GDPR 施行後の現状と保険業界における課題

主席研究員　安田　昶勲

目　　次

要旨

2018 年 5 月に施行された一般データ保護規則（GDPR）は、日本における個人情報保護法に相当し、データ主体の権利を広く認め、個人データの取扱に関して厳しい義務を課した法規制として知られている。

施行から 1 年以上が経過した現在、GDPR が定めるデータ主体の権利や GDPR の執行を担うデータ保護監督当局の存在は、各加盟国により差があるものの、多くの人々に認知され始めている。データ主体の意識が向上するにつれて、データ主体の権利行使への対応など、個人データを取り扱う管理者が負う義務の履行はさらに重要となるものと考えられる。

保険会社も個人データを取り扱う管理者として、GDPR の定める義務を履行し、データ主体の権利行使に対応する必要があるが、消去権の行使への対応をはじめとして、効果的に法規制に適応できていない事例が生じている。

本稿では、欧州委員会が GDPR 施行 1 年後に実施した調査の内容をもとに、法規制の適応の状況と保険会社が経験した問題点と今後取り組むべき課題を取り上げている。

GDPR は欧州のみならず、世界の個人情報保護法規制に影響を与えている状況を考慮すると、GDPR を巡る課題や動向は、わが国の保険会社にとっても参考になるものと思われる。

１．はじめに

「一般データ保護規則（General Data Protection Regulation：以下「GDPR」）」[1]は、欧州連合（European Union：以下「EU」）内の個人データ[2]の保護に対する権利という基本的人権の保護を目的とした法規制として 2018 年 5 月より施行された。データ主体の権利を広く認め、個人データの取扱に関して厳しい義務を課している。EU 内のデータ主体の個人データを取り扱う際には、GDPR が定めるデータ主体の権利を保護するための各種要件を適用する必要があり、保険会社も、保険契約者等の個人データを取り扱う際には同様に GDPR への適応が求められる。

GDPR は様々な権利を定めた EU 内の統一した個人情報保護法規制として、EU 内のデータ主体に広く知られるようになり、フランスのデータ保護監督当局（Commission Nationale de l'Informatique et des Libertés：以下「CNIL」）より 5,000 万ﾕｰﾛ（約 61 億円）[3]の罰科金が科された Google や、イギリスのデータ保護監督当局（Information Commissioner's Office：以下「ICO」）より 1 億 8,339 万ﾎﾟﾝﾄﾞ（258 億円）[4]の罰科金が科されたブリティッシュ・エアウェイズの事例[5]は、GDPR が定めるデータ主体の権利についての認識と、権利行使の意識をさらに向上させるものと考えられる。

一方で、実際に個人データを取り扱う管理者[6]の側では、GDPR が要求する義務に適応するだけの人的経済的資源を欠き、規制が求める要件に十分に適応できていない事象も見られる。特に中小企業においてその特徴は顕著である[7]。また、加盟国の一部では、GDPR に対応する国内法の整備ができていないなどの課題も残っている[8]。法規制の保護対象であるデータ主体においても、自身の持つ権利の内容を十分に理解できておらず、管理者との間で混乱が生じるケースも発生している。

欧州委員会（European Commission）は、2019 年 7 月に GDPR 施行後 1 年で各業界のステークホルダーが経験した課題等を、欧州議会および EU 理事会（The Council of European Union）に提出している。保険業界からは欧州の保険協会を代表して保険ヨーロッパ（Insurance Europe）が保険業界の現状と課題を報告した。

---

[1] GDPR の規制内容の詳細については、損害保険事業総合研究所「主要国における個人情報保護法規制の動向と保険業界の対応」（2017.9）、損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向」（2019.9）を参照願う。

[2] データ主体とは、「識別された、または、識別され得る自然人」を指し、個人データとは、「データ主体に関するあらゆる情報」を指す。

[3] 2019 年 10 月末時点での為替レートである 1ﾕｰﾛ＝121.43 円で換算した。

[4] 2019 年 10 月末時点での為替レートである 1ﾎﾟﾝﾄﾞ＝140.56 円で換算した。

[5] ICO, “Intention to fine British Airways £183.39m under GDPR for data breach”（2019.7）。2019 年 10 月時点では未確定。

[6] 管理者とは「単独でまたは他と共同して、個人データの取扱の目的および手段を決定する自然人、法人、公的機関、行政機関またはその他の団体」を指す。

[7] Jenny Manin, “SMEs Say GDPR Needs Reality Check”（2019.6）。中小企業にとって、管理者または処理者のいずれに該当するかどうかの判断、データ保護影響評価の判断やデータ保護オフィサーの指名の要件となる「大規模」な処理の判断、およびデータ処理活動の記録の保持などの面で、様々な問題が生じていると述べている。

[8] 加盟国別の国内法の整備状況は後掲図表 6 を参照願う。

本稿は、欧州委員会の調査の内容を中心に、GDPR 施行後の現状と、規制の対象となっている保険会社が現在直面している課題を記載することを目的としている。前段において、データ主体の法規制と権利に関する認知の状況を中心に法規制への適応の状況に触れた後に、後段において、法規制の対象である保険会社が、GDPR 施行後に経験した問題点と今後取り組むべき課題を取り上げる。

なお、本稿における意見・考察は筆者の個人的見解であり、所属組織を代表するものではないことをお断りしておく。

２．GDPR 施行後の状況

GDPR の適応状況の理解ため、本項では、GDPR の保護の対象であるデータ主体の法規制の理解・認知の状況、GDPR の執行機関である各加盟国のデータ保護監督当局の状況、および、GDPR の内容に対応する各加盟国の国内法の整備の状況を取り上げる。

（1）法規制に関する認知の状況

本項では、欧州委員会が 2019 年 5 月に欧州 28 カ国に居住する 27,524 人のデータ主体を対象に GDPR に対する認知の状況等を調査した、Special Eurobarometer 487a - The General Data Protection Regulation [9]と題した調査の内容を取り上げる。

a. 法規制の認知の状況

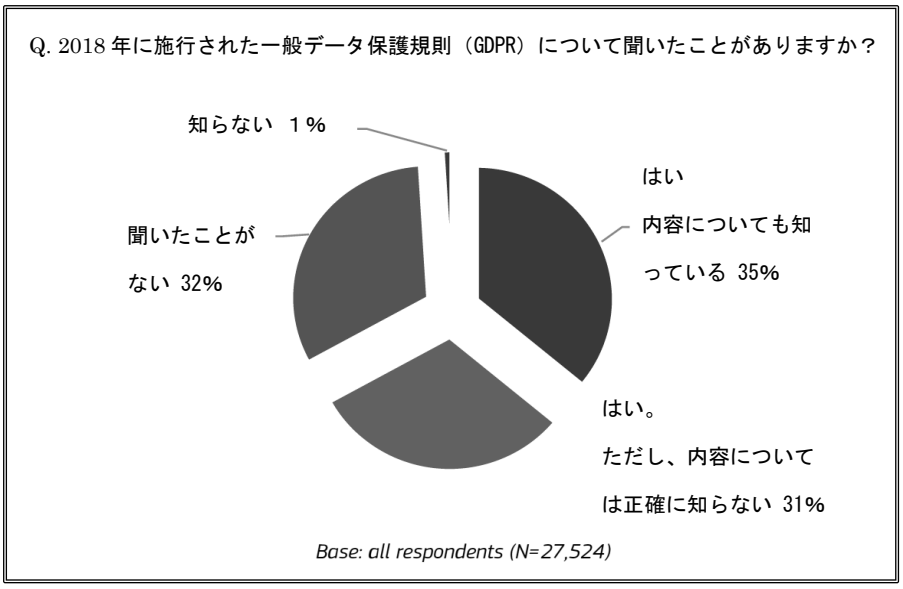
当該調査結果によると、すべての回答者のうち、67%が GDPR について認知していると回答しており、36%が法規制の内容も含めて知っていると回答している（図表 1 参照）。

