CIRCULAR

The Standard for service and security

Standard Club

組合員の皆様

2018 年 2 月 28 日

EU 一般データ保護規則 2016/679（EU General Data Protection Regulation 2016/679）の実施と組合員の皆様に対する一般ガイダンス

概要

一般データ保護規則を含む規則（EU）2016/679（以下、「**GDPR**」または「**規則**」と言います）が 2018 年 5 月 25 日に発効し、EU/EEA[1]に直接的な影響を及ぼすようになります。規則は、同時に発効が予想される 2018 年データ保護法（Data Protection Act 2018）のもとで英国の法律に摂取されます。約 88 ページの規則は、以下のリンクからご覧いただけます。

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

本一般ガイダンスは、GDPR のうち、当クラブと組合員の皆様に関係する部分だけをご紹介するのが目的です。規則によって、自然人、すなわち生存する個人に由来するデータが関わる人身傷害や疾病その他のケースに関連したクレームが特に影響を受けることになるでしょう。個人情報を含まないデータや自然人に関係のない情報は影響を受けず、GDPR の適用範囲外です。ただし、こうしたデータによって（他のデータとの組み合わせで）自然人の特定が可能になる場合は適用範囲内になります。

規則の主な趣旨は、データ保護指令 95/46/EC に代わり、個人データの収集、保管、処理、アクセス、使用、移転、消去に関する EU/EEA の手続きを強化し、調和させることです。個人データの「管理者」と「処理者」の責任を規定することで、EU/EEA 全域において同水準の強制力のある法的権利と、順守を確実にするための監督ならびに実施の枠組みを自然人に提供することが目的です。

GDPR の狙いは、個人データの処理に関して自然人を保護することです。規則は、個人データの保持や取り扱いをする EU/EEA 域内の者のほか、域外で（i）EU 域内に管理者や処理者を設置して活動する状況において個人データを処理する者、（ii）EU 域内で自然人に商品やサービスを提供する者、（iii）EU 域内における自然人の行動を監視する者にも適用されます。スタンダードクラブは EU/EEA 域内

[1] EU/EEA とは、本文書では、EU（欧州連合）加盟国と EFTA（欧州自由貿易連合）加盟国 3 カ国（アイスランド、リヒテンシュタイン、ノルウェー）を合わせた欧州経済地域（EEA）を意味します。

The Standard Club Europe Ltd
www.standard-club.com
Registered in England No. 17864. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority FRN 202805

Managers' London Agents: Charles Taylor & Co. Limited. Registered in England No. 02561548
Authorised and regulated by the Financial Conduct Authority FRN 785106

Registered Address: Standard House, 12–13 Essex Street, London WC2R 3AA, UK
Telephone: +44 20 3320 8888 Email: pandi.london@ctplc.com

Charles Taylor

で活動しているため、GDPR が適用されます。同様に規則は、組合員の皆様、EU/EEA 域内で事業活動を行ったり、EU 域内の自然人に商品やサービスを提供したりしている第三者のサービス提供者、EU/EEA 域内で処理された EU/EEA 域外の個人に関する個人データにも適用されます。また、EU/EEA の企業との契約上の義務によって EU/EEA の自然人に由来するデータを処理する EU/EEA 域外の組合員にも適用される可能性があります。

規則違反に対する罰則

新制度における行政罰金の金額は、以前の法律（データ保護指令 95/46/EU（Directive 95/46/EU）とそれを実施する法律―英国の場合には 1998 年データ保護法（Data Protection Act 1998））よりも大幅に高くなっています。罰金の金額は個々のケースにおける複数の要因によって決まり、その中には違反行為の性質や期間、データ主体の被害を軽減するためにとられた行動などが含まれますが、それだけに限定されません。ただし一部の条項に関しては、GDPR 違反の罰金は最高で 2000 万ユーロまで、企業の場合には前会計年度の世界年間売上高の最高 4%のどちらか高い方までとなる可能性があることは注目すべきです。

関連用語の定義[2]

