GDPR関連資格をとろう！QAで学ぶGDPRとCookie規制(53):GDPR遵守の監督・執行

2022/04/15　コンプライアンス, 情報セキュリティ, 個人情報保護法, 外国法

今回から，企業によるGDPR遵守の監督・遵守に関する以下の事項について解説することとし，今回は以下の(1)と(2)に関し解説します。

(1)自己統制と市民による統制

(2)行動規範およびデータ保護認証

(3)監督機関とその権限

(4)欧州データ保護会議（EDPB）

(5)欧州データ保護監督官(EDPS)

(6)主任監督機関ガイドライン

なお，本稿で，「EU域内」，「EU域外」とは，GDPRはEU以外の国も含む欧州経済領域(European Economic Area：EEAに適用されるので，実際には「EEA域内」，「EEA域外」ですが，記述の都合上，「EU域内」，「EU域外」とします。

【目　　次】

（各箇所をクリックすると該当箇所にジャンプします）

Q1：自己統制と市民による統制とは？

Q2：行動規範とは？

Q3：データ保護認証制度とは？

Q1：自己統制と市民による統制とは？

A1：以下の通りです。

１．自己統制

GDPR遵守の最も有効な手段は，管理者または処理者の自主的遵守です。これには，特に，GDPR上の以下に関する規定が含まれます。

・説明責任(5(2)，24)

・管理者による処理者の監督(28)

・個人データ侵害通知(33，34)

・データ保護影響評価(DPIA)(35，36)

・データ保護監督者(DPO)の選任(37～39)

・行動規範・データ保護認証(40～43)

このうち，行動規範・データ保護認証についてはQ2とQ3で解説します。

２．市民等による統制

GDPR遵守の監督は，以下の(a)～(f)の手段を用いた，市民やプライバシー活動団体による統制によっても間接的になされ得ます。

(a)GDPR上のデータ主体の権利の行使

【例】透明性(13,14)／アクセス・訂正・消去・処理制限請求権(15～18)／データ・ポータビリティーの権利(20)／処理禁止権(21,22)／個人データ侵害に関し通知を受ける権利(34)。

(b)GDPR違反に対する救済

データ主体は次のような権利を有します。

(i)GDPR違反の処理について，a) データ主体の常居所(habitual residence)・勤務地またはb)違反行為地，の加盟国の監督機関に苦情を申立てる(lodge a complaint)権利(77(1))。

(ii)監督機関の決定(58条是正措置・83条制裁金等)および監督機関による苦情申立への対応(3か月以内)懈怠に対する不服申立訴訟(78)。

(iii)管理者または処理者(以下「管理者等」)によるGDPR違反の処理に対する実効性ある法的救済(差止訴訟等)(effective judicial remedy)(79(1))，損害賠償請求権(82)。- この差止または損害賠償請求訴訟は，a) 管理者等の拠点のある加盟国またはb)原則としてデータ主体の常居所(habitual residence)がある加盟国の裁判所で提起することができます(79(2)，82(6))。

(c)代表訴訟(Representative/group/class/collective action/litigation/case)

データ主体は，加盟国法に従い組織された公益・非営利(not-for-profit)の個人データ保護活動団体に対し，自己に代わり，上記各権利の行使を委任する(mandate)ことができます(80(1))。

また，加盟国は，苦情申立・監督機関への不服申立て訴訟(78)・管理者等に対する差止等の訴訟(79)に関し，国内法により，これら団体にデータ主体とは独立した権利を付与することができます(80(2))。

(d)データ主体の損害賠償請求権

データ主体は，管理者等によるGDPR違反の処理により蒙った物的損害・非物的損害[精神的損害を含む] (material or non-material damage)について管理者等から賠償を受ける権利を有します(82(1))。

管理者は，自己が関与したGDPR違反の処理から発生した損害の賠償責任を負います。

処理者は，GDPR上の処理者の義務または管理者の適法な指示に違反した場合当該損害の賠償責任を負います(82(2))。

管理者等は，当該損害の発生に何ら責任がないことを証明した場合に限り賠償責任を免れます(82(3))。

複数の管理者等が同一の処理に関し損害賠償責任を負う場合(*)，データ主体に対しては各管理者等がその損害全部について賠償する責任を負います(82(4))。　但し，損害の全部を賠償した管理者等は他の管理者等に対し，その責任割合に応じ求償請求(claim back)することができます(82(5))。[(*) 特に，管理者・処理者間の他，共同管理者(26)間で考えられます。]

(e)内部通報制度による通報

EUにおいては，2019年10月7日に「内部通報指令」が成立しましました(加盟国2021年10月までに同指令の内容を自国国内法に反映)。

同指令に基づく通報の対象には，プライバシーまたは個人データの保護，ネットワーク または情報 システムのセキュリティーに関するEU法違反も含まれています。また，既に国内法で内部通報に関する法制度を有する加盟国もあります。