国別には、スウェーデン（90%）、オランダ（87%）、ポーランド（86%）で広く認知されており、28 カ国中 26 カ国で 50%以上のデータ主体が GDPR を認知している。GDPR の認知割合が 50%を下回るのはフランス（44%）、イタリア（49%）のみとなっている。その他主要国では、イギリスが 71%、ドイツが 79%と EU 平均を上回る結果となっている。

年齢別では 25 歳から 54 歳までの認知割合が 75%と高くなる一方で、55 歳以降では 58%と認知割合は低下する。また、オンラインで商品やサービスを購入した経験がある層では 79%が認知していると回答している。

[9] 欧州委員会の調査委託を受けてマーケティング会社である Kanter が調査を行っている。

図表 1　EU 内のデータ主体の GDPR に関する認知状況



（出典：Kantar, “Special Eurobarometer 487a - The General Data Protection Regulation”（European Commission, 2019.6）をもとに作成）

b. データ主体の権利の認知と権利の行使

また、本調査では、GDPR が定めるデータ主体の権利のうち、アクセス権、訂正権、ダイレクトマーケティングに異議を唱える権利、消去権、データポータビリティ権、および自動化された意思決定に服さない権利について、データ主体が認知しているか、および、実際にこれらの権利を行使したかについてまとめている。その調査の結果は図表 2 のとおりである。

自動化された意思決定に服さない権利以外は、50%以上のデータ主体がその権利の内容を認知しており、10%以上のデータ主体が施行から 1 年間で権利を行使したことが明らかとなっている。

特に、ダイレクトマーケティングに異議を唱える権利については、回答者の 4 人に 1 人に近い割合で権利が行使されているなど、GDPR が定めるデータ主体の権利が一定浸透していることがわかる。

図表 2　GDPR が定める主なデータ主体の権利の概要と認知・行使の状況

データ主体の権利	概要	認知している割合	行使した割合
アクセス権	管理者に、個人データを取り扱っているか否かを確認したり、個人データのコピーを受け取ったりする権利	65%	18%
訂正権	管理者に、不正確な個人データを訂正させる権利（不完全な個人データを完全にする権利）	61%	16%
ダイレクトマーケティングに異議を唱える権利	個人データがダイレクトマーケティングのために取り扱われる場合に、個人データの取扱にいつでも異議を唱えることができる権利	59%	24%

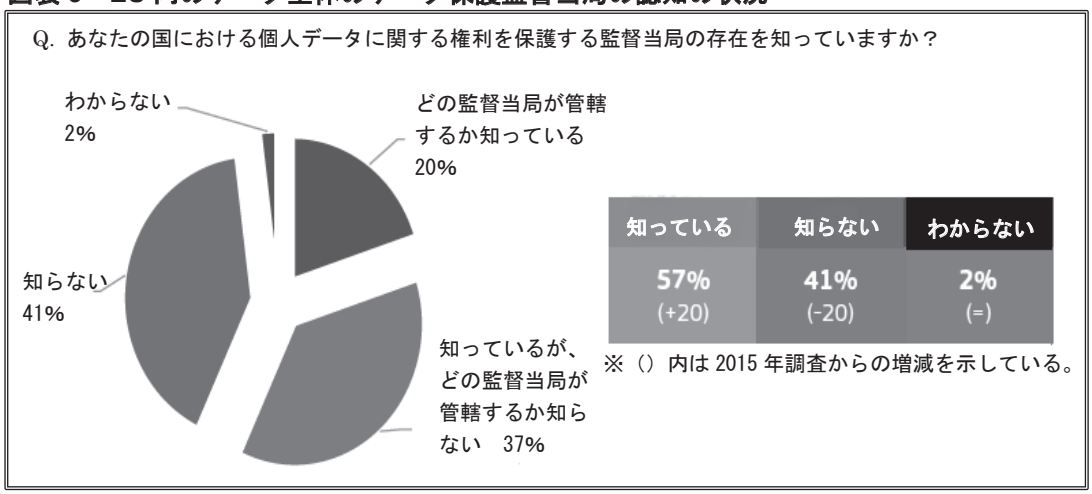
データ主体の権利	概要	認知している割合	行使した割合
消去権	管理者に、個人データを消去させる権利	57%	13%
データポータビリティ権	管理者に提供した個人データについて、構造化され、一般的に利用され、機械可読性のある形式で受け取る権利、および当該データを、他の管理者に移行する権利	50%	13%
自動化された意思決定に服さない権利	プロファイリングなどの自動化された取扱のみに基づいた意思決定に服さない権利	41%	8%

（出典：Kantar, “Special Eurobarometer 487a - The General Data Protection Regulation”（European Commission , 2019.6）ほか各種資料をもとに作成）

c. データ保護監督当局に対する認知

GDPR の執行を担う自国のデータ保護監督当局については、59%のデータ主体がその存在を知っていると回答している（図表 3 参照）。欧州委員会では同種の調査を 2015 年にも実施しており、その時点での回答では 39%にとどまっていた。このことから、GDPR の施行により、各加盟国のデータ保護監督当局に対する関心が高まったことがわかる。

図表 3　EU 内のデータ主体のデータ保護監督当局の認知の状況



（出典：Kantar, “Special Eurobarometer 487a - The General Data Protection Regulation”（European Commission , 2019.6）をもとに作成）

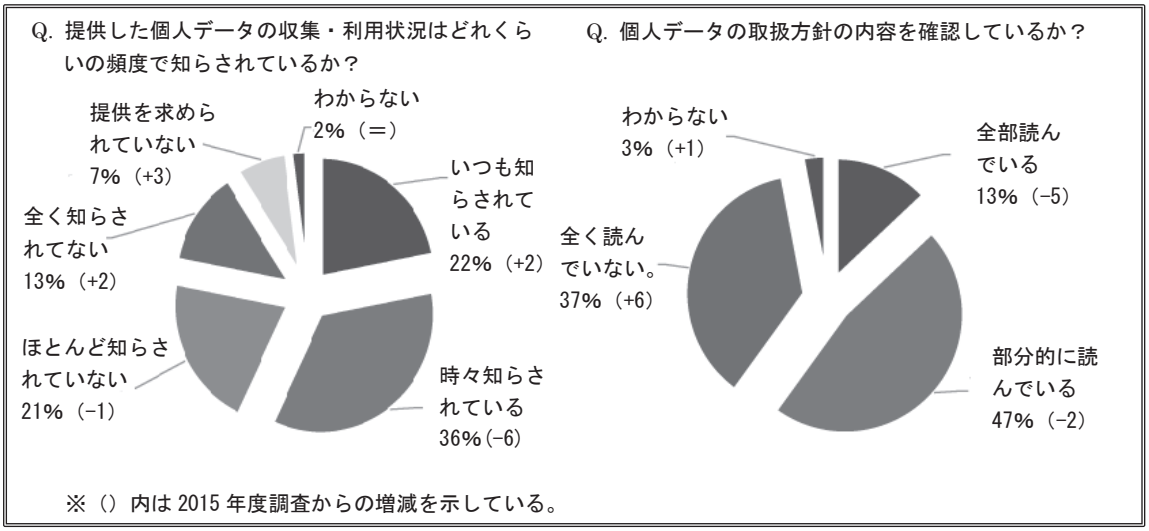
d. データの利用状況に関する認知

インターネットを使用しているデータ主体が、自身の個人データの収集と利用の状況について、個人データの管理者からある程度知らされていると回答した割合は全体の 57%であり、2015 年に行った同種の調査から 4%減少している（図表 4 参照）。

