ESOMARが推奨する
当面の対策と今後の見通し

2018.06.18

ISO/TC225国内委員会
一ノ瀬裕幸

あなたの中に未来がある。
一般社団法人 日本マーケティング・リサーチ協会

Japan Marketing Research Association

本日のポイント：「脅威論」を踏まえつつも冷静に

（一例として･･･）

◆ 脅威を煽るマスコミは多いが？

- 定性的には必ずしも間違いではないが、定量的には「煽りすぎ(!?)」
- 「十分性認定」確実な今の状況で、日本の市場調査会社が制裁を受ける可能性はかなり低い

  （⇔ もちろん、ゼロではないが…）

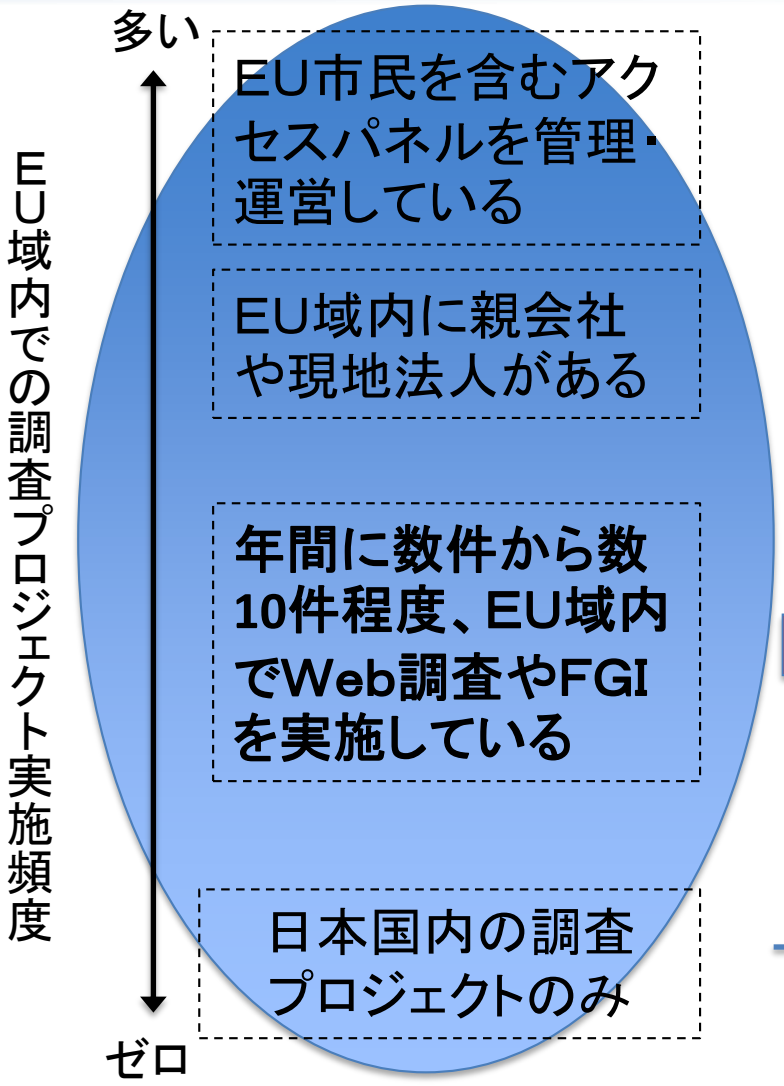
◆ ただし、中長期的には対応準備を

- 遠からず、日本の個人情報保護規制もGDPRの影響を確実に受ける

  ⇒ ESOMARと連携して「備え」を

CONTENTS

前提条件： 今回セミナーの「対象」と想定している会員社



- 本格的なGDPR対応が必要ですが、すでに親会社等からの指示・要請が出ていると思われますので、そちらに従ってください
- **今回セミナーの主たる対象と想定している会員社さんです**
  焦る必要はありませんが、順次対応体制の準備をお願いします
- 特別な対応は不要です
  Ｐマーク制度に則った対応を継続してください

はじめに：「十分性認定」でホッとひと息とはいえ…？

「気付かぬまま個人データを域外移転」による課徴金リスクは大幅軽減

◆ クライアントや現地取引先からの対応要請は継続する

- EU域内では、顧客自身の取引先や消費者への説明責任が残る
- 将来、何か問題（事件）が生じた場合には必ず対策を迫られる

⇒ 市場調査会社が「見せしめ」にされる可能性はかなり低いが、
何らかの事故が生じた場合には（業界を問わず）対処策が必要に

⇒ 対処可能な範囲・コスト内で順次備えていくことは必要

◆ 恒常的にEU域内で調査を行っている会社は準備必須

- すぐには問題にならなくても、いずれかの時点で対応を迫られる
- ただし、他社動向やEU域内での事例を見てからでも間に合うはず
- **基本的には、ESOMAR版『行動規範』の発表（年内見込）を待つ**