- 「**個人データ**」（personal data）とは、データ主体に関連したあらゆる情報を意味します。
- 「**データ主体**」（data subject）とは、特定された、または特定可能な生存する自然人、すなわち個人を意味します。氏名や認識番号、位置情報、オンライン ID、またはその自然人の身体的、生理的、遺伝的、精神的、経済的、文化的または社会的アイデンティティに固有の 1 つ以上の要素を参照することで、直接的または間接的に特定され得る個人を意味します。
- 「**管理者**」（controller）とは、単独または他者と共同で、データ処理の目的、条件、手段を決定する自然人または法人、公共機関、政府機関またはその他の組織を意味します。
- 「**処理者**」（processor）とは、管理者に代わって個人データを処理する自然人または法人、公共機関、政府機関またはその他の組織を意味します。
- 「**処理**」（processing）とは、自動か手動かによらず、収集、記録、整理、構造化、保管、適合、変更、回復、参照、使用、送信による開示、配布またはその他の手段による普及、調整または組み合わせ、制限、消去または廃棄など、個人データあるいは個人データの集合に対して行われる単独または一連のあらゆる作業を意味します。

[2] GDPR 第 4 条より抜粋

CIRCULAR

Standard Club

スタンダードクラブ、組合員、ブローカー、外部のサービス提供者、クレイマンツの役割

スタンダードクラブは、本規則の管理者（controller）にあたると考えています。当クラブは管理を全面的に Charles Taylor & Co (Bermuda)に委託しており、同社は日常業務をロンドンの Charles Taylor & Co. Limited や Charles Taylor グループ内の会社（以下、「クラブ管理者」（managers）と言います）に委託しており、ほとんどの場合、共有管理者（controller in common）としての役割を果たしています。これによって当クラブは、クラブ管理者が構築した GDPR の枠組みのもとで業務を行うことが可能になり、クラブ管理者は、管理者（controller）あるいは共同管理者（joint controller）だけに認められている管理作業を実施できるようになります。クラブ管理者はまた、スタンダードクラブを代表して関係監督当局と対応することが可能になります。

GDPR が適用される場合、組合員やブローカー、組合のコレスポンデンツやサーベイヤーなど外部のサービス提供者が管理者としての役割を果たすのか処理者としての役割を果たすのかは、サービス提供者が特定の状況における個人データ処理の目的と手段を決定しているかどうかに依ります。これが関係してくるのは、人身傷害や疾病のクレームなどの案件に個人データが含まれている場合のみです。その場合は、クレームを提起する個人がデータ主体となり、GDPR が付与する権利の恩恵を受けることになります。

スタンダードクラブは、例えばコレスポンデンツは通常は処理者であるという見解をとっています。これは以下の前提に基づくものです。(i) コレスポンデンツは、組合員ならびに／またはクラブに代わって常にデータを処理している、(ii) コレスポンデンツは、組合員ならびに／またはクラブの要件を満たすための個人データの処理方法についてある程度の自由裁量権を持つものの、その案件への対応におけるコレスポンデンツの個人データの扱い方についての最終的な方向性は組合員ならびに／またはクラブが指示する。さらに、組合員とコレスポンデンツの間で文書の契約が結ばれていない場合でも、コレスポンデンツは自らの目的のために個人データを使用する権限を持たず、実際にもそのような行為は行わない。ただしコレスポンデンツは、例えば以下のような状況においては個人データの管理者になることができます。(i) 個人データを自らの目的のために処理している場合、かつ／または (ii) スタンダードクラブならびに／または組合員と共同であるいは情報を共有して処理の方法と目的を決め、かつ／または (iii) 個人データの処理方法について高い自由裁量権を行使している場合。

関係のある GDPR の要件

- 個人データ処理の原則
- データ主体の権利
- 管理者、共同管理者、共有管理者、処理者の責任
- 関係データ監督当局への通知義務
- データ保護責任者の任命
- 個人データの第三国への移転

個人データ処理の原則[3]

個人データ処理の原則は以下のように要約できます。

- *合法性*[4]— 個人データの処理は、処理に対して同意や契約または法的義務がある場合、データ主体の重大な利益を保護するために必要な場合、管理者の正当な利益のためである場合など、法的根拠がある場合に限定されるべきです。

- *公正性* — 個人データの処理に関与する者は、データ主体に対し、データ処理とデータ主体の権利について十分な情報を提供すべきです。

- *透明性* — 情報は、すぐに理解できるような簡潔な形で提供されるべきです。

- *目的の制限* — 個人データは、具体的で明示された正当な目的のためにのみ収集および処理されるべきであり、これらの目的と無関係の理由で処理されるべきではありません。