また、インターネット上の個人データの取扱方針について、内容を読んでいると回答

したデータ主体の割合は 60%であり、2015 年に行った同種の調査から 7%減少している。このことから、GDPR 施行後も自身のデータの利用に関するデータ主体の認知状況について、改善されていないことが確認できる。

図表 4　EU 内のデータ主体の個人データの利用に関する認知の状況



（出典：Kantar, “Special Eurobarometer 487a -The General Data Protection Regulation”（European Commission , 2019.6）をもとに作成）

（2）データ保護監督当局の状況

本項では、GDPR の執行を担うデータ保護監督当局の活動の状況について取り上げる。

a. データ主体からの連絡件数の変化

GDPR の施行により、データ保護監督当局に対するデータ主体の認知が向上しているのと同時に、データ主体から、データ保護監督当局に申し立てられた苦情などの件数も増加している。

イギリスでは、ICO の統計によると、2018 年から 2019 年にかけて ICO のヘルプラインで受け付けたデータ主体からの連絡件数は、前年から 66%増加し約 47 万件となっている。また、ICO が受け付けた個人データ漏えいの報告件数も、前年の 3,300 件から 14,000 件に急激に増加している（図表 5 参照）。

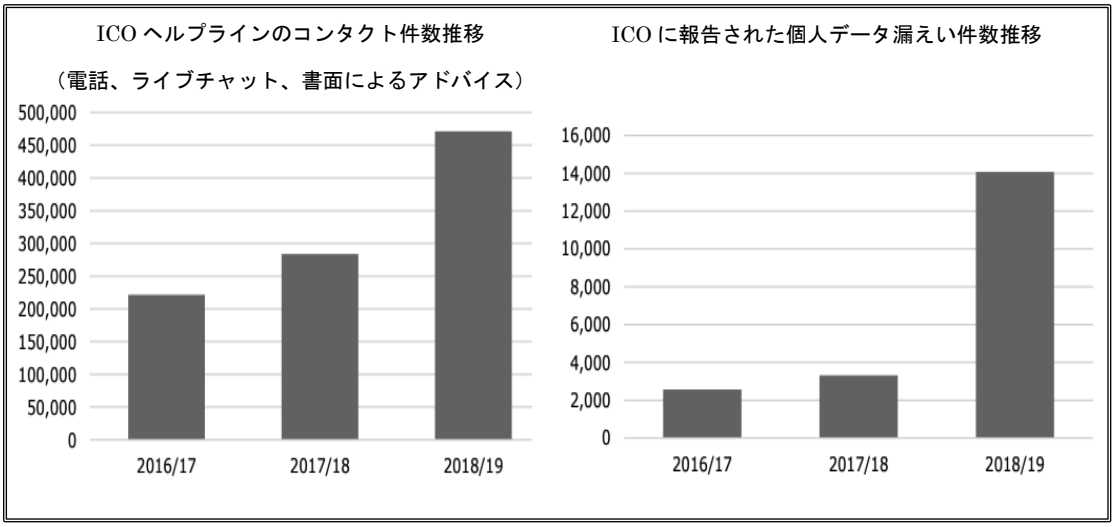
フランスにおいても、CNIL が GDPR 施行後の 1 年間で受け付けたデータ主体からの苦情件数が前年から 30%増加するなど、データ主体からのアクセスが急増している。

欧州委員会の統計によると、2018 年 5 月 25 日からの 1 年間で、EU 全体で 14 万件を超える苦情がデータ主体から各加盟国のデータ保護監督当局に申し立てられている。

こうしたデータ保護監督当局へのアクセスの増加は、GDPR の施行により、データ

主体のプライバシーの権利に関する意識が向上した結果によるものと考えられる。

図表 5　ICO へのデータ主体からの連絡件数とデータ漏えいの報告件数の推移



（出典：Information Commissioner's Office, "GDPR: One year on"（2019.5）をもとに作成）

b. 罰科金適用の現状

高額な罰科金は GDPR の特徴の 1 つであり、各加盟国のデータ保護監督当局が罰科金の適用を判断することとなっている。

罰科金の適用件数について正確な統計は取られていないものの、弁護士事務所 DLA Piper の調査では、2019 年 2 月時点で、EU 全体で 91 件の罰科金が適用されたとのことである。また、ドイツの法律事務所 JUVE によると、ドイツでは 2019 年 5 月までに 107 件の罰科金が適用されたとしている。

人権保護団体である Access Now[10]は、2018 年 5 月以降に科せられた罰科金の多くが GDPR 施行前に発生したデータ侵害等に対して科せられたものであり、GDPR 施行前の法規制に基づかれているため、適用された罰科金の金額も GDPR の規定と比較して少額であることを指摘している。今後 GDPR の規定に基づく罰科金の適用事例が増えていくものと思われる。

また、Access Now は、各加盟国のデータ保護監督当局に対し、違法行為の継続を禁止するために、抑止的な罰金を科すことを求めており、こうした行動も罰科金の適用に影響を与える可能性も考えられる[11]。

[10] 2009 年に設立された世界各地に拠点を持つ非営利団体で、デジタルセキュリティ、表現の自由、プライバシー、ネット差別、ビジネスと人権の 5 つの主要な分野に重点を置き、多くのデジタル権利を擁護している。

[11] 一方で 2019 年 2 月に欧州データ保護会議（European Data Protection Board）が作成した報告書によると、データ保護監督当局の多くが実行すべき役割に対して、予算・資源が不足しており、効率的に業務を行うためには 30%～50%の大幅な予算の手当てが必要な状況となっている。欧州データ保護会議は、29 条作業部会が改組された組織で、EU 加盟国各国のデータ保護監督当局の代表、欧州データ保護監察機

なお、2019 年 7 月に保険業界でも GDPR の罰科金が適用される事例が発生している。フランスの保険仲介事業者は、自身の運営するウェブサイトを通して他のユーザーのデータにアクセスできたという指摘を受け、データ保護監督当局から改善指示を受けたにもかかわらず、その後実施した改善対策が不十分あったとして、18 万ﾕｰﾛ（約 2,190 万円）の罰科金が科せられている。

