

寄稿

# 加盟国法を踏まえたデータ保護コンプライアンスを

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 弁護士 杉本 武重

EU一般データ保護規則（GDPR）は、一定の事項に関して、EU法または加盟国法によって定めることができる余地を残している。GDPRは加盟国の国内法に優先して適用されるが、欧州経済領域（EEA）の各加盟国は、現在、GDPRが加盟国法によって規定すべきと定める項目の規定を中心とした、国内法としてのデータ保護法の立法手続きを進めている。これら当該加盟国法上の義務がGDPR上の義務を直接構成する場合もあることから、その内容についても押さえておくことが重要である。本稿ではGDPRに関してEEA加盟国が国内法でルールを規定すべきまたは規定できる事項を整理し、特に日本企業に関係すると思われる項目を紹介する。また主な分野に関してはドイツデータ保護法の内容を紹介する。

## 加盟国法も含め関連項目の確認を

GDPRが加盟国法によるルールの策定を認めている分野は、加盟国の重要な政策事項に関わる事項が中心的ではあるが、これらは日本企業のデータ処理および移転に直接影響を及ぼす内容を多く含む（表）。

例えば、このほど成立した新ドイツ連邦データ保護法（2017年7月5日成立）はデータ保護責任者（DPO）の選任・地位〔GDPR第37条、第38条〕に関して、継続的に個人データの自動処理を実行するために10人以上の従業員を雇用する場合や、データ処理がデータ保護影響評価（DPIA）の対象となる場合などには、データ処理に係る従業員の数にかかわらずDPOの選任義務がある、とする。加盟国は、DPOの秘密保持に関する義務を規律する法律を制定できる〔第38条〕。

また、同法において従業員データの処理〔GDPR第88条第1項〕については、原則として、雇用関係の確立または実施（採用活動、上司の従業員業務評価の閲覧、給与管理等の人事情報管理等）に必要な場合に認められる。また、同法は犯罪行為の調査（を目的としたデータ処理の）制限について規定するほか、従業員の特別カテ

ゴリーのデータ（後述）の使用が認められる一定の事由、雇用関係において従業員からの同意が自由に与えられた（雇用の条件等として雇用者から強いられたものではない）と認められる条件などについても規定する。

このように、GDPRのコンプライアンス対応を行うためには、加盟国法の動向も把握しておく必要がある。以下にGDPRに関して加盟国が国内法でルールを規定すべきもしくは規定できる事項を詳しく整理する。

### 1. 処理の適法性〔第6条第1項（c）（e）、第2項〕

処理の適法性に関する要件の一部について、加盟国はより詳細な要件などを規定することができる。

### 2. 情報社会サービスに関する子どもの同意に対して適用される条件〔第8条第1項〕

子どもに対する情報社会サービスの直接的な提供に関するデータ主体の同意については、子どもが16歳未満の場合、子どもに対する保護責任を負う者による同意が必要である。加盟国は、当該年齢についてより低い年齢（13歳が下限）を法律で規定できる。

### 3. 特別カテゴリーの個人データの処理〔第9条第1項、第2項、第4項〕

特別カテゴリーのデータ（人種もしくは民族的素性、政治的思想、宗教的もしくは哲学的信条（philosophical beliefs）、または労働組合員資格に関する個人データの処理、および遺伝データ、自然人の一意な識別を目的とした生体データ、健康に関するデータまたは自然人の性生活もしくは性的指向に関するデータ）の処理は、データ主体が特定の目的のための処理に対して明示的な同意を与えた場合は適法である。ただし、EU法または加盟国法は、データ主体の同意により処理が適法化されるべきではない場合について規定できる。また、加盟国は、遺伝データ、生体データまたは健康データの処理に関して、さらに条件を課すことができる。

表 EU 法または加盟国が別途定める権利または義務を有する項目のうち、日本企業に関係すると思われる項目

データ処理の適法性および特別な処理状況に関する条項
処理の適法性に関する要件の一部 [第6条第1項 (c) (e)、第2項] …1 情報社会サービスに関する子供の同意に係る年齢制限 [第8条第1項] …2 特別カテゴリーの個人データの処理 [第9条第1項、第2項、第4項] …3 犯罪等にかかる個人データの処理が認められる場合 [第10条] …4 国民識別番号等の処理に関する特定の条件 [第87条] …16 従業員個人データ処理に関する権利を確保するための規定等 [第88条第1項] …17
データ主体の権利 (情報通知、その他の権利)
データ主体から個人データを取得しない場合に提供される情報 [第14条第5項 (c)] …5 データ主体に認められる権利の制限および例外 (削除権およびプロファイリング等に関する決定に服さない権利等) [第17条第3項 (b)、第22条第2項 (b)、第23条第1項] …6、7、8 複数の管理者が存在する場合のデータ主体の権利および情報通知に関する管理者の義務の範囲等 [第26条第1項] …9
管理者のデータ保護体制に関する義務
管理者の指示に基づかない処理の禁止の例外 [第32条第4項] …11 データ保護影響評価が要求されない場合に関する規定 [第35条第10項] …12 データ保護責任者の選任義務 [第37条、第38条] …13
データ移転
公共の利益に関する重大な理由による、特別カテゴリーの個人データの移転制限 [第49条] …14
その他の規定
GDPR において規定されている制裁金等以外の罰則 [第84条第1項] …15 職務上の守秘義務等にかかる規定 [第90条第1項] …18

注：表中の数字は、本文の小見出しの数字に対応

資料：EUの「一般データ保護規則 (GDPR)」に基づき作成

#### 4. 有罪判決および犯罪に係る個人データの処理 [第10条]

有罪判決および犯罪または関連するセキュリティー対策に係る個人データの処理に関して、どのような場合に処理が認められるかについて、EU 法または加盟国法で条件を規定できる。

#### 5. データ主体から個人データを取得しない場合に提供される情報 [第14条第5項 (c)]

データの取得または開示に関するデータ主体 (個人データが関連する当該個人) の正当な利益を保護するための適切な対策が EU 法または加盟国法により規定される場合、データ主体から個人データを取得しない場合に関する情報通知義務の例外が認められる。

#### 6. 削除権 (忘れられる権利) [第17条第3項 (b)]

データ主体は、自己の個人データを管理者に不当に遅滞することなく削除させる権利を持つ。ただし、EU 法または加盟国法を順守する上で当該データが必要な場合には、当該削除義務は免除される。他方で GDPR は、EU 法または加盟国法における法的義務を順守するために必要な場合には、当該データは削除されなければならないとも規定している。

#### 7. プロファイリングを含む自動化された個人意思決定 [第22条第2項 (b)]

データ主体は、当該データ主体に対して法的効果をもたらすなどの自動化された処理のみに基づいた決定に服さない権利を有する。しかし、管理者が従う EU 法または加盟国法によって決定が認められた場合には当該権利は適用されない。

#### 8. 制限 [第23条第1項]

EU 法または加盟国法は、特定の管理者の義務およびデータ主体の権利の適用範囲を制限することができる。

#### 9. 共同管理者 [第26条第1項]

複数の管理者が共同して処理の目的および手段を決定する場合、データ主体の権利行使に関する事項およびデータ主体に対する情報通知に関する管理者の義務の範囲などについて、EU 法または加盟国法で規定することができる。

#### 10. 管理者または処理者の権限に基づく処理 [第29条]

処理者、および管理者または処理者の権限に基づき行動し、個人データにアクセスできる者は、管理者からの指示以外に基づいて当該データを処理してはならないが、

EU 法または加盟国法で異なる規定を設けることができる。

#### 11. 処理に関するセキュリティ [第32条第4項]

EU 法または加盟国法は、管理者または処理者の権限に基づき行動する個人データへのアクセス可能な自然人が法律で定められる特定の事由に基づいて個人データの処理を行うことを明確に要求することができる。

#### 12. データ保護影響評価 (DPIA) [第35条第10項]

加盟国の監督当局は、DPIA が必要となる処理行為のリストおよび DPIA が必要とならない処理行為のリストを作成し公表することができる。特に DPIA が必要となる処理行為のリストが作成・公表された場合には、日本企業としては特にその内容を注視し、DPIA が必要な処理行為を正確に把握すべきである。また、加盟国の監督当局は、処理が法的義務の順守または公共の利益などのために必要な場合 [第6条第1項 (c) (e)] に関して、DPIA が要求されない例外事由のリストを規定することができる。処理を規制する加盟国法との関係で DPIA が既に実施されている場合、加盟国は DPIA の義務を免除することができる。

#### 13. データ保護責任者の選任・地位 [第37条、第38条]

EU 法または加盟国法は、データ保護責任者の選任が義務的である場合について、規定することができる。加盟国法上のデータ保護責任者の選任義務が、GDPR 上のそれとして取り扱うこととされているため、ドイツをはじめ、実務的に大きなインパクトを日本企業にもたらすこととなると思われる条項である。

#### 14. 特定の状況における法令上の例外 [第49条]

公共の利益に関する重大な理由により、加盟国は、特別カテゴリーの個人データの十分性認定のない第三国などへの移転を制限することができる。ここでいう「法令上の例外」には「明示的な同意」によるデータ移転も含まれるため、特別カテゴリーの個人データ、例えば健康データ(健康診断の結果)を従業員の明示的な同意によって EEA 外に移転させることが禁止されることも、加盟国法の内容によっては、理論的にはあり得る、というこ

とを意味する。本条項は、GDPR のデータ移転規制の対応を、データ主体の明示的な同意の取得によってではなく、SCC (標準契約条項) によって行うことが望ましいと言える理由の一つでもある条項である。

#### 15. 罰則 [第84条第1項]

加盟国は、GDPR 違反に適用されるその他の罰則、特に第83条による制裁金が課されない違反行為に関する規定を定めなければならない。

#### 16. 国民識別番号の処理 [第87条]

加盟国は、国民識別番号または一般に用いられるあらゆる識別子の処理に関する特定の条件をさらに決定することができる。

#### 17. 雇用に関する処理 [第88条第1項]

加盟国は、法令などによって、職場における被雇用者の個人データ(いわゆる、従業員データまたは)人事データ処理に関する権利などを確保するために、規定を定めることができる。多くの日本企業に影響を与えることとなると予想される条項の一つである。

#### 18. 守秘義務 [第90条第1項]

加盟国は、職業上の守秘義務等に関連し、監督当局の調査権限を確実にするための特定の規定を採択することができる。

上記のほか、GDPR では、公的機関による処理または公共の利益に関する処理等において、事前相談 [第36条第5項]、認証機関 [第43条]、制裁金 [第83条第7項]、処理ならびに表現および情報の自由 [第85条第1項、第2項]、処理および公文書に対する一般のアクセス [第86条]、公共の利益における保管目的等の処理に関する保護措置および例外 [第89条第2項、第3項]、教会および宗教組織の既存のデータ保護ルール [第91条第1項] に関して、加盟国が国内法でルールを規定できると定めている。