従って，企業の従業員等は，これらの内部通報制度に従い，GDPRまたはePrivacy指令違反を通報することも可能でしょう。

(f)市民等による統制の実例

以下のような市民(または市民から委任を受けた市民団体)から監督機関への苦情申立を端緒とするCJEU先決裁定・判決または監督機関の決定の例があります。

・2014年： Google検索に関する「忘れられる権利」先決裁定　- 第34回Q5参照。スペイン市民

・2015年：CJEU「セーフハーバー」無効判決　- 第50回Q3参照。オーストラリア人Maximilian (Max) Schrems氏。同氏は2017年にプライバシー活動団体"NOYB - European Center for Digital Rights"[1]を創設。

・2019年1月：仏監督機関CNILによる米Googleに対する5,000万ユーロ(約60億円)の制裁金決定　上記のNOYBともう一つのプライバシー活動団体"La Quadrature du Net" (LQDN) [2]

・2019年7月：Facebook「いいね(Like)」ボタン事件CJEU先決裁定　- 第45回Q1参照。ドイツの消費者保護団体Verbraucherzentrale NRW

・2020年7月：CJEU「プライバシーシールド」無効判決　- 第50回Q3参照。オーストラリア人Maximilian (Max) Schrems氏。

page top

Q2: 行動規範とは？

A2:行動規範の制度も，企業の自己統制の手段の一つと言えます。以下，その概要を解説します。

但し，企業が行動規範に参加しまたは認証を取得していることだけでは，これら企業に対する監督機関の権限行使を何ら妨げるものではありません(without prejudice to) (41(4),42(4))。

１．行動規範およびその作成・承認

加盟国，監督機関，欧州データ保護会議(EDPB)および欧州委員会は，各業界の特性および中小零細企業(small and medium-sized enterprises)の特殊事情を踏まえた行動規範の作成を奨励しなければなりません(40(1))。

各業界等の団体は，当該業界等の事情に応じたGDPRの具体的適用に関し行動規範を作成することができます(40(2))。

行動規範は，第3条によりGDPRの域外適用を受ける管理者等も対象とし，第46条に定める個人データのEU域外への移転を適法に行うための「適切な保護措置」(appropriate safeguard)(46(2)(e))とすることができます。但し，これらEU域外の参加者は，契約等によりこの「適切な保護措置」を講じる法的義務を負うことに合意しなければなりません(40(3))。

行動規範には，監視組織による行動規範遵守の監視(monitoring)の仕組み(mechanisms)を定めなければなりません(40(4))。行動規範(またはその改訂もしくは追加。以下同じ)の承認申請を行う業界団体等は，管轄監督機関に対し，行動規範案を提出しなければなりません(40(5))。

管轄監督機関は，その案がGDPRに適合しまたは「適切な保護措置」であると認めた場合は，これを承認(approve) (40(5))，登録および公表(40(6))しなければなりません。但し，行動規範案が複数加盟国における個人データ処理を対象とする場合，管轄監督機関は，これを，その承認前にEDPBに送付(63)しなければなりません。

EDPBはその案がGDPRに適合しまたは「適切な保護措置」であるかに関し自己の見解を述べなければなりません(40(7))。EDPBは，その案がGDPRに適合しまたは「適切な保護措置」であると認める場合はその見解書を欧州委員会に送付しなければなりません(40(8))。

欧州委員会は，EDPBから送付された承認済み行動規範がEU全域に適用可能であると判断した場合，その旨の決定をすることができ(40(9))，同決定を周知しなければなりません(40(10))。

EDPBは，全ての承認済み行動規範を登録し公開しなければなりません(40(11)。

２．行動規範の遵守監視

承認された行動規範の遵守の監視(monitoring)は，管轄監督機関が認定する(accredit)組織(以下「監視組織」という)が行います(41(1))。

監視組織として認定されるための要件は次の通りです(41(2))。

(a)組織の独立性(independence)および専門性が証明されたこと

(b)参加企業の監視と，その定期的見直しの手続を確立していること

(c)行動規範違反等に対する苦情に対応するための体制を確立し，かつ，これらについて公衆およびデータ主体に情報提供すること(transparent)

(d)監視組織としての任務と義務について利益相反(conflict of interests)の問題がないことを証明したこと

各管轄監督機関は，監視組織の認定基準案を作成し，一貫性制度[EU全域におけるGDPRの一貫した適用を確保するための制度](63，64)に従い，これをEDPBに送付(63)しなければなりません(41(3))。

認定された監視組織は，参加企業が行動規範に違反した場合，違反企業に対する行動規範適用の一時停止または除名等，適切な措置をとり，これを管轄監督機関に通知しなければなりません(41(4))。

監督機関は，監視組織が認定要件不適合またはGDPR違反の場合，認定を取消さなければなりません(41(5))。

３．行動規範ガイドライン

行動規範については，2019年6月4日に，欧州データ保護会議(EDPB)から次のガイドラインが公表されています。

"Guidelines1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679"(GDPRに基づく行動規範およびその監督団体に関するガイドライン)- Version 2.0(最終版)