（3）各加盟国の国内法の整備の状況

GDPR は「規則（Regulation）」であるため、EU 加盟国の国内立法を必要とせず直接効力を及ぼすが、後述する特殊な個人データの取扱や自動化された意思決定に服さない権利等に関して、各加盟国の国内法に従う取扱を規定している。各加盟国はこれらの規定に対応する国内法を新設・改正する必要があるが、GDPR 施行 1 年後の段階でもポルトガル、ギリシャ、スロベニアの 3 カ国が国内法の整備が完了していない状態であった（2019 年 10 月の段階ではスロベニアのみ法案段階）。欧州委員会も国内法の整備の遅れを緊急の課題として指摘している。図表 6 は各加盟国の国内法の整備の状況を示している。

図表 6　EU 加盟国の国内法の整備の状況

施行日	国名	施行日	国名
2018.5.25	アイルランド イギリス オーストリア オランダ クロアチア スウェーデン スロバキア デンマーク ドイツ フランス ポーランド マルタ	2018.7.6	リトアニア
		2018.7.26	ハンガリー
		2018.7.31	キプロス
		2018.8.20	ルクセンブルク
		2018.9.5	ベルギー
		2018.9.19	イタリア
		2018.11.13	フィンランド
		2018.12.7	スペイン
		2019.1.15	エストニア
		2019.2.26	ブルガリア
		2019.4.24	チェコ
		2019.8.9	ポルトガル
2018.6.24	ルーマニア	2019.8.29	ギリシャ
2018.7.5	ラトビア	未整備（法案段階）	スロベニア

（出典：各種資料をもとに作成）

3．保険業界における GDPR 適用の課題

欧州委員会は、EU の各ステークホルダーに、GDPR 施行後 1 年を経過して判明した現状と課題について調査を行っている。図表 7 は欧州委員会がステークホルダーに対して行ったアンケートの概要を示している。

関（EDPS）の代表によって構成され、EU 内のデータ保護に関する規則の統一的な適用を促し、データ保護監督当局間の効果的な協力を保証する役割を担っている。

本調査に関して、欧州諸国の保険協会で構成される保険ヨーロッパはステークホルダーの一員として、保険業界を代表して、保険会社が GDPR の適用に際して経験した内容に基づき、回答を行っている[12]。

本項では、当該調査における保険ヨーロッパの回答を中心に、個人データを取り扱う管理者として保険業界が直面している主な課題のうち、GDPR 適用 1 年後の時点で判明しているものについて説明する。

図表 7　各ステークホルダーに対する欧州委員会からの質問内容

項目	内容
1. 一般的なコメント	○（事業者団体の場合）GDPR を遵守するなかであなたの業界の主要な問題を教えてください。 ○（それ以外の団体の場合）GDPR の適用にあたり、ステークホルダーが経験した、または、観察した主要な問題を教えてください。
2. データ主体の権利	○12 条から 14 条に定める情報通知の義務にどのように対応しましたか？この点に関して実務の変更はありましたか？ ○アクセス権・訂正権・消去される権利・異議を申し立てる権利・自動化した決定に服さない権利に関する要求の増加はありましたか？ ○データポータビリティの要求はありましたか？ ○どの権利に関する要求が最も多かったですか？ ○要求に対する期限の遵守も含めて、要求の対応に際して困難な事象はありましたか？ ○要求の何パーセントが根拠のない、もしくは、過剰な要求でしたか？理由を含めて教えてください。
3. 有効な同意の条件	○取扱の法的根拠として同意を使用する際に問題はありましたか（例：苦情を受けた）？同意を要求する際にデータ主体はどのように反応しましたか？ ○取扱の法的根拠を同意から別の法的根拠に切り替えた構成メンバーはいますか？ ○構成メンバー[13]が同意の問題をどのように取り扱っていますか？法的根拠としての契約の履行と同意をどのように区分していますか？
4. 苦情と法的措置	○データ保護監督当局の前に構成メンバーに関する苦情を受けましたか？ ○構成メンバーに対する訴訟はありますか？ ○データ保護監督当局の決定、または、決定の欠如に対する訴訟はありますか？ ○上記全てのケースにおいて、苦情や訴訟の原因は何であり、どのような違反であったか説明してください。
5. 80 条に基づく代理人の使用	○構成メンバーに対してなされた代理活動はありましたか？または市民社会を代表する組織として行動したことはありますか？ ○どのような代理活動ですか（データ保護監督当局への苦情、訴訟、補償の要求）？ ○誰に対する、また、GDPR のどのような違反に対するものでしたか？

[12] 保険ヨーロッパを含む 9 つの業界団体（Confederation of the European Data Protection Organisations （CEDPO）、European Banking Federation （EBF）、DIGITALEUROPE、E-Commerce Europe、European Federation of Pharmaceutical Industries and Associations （EFPIA）、European Telecommunications Network Operators' Association （ETNO）-GSMA Europe、Federation of European Direct and Interactive Marketing （FEDMA）、Insurance Europe、SMEunited）と 8 つの市民団体（Access Now Europe、Bureau Européen des Unions de Consommateurs （BEUC）、The Danish Consumer Council、European Parents Association （EPA）、Privacy International、Stiftung Digitale Chancen （Digital Opportunities Foundation）、Union Fédérale des Consommateurs、Que Choisir（UFC - Que Choisir）、Verbraucherzentrale Bundesverband （Federation of German consumer organisations））、4 名の専門家が欧州委員会に回答している。

[13] ステークホルダーが事業者団体の場合は会員企業となる。

項目	内容
6. データ保護監督当局およびワンストップショップメカニズム[14]について	○データ保護監督当局への対応で困ったことはありましたか？ ○ガイダンスや助言の獲得にあたり困ったことはありましたか？ ○データ保護監督当局は苦情に対して適時適切に対応しましたか？ ○どれだけの構成メンバーが、データ保護監督当局に主たる事業所の申立を行いましたか？そして、そのうちどれだけの構成メンバーが主務監督当局を設けることによる利益を得ましたか？ワンストップショップメカニズムの機能について困ったことはありましたか？ ○EU 域外の管理者・取扱者の代表者が指名されたことはありますか？ ○欧州データ保護会議の作成したガイドラインを補足する、または矛盾する国内のガイドラインを確認したことがありますか？
7. 説明責任とリスクベースのアプローチ	○説明責任について構成メンバーからフィードバックされた内容を教えてください（例えば高リスクのデータ保護影響評価など）。 ○業界における GDPR の利点と課題は何ですか？ ○GDPR の全体の影響は、構成メンバーの技術革新にとってどのようなものになると考えますか？ ○GDPR の適用にあたり、最も投資しなくてはいけなかった分野は何ですか？この投資は構成メンバーの全体の成果にどの程度役に立ったと考えますか？ ○既存の技術的・組織的手法でどの程度対応できましたか、また、新たな管理システムを設けましたか？ ○構成メンバーが採用した GDPR を適用するための技術的・組織的対策は、顧客の意識と信頼を向上させていますか？
8. データ保護オフィサー	○構成メンバーは GDPR または国内法に従いデータ保護オフィサーを指名していますか？ ○構成メンバーは GDPR または国内法で定める要件以外に、独自の基準でデータ保護オフィサーを指名していますか？ ○管理者または取扱者を代表する団体はデータ保護オフィサーを指名していますか？ ○データ保護オフィサーの成果について経験した内容を教えてください。
9. 管理者と取扱者の関係（標準契約条項）	○現在構成メンバーが適用している契約において経験したことを教えてください。 ○28 条 7 項が定める標準契約条項を採用する必要がありますか？ ○標準契約条項を作成するときどのような要素が必要ですか（例：監査、責任分担、協力義務、補償）？ ○標準契約条項の使いやすさについて意見がありますか？ ○起草案がある場合は共有してください。
10. 域外移転に関する標準契約条項	○現在標準契約条項において経験したことを教えてください。 ○既存の標準契約条項を反映させる必要がある事項はありますか？ ○明確にすべき条項はありますか？ ○Schrems Ⅱ事件[15]の結果を標準契約条項に反映させる必要がありますか？ ○新しい標準契約条項を作成する必要がありますか？ ○標準契約条項の使いやすさについて意見がありますか？ ○起草案がある場合は共有してください。
11. 国内法	○GDPR を適用するための国内法に問題はありましたか？

