサービスの提供が、EU 域内を対象としていない、米国その他の英語圏を目的としている、EU 域外で取得した情報であるかどうか、という考え方があるかもしれません。

GDPR３条２項が、EU 域内のデータ主体を対象としているという場合に、単に英語を利用しているからといって、すぐに適用とはなりません。

この点 GDPR はその前文 23 項において「EU 域内の一又は複数の加盟国内のデータ主体に対してその管理者又は処理者がサービスを提供しようとする意図が明白かどうかを確認しなければならない。」とした上で、「一又は複数の加盟国内で一般的に用いられている言語及び通貨を用いて当該別の言語による物品及びサービスの注文ができること、又は、EU 域内にいる消費者又は利用者に関する言及があることといったような要素は、その管理者が EU 域内のデータ主体に対して物品又はサービスの提供を想定していることを明白にしうるものである。」（個人情報保護委員会仮訳）としています。

ただ、注意すべきは、英語の使用です。英語は、EU の公用語の一つとされています。現在 EU で英語を使用するのはアイルランドおよびマルタ島しか有りませんが、EU での会議のときや対立がある場合には必ず英語が使用されています。その為、英語を使用しているということは米国を対象としている、とは言い切れない面があります。従って、その他の事情、即ち、使用通貨はどうか、EU 加盟国のデータ主体を対象とする表現があるか、などが基準になるとされています。

たとえば漫画に関してはフランスの愛好者が多く、それを日本の出版者、同人誌発行者はよく知っています。フランスの漫画ファンを対象としているような表現があれば、フランス域内のデータ主体を対象としてサービス提供していることから、GDPR の適用対象になります。

これと反対に、英語の表示をしているが、主に東南アジア、中国、米国、台湾などを対象とし、支払いは日本円か、米ドル建で、クレジット決済としている場合であって、EU 域内を対象とするといった特殊な文言、表現もないといった場合には、EU を対象としているとはいえません。そのような場合には GDPR の適用はなく、仮に例外的に EU 域内の人が購入を希望して登録したり、サービスを受けていたとしても、その人々の保護は、日本の個人情報保護法で対応すればよいことになります。EU を対象と明記しているのではないため、EU 域内のデータ主体は、そこが海外サイトであって GDPR の保護がないこと、サイトの保護方針に従って処理されることなどの説明を受けており、それを理解した上で、進んで入り込んだのであることから、GDPR の保護の必要はないのです。

② EU域内でのモニタリングを実施している場合（３条２項(b)）

EU域内でのモニタリングとは、データ主体の行動に関して、行動履歴を継続的に取得していたり、位置情報を継続的に取得していたり、検索履歴を把握したりといった継続性のある監視行為を意味しているということです。

前文では、

「取扱行為がデータ主体の行動の監視と考えられうるか否かを判断するためには、自然人のプロファイリングを構成する個人データの取扱い技術が後に使用される可能性を含め、 自然人がインターネット上で追跡されているかどうか、特に、データ主体に関連する判断をするため、又は、データ主体の個人的な嗜好、行動及び傾向を分析又は予測するために追跡されているかを確認しなければならない。」 （２４項）

としています。

結局、行動履歴、位置情報、検索履歴などを取得するシステムや、アプリを利用するサービスは、いずれもこの監視に該当することになります。

こうしたアプリを配布して、情報取集している企業は、監視行為を行っているということになり、GDPRの適用があることになります。

③ このほか、EU加盟国の国内法の適用のある個人データの取り扱いの場合（３条３項）

EU域外の事業者が、EU域内に拠点があったり（同１項）、EU域内データ主体を対象としていたり（同２項）といったはっきりした場合ではなく、いずれかの加盟国において、個人データの取扱いを行った場合にも当然に適用されるとしています。この「取扱い」とは、「自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しく は変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、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遂行又は一群の業務遂行を意味する。」と極めて広範囲にわたる個人データの処理の一部分であっても、該当するものに対してはGDPRの適用があるというものです。これによって、どのような形であるにせよ、EU域内での業務活動（私的な情報交換等は除いて）に関しては、すべてにGDPRが適用されるということになります。