- *データの最小化* — 個人データは、収集・処理の目的に照らして関連性があり、かつ必要十分なものだけに制限されるべきです。

- *正確性* — 個人データは、正確で最新のものであるべきです。

- *保管の制限* — データ主体の特定を可能にする形での個人データの保管は、必要な期間に限定されるべきです。

- *安全性* — 個人データは、未承認または違法な処理、事故による喪失、破壊または損傷から保護するために適切な手段によって安全を確保する必要があります。

センシティブな個人データ

「**センシティブな個人データ**」には、具体的でより厳しい要件が適用されます。その中には、データ主体に関する人種、性的志向、民族的背景、宗教、政治的な見解、健康・医療情報が含まれます。

センシティブな個人データの処理は、明示的な同意がある場合、法的なクレームの立証、行使、または弁護に必要と帰着される場合、または裁判所が法的権限において行動している場合など、特定の条件が当てはまらない限り禁止されています[5]。ただし、すべての組合員と共同被保険者、ブローカー、代理店等が、センシティブな個人データを処理するための、適切な（GDPR に準拠した）同意、また

[3] GDPR 第 II 章
[4] GDPR 第 6 条
[5] GDPR 第 II 章第 7、9 条

は別の法的根拠を確保する措置を講じることを推奨します。これは、さらに厳格な GDPR の条件が適用される未成年者が関係しているクレームにおいては特に重要になります。

データ主体の権利[6]

以下は、データ主体が持つ情報請求の権利も含めた多くの権利の要約です。

- *透明性と情報* — データ主体に対し、管理者についての詳細や、個人データを処理する目的など、要求された情報を提供する措置がとられるべきです[7]。これには、個人データの開示先である第三者について、データ主体に通知することも含まれます。

- *アクセスの権利* — データ主体は、個人データの処理の有無、その目的、それにアクセスする権利について、確認する権利を持ちます[8]。

- *訂正の権利* — データ主体は、不正確な個人データを訂正する権利を持ちます[9]。

- *忘れられる権利* — データ主体は、一定の条件が当てはまる場合、自らの個人データを不当な遅滞なしに消去することを要求する権利を持ちます[10]。

- *処理を制限する権利* — データ主体は、例えば個人データの正確性について異論がある場合などは、管理者に処理の制限を求める権利を持ちます。

管理者、共同管理者、共有管理者、処理者の責任

管理者と共同管理者（The controller and joint controller）

管理者と共同管理者は規則に従って個人データの処理のための適切な措置をとることが義務付けられています[11]。その中には、「データ保護方針」や、その他以下のような具体的な要件の確立や実施が含まれます。

- *目的に必要なデータのみ* — その目的に必要な個人データだけが処理されることを、手続きによって確実にする必要があります[12]。

[6] GDPR 第 III 章
[7] GDPR 第 III 章第 12、13、14 条
[8] GDPR 第 III 章第 15 条
[9] GDPR 第 III 章第 16 条
[10] GDPR 第 III 章第 17 条
[11] GDPR 第 IV 章第 24 条
[12] GDPR 第 IV 章第 25 条

- *処理者* — 処理者が準拠した措置を実施したことを、手続きによって確実にする必要があります。

管理者と共同管理者は、規則を順守していることを示す責任があります[13]。

共有管理者（Controllers in common）

共有（in common）という単語は、2 人以上の人が個人データの集合体を共有し、別々に処理している場合に当てはまります。

スタンダードクラブの場合、ほとんどの状況において、クラブとクラブ管理者が共有管理者となることが想定されています。組合員と被保険者は、乗組員やクレイマンツから受領した個人データの管理者になります。

処理者（The processor）

処理者は、データ処理が規則の要件を満たし、データ主体の権利が確実に保護されるように、適切な技術的、組織的措置が講じられていることを管理者に保証する必要があります[14]。管理者と処理者の間で、具体的な要件を順守する別個の契約を結ぶ必要があります。

管理者および処理者は、両者とも以下のことに責任を持ちます。

- *処理の記録* — 処理記録を保持し、関係監督当局による検査のために提供する必要があります[15]。

- *処理の安全性* — 適切な安全措置を確立し、維持する必要があります[16]。

<u>監督当局への通知義務</u>

管理者は、データ主体の権利や自由が影響を受けた場合、GDPR に従い、適切な監督当局に個人データ違反を通知します[17]。処理者は、GDPR 違反に気づいた場合、通知する義務があります[18]。