（出典：European Commission, “Multi-stakeholder expert group to support the application of Regulation (EU) 2016/679 QUESTIONS TO PREPARE THE STOCK-TAKING EXERCISE OF JUNE 2019 ON THE APPLICATION OF GDPR”（2019.3）をもとに作成）

[14] 事業者が複数の加盟国にわたって個人データを取り扱う場合は、当該事業者の主たる事業所のある加盟国の監督当局（主監督当局）が管轄するシステムのこと。

[15] オーストリアのプライバシー保護活動家である Max Schrems 氏が、データ収集が GDPR の規定に違反するとしてデータ保護監督当局に申し立てた事件。現在個人データの域外移転に使用されている標準契約条項の有効性も争点となっている。

（1）データ主体の権利行使における課題

本項では、保険会社におけるデータ主体の権利行使への対応の状況と、直面する課題について記載する。

a. データ主体からの保険会社に対する権利行使の状況

保険ヨーロッパの回答は、保険会社に対するデータ主体の権利行使の状況およびその対応状況を以下のとおり回答している。

（a）アクセス権、訂正権

アクセス権については、GDPR 施行直後にデータ主体からの権利の行使が一時的に増加した事象はあったものの、ほとんどの保険市場で大幅な増加は見られず、わずかに増加している程度に留まっている。ただし、フランス、イタリアなど一部保険会社において、アクセス権の行使要求件数が前年の 80%以上増加したケースも存在している。

（b）消去権

ほとんどの加盟国において、消去権の権利の行使件数が増加している。保険契約の締結に至らず、保険の見積だけを行った見込顧客から権利行使を受ける事象が多く、また、契約を締結したばかりのデータ主体からの消去権行使も多く見られている。

保険ヨーロッパの回答では、根拠のない、または、過剰な権利の行使はあまり見られていないとしているが、保険会社が行った消去権の対応を不服として、データ保護監督当局に苦情が申し立てられた事例も発生している[16]。

（c）訂正権、自動化した決定に服さない権利、データポータビリティの権利

訂正権については、GDPR 施行後もほとんど増加は見られていない。

自動化した決定に服さない権利とデータポータビリティの権利については、ほとんどの加盟国で権利行使の要求を受け取っていない。

データポータビリティの権利については、自動車保険の請求履歴の移転に関する要求がなされたケースがあったことが報告されている。

b. 問題点と課題

ほとんどの加盟国において、データ主体からの権利行使の要求に対して、1 カ月の期

[16] オーストリアの保険会社が、データ主体から保険契約の申請時に提供した個人データの削除の要求を受けた事例。要求を受けた保険会社は削除要求を受けたデータのうち、一部を削除し、残りを匿名化したところ、データ主体から完全に消去するという要請を満たしていないとして、オーストリアのデータ保護監督当局（DSB）に苦情が申し立てられたもの。DSB は、匿名化により個人の追跡可能性は除外されており、データ削除の要請が満たされているとして、データ主体の要求を退けている。

限内に対応することが困難である実態が報告されている。その要因として、以下の 4 点が報告されている。

○　権利行使の要求件数が増加したこと
○　データ主体からの要求内容が複雑であること
○　アクセス権の行使の要求の場合、提供する必要があるデータの整備に時間がかかること
○　データ主体の権利行使の要求に対応するシステムを導入していないと、手動で対応しなくてはならないこと

また、保険ヨーロッパは、データ主体の消去権の行使に対応するシステム化の課題として、以下の点を挙げている。

○　長期の保険期間を持つ保険商品もあり、保険期間の終了を正しく識別する必要がある。
○　消去する必要のあるデータを所定の時間内に処理する必要がある。
○　保険会社だけでなく、代理店やブローカー、サービス提供事業者の持つデータとマッチングする必要がある。
○　保険数理上の計算を行うための履歴データは必要であり、消去される前にデータの変換・保存のプロセスが必要である。

さらに、これらの要件を満たしたソフトウェア・IT ソリューションの開発が必要であると報告している。

(2) 情報権に関する課題

本項では、保険会社がデータ主体から個人データを受領した場合に、データ主体が情報の通知を受ける権利に関して、保険会社が直面する課題について説明する。

a. 保険会社の情報提供義務

データ主体は、管理者が自身の個人データを取得した場合、およびデータ主体がアクセス権を行使した場合に情報の通知を受ける権利を有する。これに対応して、情報を取得した管理者はデータ主体に対して、管理者やデータ保護オフィサーの連絡先、個人データの取扱や法的根拠、EU 域外への移転に関する情報等を記載したプライバシー通知を行わなくてはならない。また、プライバシー通知には、通知を行う管理者以外に、個人データを取得する共同管理者、取扱者や第三者などが存在する場合は、当該取得者の名称または種類を記載しなくてはならない。

管理者は、データ主体に包括的な情報を提供する義務を有していると同時に、その情報を簡潔で、透明性があり、理解しやすくかつ容易にアクセスしうる形式で提供しなくてはならないとされている。その方法として、欧州データ保護会議の作成した透明性に関するガイドラインでは、デジタル環境でプライバシー通知を行う際には、階層化アプローチが推奨されている。

階層化アプローチとは、データ主体に提供しなくてはならないすべての情報を単一の通知として提供すると、情報が煩雑で、データ主体が必要な情報をすぐに確認することできなくなるような事態が懸念される場合、単一の通知として表示するのではなく、様々な情報にリンクする階層的なプライバシー通知を利用することである。

データ主体が最初に積極する接触する第１層には最も重要な情報である、取扱の目的、管理者の身元、データ主体の権利の説明およびその他データ主体への影響が大きい取扱に関する情報が記載されていることが推奨されており、その他の階層の情報はデータ主体が必要な情報がどこにあるか明瞭に確認できる設計と配置になっていることが求められる。

b. 現状と課題

保険ヨーロッパは、多くの保険会社がプライバシー通知を修正し、階層化アプローチを採用した形で新しい情報提供義務に対応していると報告している。

一方で、一部のデータ保護監督当局が、管理者が階層的に情報提供を行う際に使用するメディアを変更することを避けるように主張しているため、保険会社にとっては複雑で費用のかかる事態が生じたという問題点も指摘している。