４　現地企業などの第三者からの取得の場合

日本企業のなかには、自らEUで個人データを取得する（前記３の場合）のではなく、EUの事業者の収集した個人データを、まとめて提供を受けて、取得するところも多いと考えられます。旅行事業者などはEU域内の旅行業者と業務提携し、EU域内企業がとりまとめた旅行希望者の情報を、契約に従って取得して、彼らの日本での旅行をサポートする事になるでしょう。航空会社では、日常的にEUのエアライン企業から乗客名簿や旅行者の情報を取得して、サービス提供しているのです。

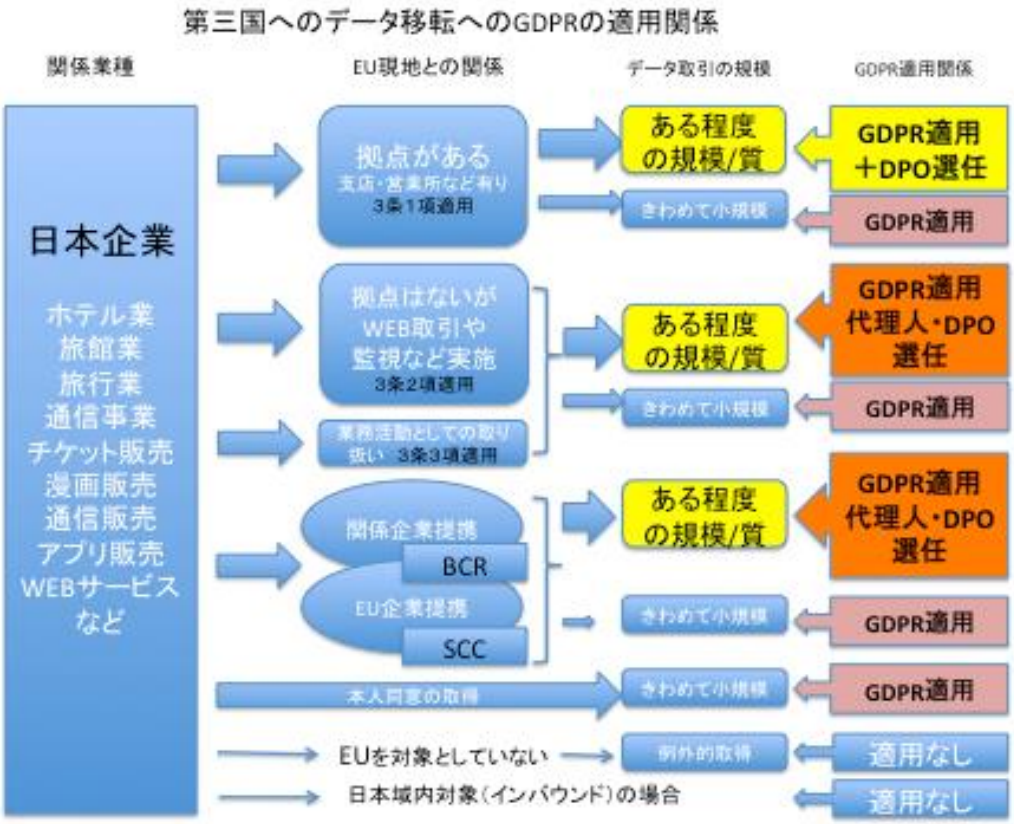
また、日本の関連会社、グループ会社などがEUにある場合には、その他の日系企業から旅行希望者などの情報の提供を受ける構造も考えられます。日本企業の支社や営業所であれば「拠点」ですから直接適用の問題（前記３）となりますが、関係企業であれば、拠点とまではいえないのであって、その場合にはEU企業からの取得と同様になります。

この形態は日本企業にとっては、第三国への越境データ、データの第三国企業への移転問題となり、特別な「保護措置」が必要なケースとなります。すなわち、SCC(SDPC)、BCRを締結するか、例外的な場合として厳格に本人同意をとる必要があります。