このガイドラインには，行動規範の承認申請団体(Code owners)から監督機関への承認申請，監督機関による行動規範案の評価・承認・公表等の手続，行動規範の内容に関する要件等が記載されています。

page top

Q3: データ保護認証制度とは？

A3:データ保護認証(data protection certification)の制度も，企業の自己統制の手段の一つと言えます。以下，その概要を解説します。

１．認　証(Certification)

加盟国，監督機関，欧州データ保護会議(EDPB)および欧州委員会は，特にEU レベルで，個人データの処理がGDPRに適合していること(compliance)を証明(demonstrate)するため，データ保護認証(data protection certification)ならびにデータ保護シールおよびマーク(data protection seals and marks)(以下総称して「認証」という)制度の確立を推進しなければなりません。この場合，中小零細企業のニーズを考慮しなければなりません(42(1))。

認証は，第3条によりGDPRの域外適用を受ける管理者等も対象とし，第46条に定める個人データのEU域外への移転を適法に行うための「適切な保護措置」(appropriate safeguard)(46(2)(f))とすることができます。

但し，これらEU域外の管理者等は，契約等によりこの「適切な保護措置」を講じる法的義務を負うことに合意しなければなりません(42(3))。

認証の利用は任意(voluntary)とされます(42(3))。

認証は，後述の認証組織(certification body)または管轄監督機関から，その管轄監督機関(58(3))またはEDPB (63)が承認した基準に基づき，発行されるものとされます(43(5))。

管理者等は，認証組織または管轄監督機関に対し認証申請を行います(42(6))。

認証期間は最長3 年とし，更新可能。認証要件を満たさなくなった場合認証は取消されます(42(7))。

EDPBは，全ての認証を登録し公開します(42(8))。

２．認証組織(Certification bodies)

認証組織としての認定(accreditation)は，管轄監督機関または所定の加盟国認定機関(national accreditation body)が，監督機関またはEDPBが承認した基準(criteria)(以下「認証組織認定基準」という)に従い行います(43(1),(3))。

認定要件は以下の通りです(43(2))。

(a)組織の独立性(independence)および専門性が証明されたこと

(b)認証組織認定基準の遵守に合意すること

(c)認証の発行(issuing)，定期的見直しおよび取消の手続を確立していること

(d)違反等に対する苦情に対応するための体制を確立し，かつ，これらについて公衆およびデータ主体に情報提供すること(transparent)

(e)認証組織としての任務と義務について利益相反(conflict of interests)の問題がないことを証明したこと

認証組織は，最長5 年で更新可能(42(4))。

EDPBは，全ての認証制度(certification mechanisms)およびデータ保護シール(data protection seals)を登録し公開します(43(6))。

監督機関または加盟国認定機関は，認証組織が認定要件不適合またはGDPR違反の場合，認定を取消さなければなりません(43(7))。

３．認証ガイドライン

EDPBは，認証の基準に関し，2019年6月4日，以下のガイドライン案を公表しました。

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation Version 3.0

今回は以上です。

【筆者の最近の個人情報保護関連書籍】

NEW!! “China Data and Personal Information Laws” 2022/1/31

「中国におけるセキュリティ脆弱性情報の取扱い規制('21年9月施行)」2022/01/05

『中国「ネットワークデータ安全管理条例(意見募集稿)」の公表とその概要』2021/11/18

「中国個人情報保護法への対応事項リストと国外提供規制」2021/09/24

「中国データ・情報関連法」 2021/9/18

「改正個人情報保護法アップデート(ガイドラインの公表)」2021/08/10

「中国データセキュリティ法の成立とその概要」2021/06/18

「Q&Aで学ぶCPRA カリフォルニア州プライバシー権法」 2020年12月

「Q&Aで学ぶCCPA カリフォルニア州消費者プライバシー法」 2020年7月

「GDPR関連資格CIPP/E準拠 詳説GDPR (上)- GDPRとCookie規制」 2019年11月

「GDPR関連資格CIPP/E準拠 詳説GDPR (下)- GDPRとCookie規制」 2019年11月

page top

[3]

【注】

---

[1] 【NOYBのサイト】 こちら

[2] 【LQDNのサイト】 こちら

[3]

＝＝＝＝＝＝＝＝＝＝＝

【免責条項】

本コラムは筆者の経験にもとづく私見を含むものです。本コラムに関連し発生し得る一切の損害などについて当社および筆者は責任を負いません。実際の業務においては,自己責任の下,必要に応じ適宜弁護士のアドバイスを仰ぐなどしてご対応ください。

【筆者プロフィール】

浅井 敏雄 （あさい としお）

企業法務関連の研究を行うUniLaw企業法務研究所代表／一般社団法人GBL研究所理事

1978年東北大学法学部卒業。1978年から2017年8月まで企業法務に従事。法務・知的財産部門の責任者を日本・米系・仏系の三社で歴任。1998年弁理士試験合格（現在は非登録）。2003年Temple University Law School （東京校）Certificate of American Law Study取得。GBL研究所理事，国際商事研究学会会員，国際取引法学会会員，IAPP （International Association of Privacy Professionals）会員，CIPP/E （Certified Information Privacy Professional/Europe）

【発表論文・書籍一覧】

https://www.theunilaw2.com/

シェアする

: