P&I 特別回報

第 17-016 号
2018 年 3 月 16 日

日本船主責任相互保険組合

外航組合員各位

EU一般データ保護規則 2016/679 施行について
（概要案内）

序文

一般データ保護規則（General Data Protection Regulation、以下”GDPR”または”当該規則”）を含む EU 規則 2016/679 が本年 5 月 25 日に発効することにより、EU/EEA 域内に直接的な影響を与えることが見込まれます。[1]　当該規則（全 88 ページ）は、以下 URL よりご参照頂けます。：http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

当該ご案内は、GDPR に関し当組合および組合員に関係する箇所を簡潔にご紹介することを目的とするものです。当該規則による影響のほとんどは、傷病等の人身損害やその他個人に関する情報が伴うクレームにおけるものと見込まれます。個人情報を含まない法人に関する情報や個人に関係しない情報には、当該規則は影響しません。

当該規則は、現行の 95/46/EC 指令に代わり、個人データの収集、保管、処理、アクセス、利用、移転および削除に関する手続きを EU/EEA 域内で強化・統一することを広く意図するものであり、個人情報の”管理者”と”処理者”の責任を明確化することで、個人に対し、法的拘束力のある権利と遵守のための監督・執行の枠組みを、域内で同水準にて提供することを目的としています。

GDPR の目的は情報の処理において個人を保護することです。当該規則の適用対象には EU/EEA 域内において域内外の個人に関する情報を保持している者だけでなく、域外に所在し域内の個人に商品やサービスを提供している者や域内の組織から個人データを受領している者も該当します。当組合は域内で事業を展開しており、また域内の組織から受領した個人データを処理していることから、当該規則の対象となります。同様に、組合員や取引業者におかれても、EU/EEA 域内で事業を展開したり、域内の個人に商品やサービスを提供したり、域外に所在する個人に関する情報を域内で保管している場合、当該規則の対象となります。

違反に対する制裁金

新制度下での制裁金の水準は、現行制度に比べ大幅に引き上げられます。制裁金の額は個々のケースにおいて関係する要因の内容によって異なり、その要因には違反の性質および期間、データ主体への被害の軽減措置の実施を含みますがこれに限定されません。しかしながら、規則違反に対する制裁金が、一定条件下では、最大 2,000 万ユーロ、または企業の場合、前年度全世界売上高の 4%のいずれか高い方とされていることは注意しておく必要があります。

[1] ここでの EU/EEA とは、EU 加盟国と 3 つの EFTA 加盟国(アイスランド、リヒテンシュタイン、ノルウェイ)を合わせた、欧州経済領域(The European Economic Area 、”EEA”)を指します。

関連用語の定義[2]

- **"個人データ"** とは、データ主体に関するあらゆる情報を指します。

- **"データ主体"** とは、識別された、または識別され得る生存する自然人または個人であり、氏名、識別番号、所在地データ、オンライン識別子や、一つ以上の身体的、生理学的、遺伝的、精神的、経済的、文化的、社会的独自性に関する要因により、直接的または間接的に識別され得る人を指します。

- **"管理者"** とは、単独または共同で個人データの処理の目的と手段を決定する自然人、法人、公共団体、代理人またはその他の組織を指します。

- **"処理者"** とは、管理者に代わり個人データの処理を行う自然人、法人、公共団体、代理人またはその他の組織を指します。

- **"処理"** とは、その手段が自動か手動に関わらず、個人データまたは個人データの集合に対して行われる、あらゆる単一の作業または一連の作業であり、例えば、取得、記録、編集、構造化、保存、修正または変更、復旧、参照、利用、送信による開示、周知または周知を可能にすること、整理または結合、制限、消去または破壊することを指します。

組合、組合員、保険仲立人、取引業者およびクレーマントの役割

当組合は、当該規則上の自身の役割は”管理者”にあたると考えております。

さらに、GDPR が適用される場合において、組合員、保険仲立人、また、コレスポンデントやサーベイヤー、その他の専門家といった取引業者も、各自において当該データの処理の目的と手段を決定していると考えられることから、概して管理者であると考えております。もし処理者が処理の目的と手段を決定しているならば、処理者はその処理における管理者であると見做されます。[3]

これらは、傷病などの人身クレームのように、個人データを含む問題でのみ関係するものであり、その場合、クレームを提起した本人（達）が GDPR 上の権利を享受するデータ主体となります。

GDPR における関連要件

- 個人データの処理に関する原則
- データ主体の権利
- 管理者と処理者の責任
- データ保護監督機関への通知義務
- データ保護責任者の選任、および
- 第三国への個人データの移転

[2] GDPR, Article 4
[3] GDPR, Article 28

個人データの処理に関する原則[4]

個人データの処理に関する原則の概要は以下の通りです。

- 適法性[5] – 個人データの処理に際しては、同意、契約、データ主体の重大な利益を保護するため、もしくは管理者が法的義務を遵守するために必要である場合の法的義務等の法的根拠がなければならない。

- 公平性 – 個人データの処理に携わる者は、データ主体に対し、その処理とデータ主体の権利について十分な情報を提供しなければならない。

- 透明性 – 情報は、簡潔且つ容易に理解できるように伝えられなければならない。

- 目的の限定 – 個人データは、特定の明示された正当な目的のためにのみ収集・処理されなければならず、これらの目的とは無関係の事由により処理されてはならない。

- データの最小化 – 個人データは、その収集および処理の目的に照らして、適切で関連性があり、その達成に必要な範囲に限定されていなければならない。

- 正確性 – 個人データは、正確且つ最新に保たれていなければならない。

- 保管の制限 – 個人データは、処理の目的に必要な期間を超えない間はデータ主体の識別を可能とする形式で保持しなければならない。

- セキュリティ – 個人データは、不正・違法な処理や偶発的な滅失・破壊・損壊から適切な手段により、安全に保護されていなければならない。

個人データ

個人データの処理は、明示的同意がある場合、法的請求の立証、行使、弁護の結果として必然であった場合、裁判所がその司法権に基づき実行した場合など特定の状況で無い限り禁止されています。[6] しかしながら、全ての組合員およびその共同被保険者、保険仲立人、代理人等におかれては、認容された根拠に基づき個人データを処理できるよう、当該規則上適切な同意の文言の契約、雇用契約、労働協約、運送約款等への挿入を検討されることをお勧めします。未成年者を巻き込むクレームでは一層厳しい規則条件が適用されるため、この点がクレーム処理において特に重要となります。

データ主体の人種、民族的背景、宗教的・政治的信条及び健康や医療に関する情報等を含む機微情報（特別な種類の個人データ）には、特別且つより厳格な要求が適用されます。

[4] GDPR, Chapter II
[5] GDPR, Article 6
[6] GDPR, Chapter II, Articles 7 および 9

データ主体の権利[7]

以下は、情報を要求する権利など、データ主体が持つ権利をまとめたものです。

- 透明性と情報 – 管理者の詳細や当該個人データの処理の目的を含め、要求した情報の提供を受ける権利[8]（データ主体へのデータの開示先の通知を含む）

- アクセス権 – 個人データが処理されたか否かとその目的の確認を要求し、またそのデータにアクセスできる権利[9]

- 訂正権 – 不正確な情報を訂正する権利[10]

- 忘れられる権利 – 一定の条件下において、自己の個人データを過度な遅滞なく削除するよう要請する権利[11]

- 制限権 –個人データの正確性に異議がある場合などにおいて、管理者に対し、データ処理の制限を要請する権利

管理者と処理者の責任

管理者

管理者には、当該規則に基づき、個人データの処理において適切な措置を講じることが求められます。[12] その中には、データ保護指針の制定・実施やその他以下のような特定の要件への適合が含まれます。

- *目的に必要最小限の個人データの処理* – 目的のために必要な個人データのみが処理されることを保証しなければならない。[13]

- *処理者* – 処理者が GDPR を遵守するための措置を実施していることを保証しなければならない。

管理者は当該規則への遵守について立証責任を負っています。[14]

当組合は自身を管理者として認識しています。また、組合員およびその共同被保険者も、船員やクレーマントから受領した個人データの管理者となります。

[7] GDPR, Chapter III
[8] GDPR, Chapter III, Articles 12, 13 および 14
[9] GDPR, Chapter III, Article 15
[10] GDPR, Chapter III, Article 16
[11] GDPR, Chapter III, Article 17
[12] GDPR, Chapter IV, Article 24
[13] GDPR, Chapter IV, Article 25
[14] GDPR, Article 5

処理者

処理者は、管理者に対し、当該規則の要件に適合した処理の実施と、データ主体の権利の確保のために適切な技術的・組織的措置を取っていることを保証しなければなりません。[15] 管理者と処理者の間では、特定の要件を遵守するための、別段の契約や同意書を取り交わさなければなりません。

管理者と処理者は共に次の事由に対する責任を負います。

- 処理の記録 – 処理の記録を維持・管理し、監督機関の検査時にその求めに応じられるようにしなければならない。[16]

- 処理のセキュリティ – 適切なセキュリティ対策が講じられていなければならない。[17]

監督機関への通知義務

管理者は、データ主体の権利と自由を侵害する事態が発生した場合、自身を管轄する監督機関に個人データの侵害[18]を通知します。また、処理者は、当該規則への違反を認識したら管理者に通知する義務があります。[19]

データ保護責任者

個人データを大規模に処理する場合などの特定の条件下では[20]、データ保護責任者（Data Protection Officer、“DPO”）を選任する義務があります[21]。 データ保護責任者は GDPR への遵守状況のモニターを含め、報告や内部へ助言を行うなどの特別な責務を負います。当組合は今後 DPO を選任する予定です。

第三国へのデータ移転

第三国、すなわち EU/EEA 域外へデータ移転を行うためには、正当な法的根拠または GDPR 上の認容された例外事項の適用（例：人損などのクレーム提起において法的義務により第三国へのデータ移転が必須である場合等）が無い限り、欧州委員会がその第三国をデータ保護において十分な水準にあると認定していること[22]、もしくはその第三国の管理者または処理者[23]が十分なセキュリティ水準を整備している（またはその予定である）ことのいずれかが求められます[24]。

---

[15] GDPR, Article 28
[16] GDPR, Chapter IV, Article 30
[17] GDPR, Chapter IV, Article 32
[18] GDPR, Article 33
[19] 当組合が EU の拠点を置く英国の監督機関は Information Commissioner’s Office(ICO)となります。
[20] GDPR, Chapter IV, Article 37, 38 および 39
[21] 当組合のデータ保護責任者(DPO)の連絡先は後日当組合ホームページに掲載予定です。
[22] 本回報発行時点における十分性認定国はアンドラ、アルゼンチン、カナダ(民間部門)、フェロー諸島、ガーンジー島、イスラエル、マン島、ジャージー島、ニュージーランド、スイス、ウルグアイ、米国(プライバシーシールド)であり、日本と韓国は認定に向け政府間交渉が進められています。詳細につき、欧州委員会ウェブサイトをご参照下さい。
[23] GDPR, Chapter V
[24] GDPR; Chapter V, Article 49.1

特定の状況下では、データ移転に際し、その第三国の管理者または処理者と EU 標準契約条項を利用して契約締結を行うことも適切な対応と見做されます。
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

GDPR が組合と組合員にとって持つ意味、取るべき対策

当組合では、GDPR に対応するため今後以下のような対策を講じるべく対応しています。

- プライバシーポリシーの更新
- データ保護責任者の選任
- データの取り扱いに関する社内規則の更新・見直し、等

組合員への更なる影響

EU/EEA 域内で事業を展開したり、域内の個人に商品やサービスを提供したり、域外に所在する個人に関する情報を域内で保管している組合員は、同様の対応を取る必要があるかもしれません。当該規則の対象となる組合員には以下の点を中心に見直しを行うことをお勧めします。

- データ保護指針の更新または制定及び実施
- （個人データを大規模に処理している場合）データ保護責任者の選任の検討
- データ主体が個人データの処理と自身の権利について適切な情報を受け取れることを保証する業務フローを整備すること
- その情報の保管継続を行うための合理的理由が無い限り、不要となった個人データを削除すること
- 機微な個人データと定義されるもの（例：健康や医療情報等）の第三者とのやり取りにおいてセキュリティを高めること
- 第三国へのデータ移転が、法的根拠や別途の同意書がある等の容認される状況のみ行われよう、更なる確認体制を整備すること

本回章は法的見解をご提示するものではありません。組合員におかれましては、GDPR での要求に即した業務フローへ変更をされる際には、弁護士や自身を管轄するデータ保護監督当局に照会することをお勧めします。

当該回報に関するご質問やご意見につきましては、当組合契約窓口もしくは企画部へご連絡下さい。

国際 P&I グループの全てのクラブが類似した内容の回報を発行しています。

以上