なお、EUからの旅行者を受け入れて、日本国内を案内する事業においても、募集の段階で既に我が国に来ている旅行者のみを対象としている場合には、いわゆる「インバウンド」といって、日本国内の情報を取得するだけですから、越境データの取得にはならず、GDPRの適用対象外となると考えられます。

しかし、一般にはEU域内から事前登録をしてもらう方法をとったり、EUの旅行事業者が募集した人を対象として、我が国事業者がEUの旅行事業者と提携し、あるいはその情報の提供を受けて、日本への旅行を実施することが多いと思われます。

EU域内から情報提供を受ける限りは、越境データの取得になりますので、GDPRの適用があり、十分な対応が必要となります。

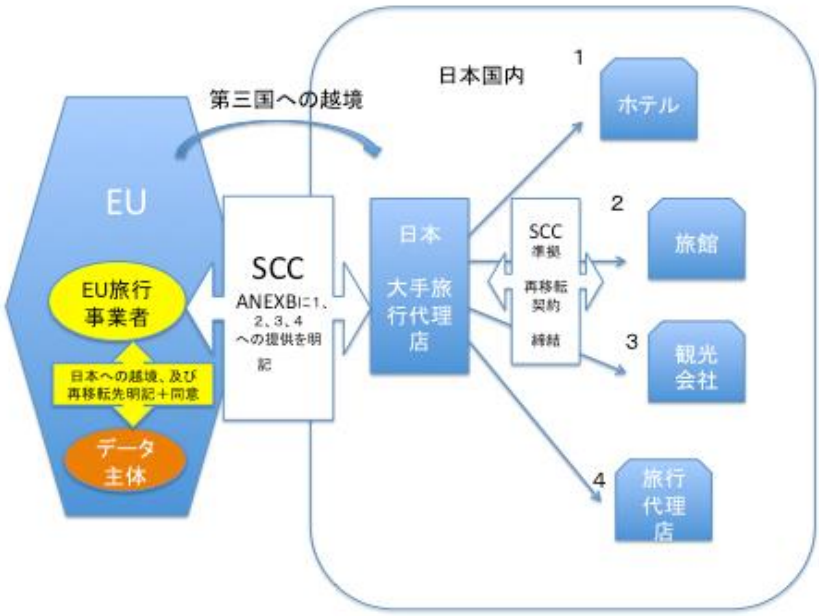


注意：そもそも越境データ（データ移転）が可能かについては、現時点で十分性認定がないため、第三国への越境に関する保護措置を取っているか（４７条）、あるいは例外的な同意が取られているか（４９条１項）が、必須となる。

○　サービス提供の場合　旅行業、ホテル業、旅館業など

これらの業種の場合には通常は予約を取る形で、旅行の前に電話やメールなどで個人データを含む予約情報の提供を受けるはずです。我が国に来ている旅行者から、当日宿泊の申し込みを受ける場合にはインバウンドとなり（前記図　インバウンド参照）越境データの取得にはならず、GDPR は適用がありません。

しかし、EU 域内からの移動になれば、通常事前に、EU 旅行事業者等を通して、予約することが多いでしょう。日本の旅行などの事業者が EU の事業者と業務提携を行うなどして、あるいは、大手旅行代理店を通して、日本の宿泊施設、ホテル、旅館、さらには民泊施設に情報提供して、旅行・サービス提供する場合には、EU 域内からのデータ移転を受ける以上は、GDPR の適用を受けることになります。



○　物品販売　WEB を利用した国際的通信販売事業など

「EU 域内のデータ主体に対する物品又はサービスの提供」を行う場合には、EU に拠点のない管理者または処理者にも GDPR は適用されます（３条２項(a)）。

GDPR では「一又は複数の加盟国内で一般的に用いられている言語及び通貨を用いて当該別の言語による物品及びサービスの注文ができること、又は、EU 域内にいる消費者又は利用者に関する言及があることといったような要素は、その管理者が EU 域内のデータ主体に対して物品又はサービスの提供を想定していることを明白にしうるものである。」（前文２２項　個人情報保護委員会仮訳）として、「EU 域内のデータ主体に対する物品又はサービスの提供」を行う場合といえるかを判断する、としています。