また、情報権については、データ主体が保険契約の当事者ではない場合に、こうした情報通知の義務を果たすことは非常に困難であり、保険会社にとって大きな負担になるという指摘も存在する[17]。

（3）健康データ取扱における法的根拠に関する課題

本項では、個人データを取り扱う保険会社が、GDPR の規定に基づき、どのような法的根拠をもって個人データを取り扱っているか、および、傷害保険等で取り扱う特殊な個人データの 1 つである健康データの取扱にあたって直面している課題について説明する。

a. 個人データの取扱が認められる法的根拠

GDPR では、管理者の個人データの取扱が適法とされるには、法が定める法的根拠を満たすことが必要である旨を定めている（6 条 1 項）。一方で、特別な種類の個人データは、原則として取扱が禁じられているが（9 条 1 項）、一定の法的要件に基づく場

[17] KPMG, “The GDPR and key challenges faced by the Insurance industry”（2018.2）

合は取扱が認められる（9 条 2 項）。

また、特別な種類の個人データのうち、遺伝データ、生体データおよび健康データについては、加盟国の国内法により取扱の法的根拠に追加ないし制限することができる（9 条 4 項）。

図表 8 は 6 条 1 項の定める個人データの取扱が適法とされる法的根拠と、9 条 2 項が定める、健康データを含む特別な種類の個人データの取扱が適法とされる法的根拠を示している。

保険ヨーロッパによると、一般に保険会社は、後記 b.（a）に記載の理由により同意の取得を法的根拠とするのは困難であるため、個人データを取り扱う法的根拠として、「契約の締結または履行に必要な場合」、「法的義務の遵守に必要な場合」および「管理者等の正当な利益に必要な場合」に依拠している。同意の取得を法的根拠とするのは、これらの法的根拠を使用することができない特別な種類の個人データを取り扱う場合等に限られていると述べている。

図表 8　個人データの取扱が認められる法的根拠

データの種類	取扱が認められる法的根拠
通常の個人データ（GDPR6条1項）	（a）有効な同意がある場合 **（b）データ主体が当事者となっている契約の締結または履行に必要な場合** **（c）法的義務の遵守に必要な場合** （d）データ主体等の利益の保護に必要な場合 （e）公共の利益または公的権限の行使に必要な場合 **（f）管理者等の正当な利益に必要な場合**
特別な種類の個人データ（GDPR9条2項）	**（a）明示的な同意がある場合** （b）雇用等に関する法に基づく義務・権利の履行・行使に必要な場合 （c）データ主体等の重要な利益の保護に必要な場合 （d）政治団体や労働組合等による取扱である場合 （e）データ主体により公開されている場合 （f）法的主張に必要な場合 （g）実質的な公共の利益に必要な場合 （h）医療目的等に必要な場合 （i）公衆衛生の分野における公共の利益に必要な場合 （j）科学的研究や統計目的等に必要な場合

（出典：各種資料をもとに作成）

b. 健康データの取扱についての問題点

（a）同意を法的根拠とすることの困難さ

データ主体からの明示的な同意を取り付けることで、健康データを取り扱うことが可能であるが、以下の場合には、同意の取付を個人データ取扱の法的根拠とすることが困難となっている。

○　団体傷害保険の場合など、収集すべき個人データを持つデータ主体が契約の直接の当事者ではない場合、保険会社がデータ主体に個人データが必要な理

由を説明し、同意を取り付けることが困難である。再保険の分野でも同様の問題が生じる。

○　賠償責任保険の場合等で、契約の当事者ではない受傷者に対して、保険会社がデータ主体に個人データが必要な理由を説明し、同意を取り付けることが困難である。

○　不正請求を防止・検出するために健康データを取り扱う必要がある場合に、保険金詐欺の懸念があるデータ主体から、健康データの利用の同意を得ることは困難である。

（b）加盟国間での取扱の相違

健康データについては、GDPR9 条 2 項で定められている法的根拠以外にも、加盟国の国内法によってはその取扱が認められる。

保険ヨーロッパによると、こうした背景もあり、健康データを適法に取り扱うことのできる法的要件に対する考え方が、加盟国間で異なっていることを報告している。図表 9 は健康データの取扱に関する法的根拠の類型および主な取扱の事例を示している。

図表 9　健康データの取扱に関する法的根拠についての類型および主な取扱の事例

法的根拠の類型	主な取扱の事例
国内法により法的根拠を整備（9条4項）	加盟国において定めた国内法によって、データ主体からの同意の取得を必要とせずに、保険における健康データの取扱を認めている。 ○スペインでは、「影響を受ける当事者の保険契約の実行に必要な場合」に、保険の分野で健康データの取扱を認める旨規定されている。 ○アイルランドでは「データ主体の基本的な権利と自由を保護するために適切かつ具体的な措置が講じられることを条件」として、保険の分野で健康データの取扱を認める旨規定されている。 ○フィンランドでは、保険の分野で健康データを使用する場合は、GDPR9条1項の規定は適用されないと定めている。
同意を除く9条2項のいずれかに該当	加盟国によっては保険会社の健康データの取扱が、同意の取得以外の9条2項の要件を備えているとし、データ主体の同意を取り付けることなく、保険における健康データの取扱を認めている。 ○イギリスのデータ保護法では、一定の条件を満たした場合に限り保険による健康データの取扱を9条2項（g）「実質的な公共の利益に必要な場合」に該当するものとして、保険における健康データの取扱を認めている。 ○一部加盟国においては、9条2項（f）「法的主張に必要な場合」に該当するものとして、保険における健康データの取扱を認めている。 ○健康保険の場合等については、9条2項（b）「雇用等に関する法に基づく義務・権利の履行・行使に必要な場合」に該当するものとして、健康データの取扱を認めているケースも存在する。

法的根拠の類型	主な取扱の事例
同意以外に有効な法的根拠がない	加盟国によっては、保険会社の健康データの取扱に際して同意の取得以外に有効な法的根拠がなく、契約前の健康データ取得時および契約の履行時にそれぞれ同意の取付が必要である。 ○フランスでは、保険会社が健康データの取扱にあたって、CNILより健康データの機密性を確保するルールを遵守することが求められる[18]。 ○ポルトガルでは、保険の分野における特別な種類の個人データの取扱について明確な規定がない。ただし、法的に加入が義務付けられている保険については9条2項（g）「実質的な公共の利益に必要」なものとして、保険における健康データの取扱を認めている。

（出典：各種資料をもとに作成）

c. 健康データの取扱に関して保険会社が直面している課題

保険ヨーロッパは、前記b.（a）のとおり、保険会社にとって同意を要件とすることが困難な場合があるとともに、健康データの取扱に関する課題として、以下の点を報告している。

- ○ 健康データの取扱に関して加盟国間で取扱が異なるため、複数の加盟国間で事業を行う保険会社とって、法規制が遵守が困難となっている。
- ○ 特に再保険の分野において、国内法の規定がなければ元受保険会社と同様に健康データの取扱について法的根拠が必要となるため、加盟国間での個人データの取扱の相違は、再保険会社が複数の加盟国で事業を行うことに大きな制限を課す可能性がある。
- ○ 顧客が、健康データの取扱に明示的な同意が必要であることを認知しておらず、顧客の不満や返答の遅れにつながり、顧客対応が遅れるケースが生じている。