<u>データ保護担当者（Data Protection Officer）</u>

個人データが大規模に処理されているケース[19]を含む特定の状況においては、データ保護担当者（「DPO」）を任命する義務があります。DPO は、規則の順守の監視、報告、内部への助言などを含む一定の責任を負っています。

[13] GDPR 第 5 条
[14] GDPR 第 28 条
[15] GDPR 第 IV 章第 30 条
[16] GDPR 第 IV 章第 32 条
[17] GDPR 第 33 条
[18]英国の監督当局は、情報コミッショナーオフィス（Information Commissioner's Office）
[19] GDPR 第 IV 章第 37、38、39 条

第三国へのデータ移転

人身傷害クレームなどの保険クレームを行うために、データ移転が必要とされる場合（例えばデータ主体の利益のための契約締結や履行）など、第三国（つまり EU/EEA 域外の国）にデータを移転する正当な法的根拠がない限り、第三国へのデータ移転には、欧州委員会が、当該第三国が十分な保護水準を確立した、または当該第三国の管理者や処理者が[20]適切な安全措置を確立した、または今後確立すると判断することが必要になります[21]。十分な安全措置が求められる場合には、EU 標準モデル条項が適用される可能性があります。

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

スタンダードクラブとその組合員にとっての規則の意味、また取るべき措置は何でしょうか。

5 月の規則発効を見越して、当クラブが取った、または講じている最中である措置の一部は、以下の通りです。

- データ保護方針を確立しました — 同方針の実施は、2018 年 5 月に予定されています。
- 当クラブのルールが改正され[22]、当クラブと組合員の間の、当クラブと組合員による、そして／または当クラブと組合員のための、個人データの共有と処理に関連した条件が、当クラブのウェブサイトに掲載されている、独立したデータ共有契約（data sharing agreement）に含まれていることが明確になりました。
- DPO を任命しました。
- 不必要な個人データの削除を確実にするための定期的な見直しなどを含めるため、社内の手続きやプロセスに関する文書を更新中です。
- 必要とされる場合には、GDPR のもとでの権利を詳細に説明する標準プライバシー通知がデータ主体に発行されます[23]。
- 個人データを含むシステムならびにセンシティブな個人データを含むシステムの双方に関して、IT と通信システムの安全性と整合性が検証されました。

[20] GDPR 第 V 章
[21] GDPR 第 V 章第 46、49.1 条
[22] http://www.standard-club.com/media/2633623/21-december-2017-standard-europe-circular-rule-changes.pdf
[23] GDPR 第 12 条

CIRCULAR

Standard Club

組合員へのさらなる影響

EU/EEA 域内で事業運営する組合員、同地域の個人に商品やサービスを提供する EU/EEA 域外の組合員、または EU/EEA 域外の個人に関して EU/EEA 域内で個人データを保持または処理する組合員、または EU/EEA の企業との間の契約義務によって EU/EEA の自然人に由来するデータを処理する EU/EEA 域外の組合員も、同様の作業が必要になるかもしれません。当クラブは、影響を受ける組合員に以下の点を重視した検討を行うことを推奨します。

- データ保護方針の更新または採用と実施
- 大規模にデータを取り扱う組織の場合は DPO の任命の検討
- データ主体が個人データの処理と自らの権利について、適切な情報を確実に受け取れるようにする手順の確立
- 保管を続ける他の法的根拠がない場合における、不要になった個人データの削除
- センシティブな個人データと定義されたもの（健康・医療データなど）に関して、第三者（他の P&I クラブを含む）との通信の安全の強化
- 許可された場合（法的根拠がある場合、または別の合意が存在する場合など）にのみ個人データが第三国に移転されることを保証するための、追加チェック体制の確立

本回覧は、法的助言と解釈されるべきではありません。組合員は、確実に GDPR を順守するために作業手順を変更する際には、弁護士や地域の監督当局に独立した助言を求めるべきです。

お問い合わせやご意見は、ロンドンオフィスのコンプライアンスマネージャー（shahram.shayesteh@ctplc.com）までお願い致します。

国際グループの全加盟クラブが、同様の回覧を配布しています。

以上

Jeremy Grose
Chief Executive
Charles Taylor & Co Limited
Direct Line: +44 20 3320 8835
E-mail: jeremy.grose@ctplc.com

（本回覧は、英文クラブ回覧を組合員各位の便宜のために日本語に仮訳したものです）