したがって、販売のためのサイトにおいて英語表記をしている場合（英語は EU の公用語のひとつとなります）や、EU の加盟国の言語を使用したり、EU 域内の人を対象としているような表現を使用している場合には、GDPR が適用されます。

５　取得した情報の保護　　GDPR の適用がある場合

我が国では、かつての（改正前）個人情報保護法では、５０００件要件という限定があり、５０００件までの個人情報の取扱いしかしていない事業者（小規模事業者）は個人情報取扱事業者とはならず、個人情報保護法上の義務を課されない、という取扱いになっていました。

しかし、こうした取扱いはEUに強く批判されていました。個人情報の提供者（データ主体）から見たとき、小規模事業者が取り扱う場合には保護されず、大規模事業者が取り扱う場合には保護される、という取扱いは合理的ではなく、個人情報を十分保護していない、というものでした。

我が国ではこうした批判を受け、平成２７年に個人情報保護法が改正され、５０００件要件が廃止され、個人情報を取り扱う事業者は、規模の大小を問わず、個人情報取扱事業者として法律上の義務を負うというルールになりました（改正個人情報保護法は平成２９年５月に全面施行されました。）。

こうした我が国の個人情報保護法改正の経緯を前提にすると、EU域内の情報を、少ししか取り扱っていないからといって、その権利保護をないがしろにすることはできないのがわかります。極端に言えば、１名の個人データであっても、それがEU域内の個人データであり、GDPRの適用のある場合である以上は、保護すべきものとなるのです。

６　大量、特殊な個人データを取り扱う場合などの注意

我が国の事業者で、EU域内の個人データを大量に取り扱う場合、あるいは指定された特別なデータを取扱う場合、さらに注意が必要です。

事業者が、

① データ主体の定期的、系統的監視を大規模に行う場合

② ９条、１０条のデータを大規模に取扱う場合

には、代理人およびDPOの選任が義務となります。

代理人は、管理者、処理者の連絡先となるべき、企業の出先機関としての意味で必要なのですが、DPOは、企業とは独立した地位にあり、企業を指導、監督できる専門職の人間を選ぶことになります。

①の定期的、系統的監視の意味ですが、WEB上での行動ターゲティング広告の実施は、この監視に当たり、また、位置情報の取得行為も同様に該当することになります。従って、ＷＥＢページで、EU域内の人のアクセスを念頭に置いたクッキーの取得や、ＷＥＢビーコンなどの装置によるデータ取得は、監視となることから、DPO選任が必要となりますので、注意が必要です。

我が国の企業が、EU域内に「拠点」を持っている場合には、その拠点が、所管の（加盟国の）監督機関と連絡を取り、あるいはEU域内のデータ主体からの問い合わせや各種請求の受付ができるので、新たに代理人を選定する必要はありません。しかし、WEBを通し

てサービス提供を行っている場合や、EU 域内の事業者と業務提携しているような場合で、現地に連絡拠点がない場合には、代理人選定義務が発生します。

(1) 代理人を選定する義務（２７条）

GDPR は、「第３条２項が適用される場合、管理者又は処理者は、書面により、EU 域内における代理人を指定する」としており、その代理人は、「データ主体に対する物品若しくはサービスの提供と関連してその個人データが取扱われるデータ主体、又は、その行動が監視されるデータ主体のいる加盟国中の１つに設けられる」としており、サービス提供先、あるいはモニタリング対象のデータ主体のいる加盟国内に設けて、届け出ることになります。

代理人は、管理者、処理者から、委任を受けて、監督機関およびデータ主体との連絡等の仕事を行うことになります。代理人の特別な資格や、要件は特に指定されていません。

ただし、センシティブなデータ（９条）、有罪判決情報（１０条）などを大量には含まず、権利侵害が発生することが考えられない場合には代理人は不要とされます（同２項(a)）。