（4）保険商品の革新における課題

保険ヨーロッパはGDPRの適用により保険商品の革新に与える影響として以下の点を報告している。

a. 自動化された意思決定に服さない権利による影響

保険会社は、保険商品の提供にあたって、リスク分析、保険料の算定または不正請求の排除などの目的に、様々な自動化された手段による意思決定を行っているが、GDPRではこの決定に服さない権利を定めている。GDPR では「契約の履行や締結の必要性がある場合」等に例外を設けているが、欧州データ保護会議の作成したガイドラインでは、他のプライバシーの侵害の少ない方法が適用できるかどうかを考慮して、この種の

[18] CNIL, “Rapport d’activité 2018 Protéger les données personnelles, Accompagner l’innovation, Préserver les libertés individuelles”（2019.4）。本レポートの中で、CNILは保険の分野での健康データの取扱について、フランス保険協会（Fédération Française de l'Assurance）等と協議をしていることについて記載している。

取扱が必要であることをデータ主体に示すことができなければならないとしており、必要性については厳格な解釈をとっている。こうした制約は革新的な保険商品の設計を妨げる可能性がある。

なお、自動化された意思決定に服さない権利については国内法の規定によりその内容を制限することができる。EU 加盟国のうち、オーストリア、ベルギー、フランス、ドイツ、ハンガリー、アイルランド、スロベニア、オランダ、イギリスの 9 カ国が、国内法によって権利の制限を設けており、そのうちイギリスおよびドイツは、保険契約の締結に一定の条件下で自動化された意思決定に基づく取扱を行うことを明示的に認めている。

また、Access Now は、こうした加盟国間の取扱の相違があることについて、1 人のデータ主体のデータの取扱を複数の加盟国にて行う場合に、データ主体の権利がどのように保護されるのかという懸念を示している。

b. データ取扱の原則やセキュリティ要件による影響

GDPR の定めるデータ最小化の原則と目的制限の原則により、収集データとデータの使用目的が制限され、また、バイデザイン・バイデフォルト[19]の原則などのセキュリティ対策の実施は製品開発のコストを増加させており、こうした点が保険商品の進化に悪影響を与える可能性があると指摘している。

（5）外部事業者との関係における課題

GDPR では、管理者は、自身の代わりに事業者（取扱者[20]）にデータの取扱を実施させる場合には、事前に書面による契約を締結し、取扱者が遵守すべきセキュリティ対策に関する義務やデータ主体の権利行使に際して管理者に協力する義務などを定めるように求めている。

保険ヨーロッパは、保険会社と、保険会社から業務を請け負う外部事業者の間で以下の課題が生じていることを報告している。

a. 外部事業者との関係について

（a）外部事業者との関係

保険会社が IT 会社に個人データの分析等を委託するなどの外部委託においては、委託元の保険会社が「管理者」に該当し、委託先の IT 会社が「取扱者」に該当する

[19] GDPR の規定するセキュリティ対策の 1 つで、個人データを取り扱うコンピュータシステムは、プログラムの設計段階から GDPR に沿った取扱を埋め込むこと（バイ・デザイン）や、初期設定として、入力したすべての個人データに対して適切な技術的および組織的対策が行われること（バイ・デフォルト）が求められている。

[20] 取扱者とは、「管理者のために個人データの取扱を行う自然人、法人、公的機関、行政機関またはその他の団体」を指す。

とされている[21]。

管理者である保険会社は、GDPR の要件に合致した取扱者を選定し、データ主体の権利の保護を確保するような取扱方法で、適切な技術的・組織的措置を講じることのできる取扱者のみを利用しなくてはならない。また、管理者は取扱者のセキュリティ要件や GDPR の定める各種義務等を記載した契約を、取扱者と締結することが定められている。

保険ヨーロッパによると、いくつかの保険会社が、取引外部事業者との契約について困難が生じていることを報告しており、その原因として、以下の点を指摘している。

○ 保険契約の取扱を行うために徹底的な検査が必要になるが、外部業者がそれを実行する組織と能力を有することは困難である。
○ 保険会社が契約する外部事業者が、取扱者、共同管理者、もしくは独立した別の管理者に分類されるのか判断することが困難である[22]。
○ GDPR で定める様々な義務や責任について、保険会社と外部事業者間を明確に確立することが困難である。

その結果、多くの保険会社が自身の取引する外部事業者との契約関係の整理・交渉に時間を要していることを指摘している[23]。

（b）保険仲介事業者との関係

保険市場においては、一般的に保険会社、保険仲介事業者、再保険会社など複数の市場関係者は、それぞれ自身のサービス提供や顧客管理のために個人データを取り扱うため、それぞれ独立した管理者に該当する[24]。

保険ヨーロッパは、一部の保険市場において、これらの市場関係者の分類について困難に直面している実態を報告している。

欧州保険仲介事業者連盟（European Federation of Insurance Intermediaries）が所属する欧州の中小企業の事業者団体である SMEunited に報告した内容によると、一部の保険会社が保険仲介事業者を一律に取扱者と分類しており、保険仲介事業者との間で長い交渉が発生しているケースが存在している[25]。

---

[21] 損害保険事業総合研究所「主要国における個人情報保護規制の動向と保険業界の対応」（2017.9）
[22] 欧州委員会によると、一部ソフトウェアの保守とサポートを行う事業者が、自身の業務に個人データの処理は含まれていないとして、取扱者となることを拒否している事例が存在している。
[23] ただし、こうした状況も加盟国すべてに一様に生じているのではなく、フランスやチェコで適用に困難が生じている一方で、スペインでは GDPR 施行前から国内法で類似の関係が存在していたため、大きな問題は発生していない。
[24] 損害保険事業総合研究所「主要国における個人情報保護規制の動向と保険業界の対応」（2017.9）
[25] SMEunited “Multi-stakeholder expert group to support the application of Regulation (EU) 2016/679 SMEunited1 input to the QUESTIONS TO PREPARE THE STOCK-TAKING EXERCISE OF JUNE 2019 ON THE APPLICATION OF GDPR”（2019.4）

なお、欧州保険仲介事業者連盟の見解では、保険仲介事業者は、保険会社とは別の管理者に分類され、保険会社、保険仲介事業者とも、一方がそれぞれの業務において他方のデータを処理する場合には、取扱者となると判断しているとのことであり、その見解を業界内で共有するように進めている。

b. 外部事業者との契約における標準契約条項の設定について

GDPR の規定により、欧州委員会は、管理者と取扱者の契約に定める内容について標準契約条項を規定することができる。

欧州委員会の標準契約条項の作成の要否についての質問に対して、保険ヨーロッパは、各保険市場で意見が異なっており、明確な合意が得られていないと報告している。

保険会社の意見には、契約の権利義務を標準化することにより相手方との交渉の負担を減少させる点などで利点があるというものもある一方で、外部事業者との契約はそれぞれ独自の特殊性があり標準契約条項の内容を加えることは困難であるというものも存在する。

一方で、域外移転における標準契約条項[26]に外部事業者との関係を盛り込んだ標準契約条項の組み合わせを持つことについては多くの保険会社が賛成している[27]。

4．おわりに

欧州委員会は、データ主体の GDPR の認知の状況について 67%の回答者が規制について認識し、権利に対する意識の向上が見られることを評価しつつも、加盟国間で認識の差異が大きいことや、プライバシー通知に対するデータ主体の認識が高くないこと等を課題として挙げており、さらなる意識向上のための取組が必要であると述べている。こうした意識向上の取組が進むにつれて、データ主体による権利行使への対応や管理者が負う義務の履行はさらに重要となるものと考えられる。

保険業界としては、今後予想されるデータ主体からの権利行使の増加に備えて、システム整備を含めた対応力の強化が求められる。特に消去権の行使については、2019 年 9 月に Google と CNIL の争いに欧州司法裁判所の判決が下されるなど、近年注目が高まっており早急な対応が求められる。その他にも、外部事業者との契約関係の整備、特に双方の契約における権利義務の明確化も課題となる。また、データ主体のデータ利用状況に関する認識が低いことを考えると、より実用的な情報提供の方法の検討も必要と思

[26] 域外移転とは、EU 域内に所在する個人データを、EU 域外の国・地域または国際機関に移転することである。域外移転は原則禁じられているが、一定の法的根拠を満たすことで可能となる。標準契約条項はその法的根拠の 1 つで、データ移転の当事者が欧州委員会の作成した標準契約条項を使用したデータ移転契約書を締結することで、域外移転を可能とするものである。

[27] 保険ヨーロッパの指摘にはないものの、Schrems Ⅱ 事件の結果が、域外移転を可能とする標準契約条項の効力に影響を与えると懸念する意見も存在する。

われる。

一方で、健康データの取扱に関する法的根拠や自動化された意思決定に関する各加盟国間での相違等に関しては、今後法規制がどのように推移していくかを注視していく必要がある。欧州委員会は 2020 年に法規制の評価と見直しに関する報告書を欧州議会および EU 理事会に送付することが定められており、これらの課題も検討されることが想定される。また、欧州委員会、欧州司法裁判所および各加盟国のデータ保護監督当局の今後の動向を把握することも重要であり、複数の加盟国にわたって業務を行う場合は、各加盟国間での取扱の相違を常に把握しておく必要が生じる。

近年では、2019 年 5 月にタイで GDPR の内容に準拠した個人情報保護法規制が施行されており、シンガポールでも同じく 2019 年 5 月に公表した個人情報保護法に関するガイドラインで、情報漏洩が発生した場合のデータ主体への通知義務等、GDPR と同様の規制を運用面で取り入れている事例が見られる。米国でも「米国版 GDPR」ともいわれるカリフォルニア州消費者プライバシー法が 2018 年 6 月に成立し、2020 年 1 月に発効する予定である。GDPR が世界の個人情報保護法規制に与えている影響を考慮すると、GDPR を巡る課題や動向は EU 内のみに留まらず、わが国を含めて多くの国の個人情報保護法規制に影響を及ぼすことが予想され、今後も注視していくことが必要であろう。

＜参考資料＞

・損害保険事業総合研究所「主要国における個人情報保護規制の動向と保険業界の対応」（2017.9）
・損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向」（2019.9）
・山村真澄「解説！GDPR（EU 一般データ保護規則）の概要 2」（山村忠夫法律事務所、2019.5）
・米山怜子「欧州委員会、GDPR の 1 年間のレビューを発表。その経緯とこれからの指針」（ブラーブメディア、2019.8）
・Access Now, “One Year Under The EU GDPR An Implementation Progress Report”（2019.5）
・Adam Panagiotopoulos, “National laws implementing the GDPR: The case of health research in Ireland”（Trilateral Research, 2019.10）
・Alex Anisie, “GDPR: Catalyst or deterrent for innovation in Insurance”（ABI, 2017.10）
・Article 29 Data Protection Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation”（2018.2）
・Article 29 Data Protection Working Party, “Guidelines on transparency under Regulation”（2018.4）
・CNIL, “Rapport d’activité 2018 Protéger les données personnelles, Accompagner l’innovation, Préserver les libertés individuelles”（2019.4）
・DLA Piper, “SCHREMS 2.0 – The Demise Of Standard Contractual Clauses And Privacy Shield?”（2019.7）
・European Commission, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data protection rules as a trust-enabler in the EU and beyond – taking stock”（2019.7）
・European Commission, “CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE STOCK-TAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION”（2019.6）
・European Commission, “Multi-stakeholder expert group to support the application of Regulation (EU) 2016/679 QUESTIONS TO PREPARE THE STOCK-TAKING EXERCISE OF JUNE 2019 ON THE APPLICATION OF GDPR”（2019.3）
・European Data Protection Board, “First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities”（2019.2）
・Helena Tapp Barroso, “Processing personal health data for insurance purposes under GDPR”（Morais Leitão, Galvão Teles, Soares da Silva & Associados, 2019.4）
・Information Commissioner’s Office, “GDPR: One year on”（2019.5）
・Insurance Europe, “Response to EC stocktaking exercise on application of GDPR”（2019.4）
・Jenny Manin, “SMEs Say GDPR Needs Reality Check”（SMEunited, 2019.2）
・Kantar, “Special Eurobarometer 487a –The General Data Protection Regulation”（European Commission, 2019.6）

・KPMG, “The GDPR and key challenges faced by the Insurance industry”（2018.2）
・Laureline Lemoine, “On its first birthday, the GDPR needs to grow some teeth”（Access Now, 2019.3）
・Leo Kelion, “Google wins landmark right to be forgotten case”（BBC, 2019.9）
・Lydia F de la Torre, “Austrian Data Protection Authority: the erasure of personal data is also possible through anonymization”（Medium, 2019.5）
・Magdalena Bartosik & Kamila Nieweglowska-Kennedy, “Response to EC stocktaking exercise on application of GDPR”（Dentons, 2019.5）
・Sascha Kuhn, “First figures published on GDPR fines in Germany”（Simmons & Simmons, 2019.7）
・Sarah Delon-Bouquet, “GDPR: new CNIL fine of 180,000 euros for a car insurance company”（Bryan Cave Leighton Paisner, 2019.8）
・Schürmann Rosenthal Dreyer Rechtsanwälte, “Profiling: The Challenges of the GDPR”（2018.5）
・SMEunited, “Multi-stakeholder expert group to support the application of Regulation (EU) 2016/679 SMEunited input to the QUESTIONS TO PREPARE THE STOCK-TAKING EXERCISE OF JUNE 2019 ON THE APPLICATION OF GDPR”（2019.4）

＜参考ウェブサイト＞

・欧州委員会（European Commission） https://ec.europa.eu/
・欧州データ保護会議（European Data Protection Board） https://edpb.europa.eu/
・欧州連合（European Union） https://europa.eu/
・保険ヨーロッパ（Insurance Europe） https://insuranceeurope.eu/
・Bird & Bird https://www.twobirds.com/
・CNIL https://www.cnil.fr/
・DSB http://www.dsb.gv.at/
・EUR-Lex https://eur-lex.europa.eu/
・FINLex https://www.finlex.fi/
・ICO https://ico.org.uk/
・Linklaters https://www.linklaters.com/