(2) DPO（Data Protection Officer　データ保護監督官）選任の義務（第４節、３７条）

GDPR は、管理者に対して、新しい技術の導入などによって、「自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者は、その取扱いの開始前に、予定している取扱業務の個人データの保護に対する影響についての評価を行わなければならない。」（３５条）と規定し、DPIA(Data Protection Impact Assessment データ保護影響評価)の実施を求めています。自動処理によるプロファイリング、開かれた場所での監視行為の実施などの場合は必ず行うべきとしており、さらに専門家である DPO に相談しなければならない、ともしています。

その上で、その評価においてリスクが高いとされ、かつ十分な対応策が無い時は、事前に監督機関と協議しなければならないとされています（３６条）。これを、事前協議と言います。

そうした前提のもとで、GDPR は、専門家である DPO を選定することを求めています。３７条は、

① 公共機関が取り扱う場合

②管理者又は処理者の中心的業務が、その取扱いの性質、範囲及び又は目的のゆえに、データ主体の定期的かつ系統的な監視を大規模に要する取扱業務によって構成される場合

③ 管理者又は処理者の中心的業務が、第９条による特別な種類のデータ及び第１０条で定める有罪判決及び犯罪行為と関連する個人データの大規模な取扱いによって構成される場合。

には、DPO の選任義務があるとしています。

DPO は、その職務として、

a. 本規則及びそれ以外の EU 若しくは加盟国のデータ保護条項による義務を通知し、かつ、助言すること

b. 取扱業務に関与する職員の責任の割当て、意識向上及び訓練、並びに、関連する監査を含め、本規則の遵守、それ以外の EU 又は加盟国の個人データ保護条項遵守、並びに、個人データ保護と関連する管理者又は処理者の保護方針の遵守を監視すること

c. 要請があった場合、第３５条によるデータ保護影響評価に関して助言を提供し、その遂行を監視すること

d. 監督機関と協力すること；

e. 取扱いと関連する問題に関し、監督機関の連絡先として行動すること。第３６条に規定する事前協議、適切な場合、それ以外の関連事項について協議することを含む。

（以上３９条）

としており、その職務を行う DPO は、独立性のある地位が確保されなければならないとしています。

独立性については次のように規定します。

「管理者及び処理者は、データ保護オフィサーが、その職務の遂行に関し、いかなる指示も受けないことを確保しなければならない。当該データ保護オフィサーは、当該データ保護オフィサーの職務の遂行に関して、管理者又は処理者から解任され、又は罰則を受けることがない。データ保護オフィサーは、管理者又は処理者の最高経営者レベルに対して直接報告しなければならない。」（３８条３項　個人情報保護委員会仮訳）。

DPO が、その職務の実施に関して「いかなる指示も受けない」上に、その業務遂行を理由に解雇や処罰を受けないとして身分保障を求め、かつ企業のトップに直接報告する立場にある、というわけです。

ただ、DPO が企業のメンバーから選定されることを禁止していません（３８条６項）が、ただ、従業者からの選出になると、人事上の指揮権や、通常業務での指揮命令などがあり、DPO としての権利と義務が、職務上の指揮命令と矛盾したり、統制がとれなくなったり、利益相反するなどのことが考えられることから、管理者らは、そうした混乱や利益相反とならない仕組みを作らなければならないとされています。

DPO の選任に関しては、企業ブループで単一の DPO を選出できる（３７条２項）ほか、関係企業、関連業種として１名の DPO を選出すること（同４項）も認められています。

DPO の資質としては「データ保護オフィサーは、専門家としての資質、及び、特に、データ保護の法令及び実務に関する専門知識並びに第 39 条で定める職務を充足するための能力に基づいて指定される。」（３７条５項）としており、GDPR 上の指導を的確に進めることのできる資質、経験、専門的識見が必要とされます。

企業としては、そうした専門家を選定し、登録する義務を負うことになります。

以上