はじめに： すぐに対応を始めるべき会員社は？

1. EU域内で FGI や 1 on 1 を受注している（外注委託を含む）

- GDPR対応必須（＝貴社が「データ管理者」に）

  ⇒ 小規模とはいえ、対処策（P14～P15）を整備していく必要あり

  （Web調査を外注している場合は次ページ参照）

2. EU市民を含む可能性があるアクセスパネルを運用している

- EUのアクセスパネル会社と提携している場合を含む
- **日本国内のみのアクセスパネルも、将来的には対策が必要に**

  ⇒ 今後、日本の個人情報保護規制も順次GDPRに近づいていくはず
  やがて対処を迫られる（＝**次期システム改訂時にはGDPR対策を**）

3. EU域内で活動している大手顧客を有する

- 顧客に迷惑をかける恐れがある（＝顧客の啓蒙を含めた対策必須）

はじめに： 当面する対応の基本方針

① Web調査を現地調査会社（アクセスパネルを含む）に委託？

- 集計表（統計データ）または匿名化されたデータのみ入手を

  ⇒ 個人データは極力移転しない （⇒ 難しい場合には下記③へ）

  ⇒ 仮名化データはいちおう流通可能だが、まだ評価未定（⇒ 次頁）

② FGI や 1 on 1 を現地調査会社に委託？

- GDPR対応責任者を明確にし、文書記録管理システムを再点検
- 対象者からの（書面による）同意取得を徹底する

  ⇒ 取得方法の詳細は、現地委託先に相談を

③ EU域内の個人データをやむなく収集・加工することがある？

- 今からだと、ESOMAR Plusをご紹介する他に手はない？（後述）

＜参考＞ 現時点でのWeb定量調査「ローデータ」の解釈

◆ 正式見解は未確定 ⇒ ESOMAR版『行動規範』を待つ（が…）

データ種類（仮）	現時点の解釈	問題となるデータ要素
ｱｸｾｽﾊﾟﾈﾙ原ﾃﾞｰﾀ	個人データ	氏名、住所、デモ属性（特定機微情報含む）、…etc.
ローデータ ①	個人データ	実査直後のデータ：IPｱﾄﾞﾚｽ、Cookie、ADID等を含む （例：複数のｱｸｾｽﾊﾟﾈﾙ会社に委託し、重複ﾁｪｯｸに利用）
ローデータ ②	仮名化データ	ｱｸｾｽﾊﾟﾈﾙ会社と情報をやり取りするための管理用ID （例：ｱｸｾｽﾊﾟﾈﾙ会社保有の詳細情報含めてデータ分析）
ローデータ ③	匿名化データ	（調査回答データのみで、IDや個人識別可能データなし）

➢ 自社で完全なGDPR対応ができない場合、想定される対処策は…

データ種類（仮）	想定され得る対処策（＝確定版ではない）
ローデータ ①	基本：ｻﾝﾌﾟﾙ重複ﾁｪｯｸ等の処理は現地企業に委託し、日本には移転しない ・（可能であれば）GDPR対応を終えた日本のシステム企業等に委託する
ローデータ ②	・データ管理体制の明確化、削除手法を含む記録管理の徹底 ・特定機微情報（宗教、健康、労組等）を含む場合は、要追加対策の可能性

1．ESOMARとJMRAが目指すゴール

注）事故対応は別

◆ ESOMAR綱領とGDPR『行動規範』遵守企業へのお墨付き

- ESOMAR会員、またはESOMAR綱領を批准した各国協会員で、ESOMAR版 GDPR『行動規範』の遵守宣言を行った企業を、
  ⇒「**個人データ域外移転規制の免除**（＝クリアとみなす）対象」に
- つまり、「GDPR行動規範を遵守するJMRA会員であれば、GDPRの制約を逃れてEU域内で調査活動を行える」ようにすること
- ただし、宣言（＝行動規範）に違反した場合には厳罰に処される
  ⇒ 遵守を証明する**文書記録管理**が重要

※） 欧米流の規制や管理に特徴的な考え方

- ✓ 基本原則や重要な事項は、法律で厳格に規制
- ✓ 詳細は、業界ごとの自主規制や行動規範に委ねる（性善説？）
- ✓ しかし、それに違反した場合には厳罰で臨む（＝即アウト！）

＜参考＞ ESOMAR版『行動規範』で規制をクリアできる理由は？

◆ 最初期からのロビー活動の成果

- ESOMARの長年の実績と、それに基づく信頼
- 本来、市場調査業は個人データをそのまま使用する業種ではなく、統計的に処理して使うことが主目的のため
- **もともと業界別『行動規範』は、規制クリアのための正規ルート**
  （規制当局側でも、対応リソースは限られている）

◆ 個人データ取得の必要がなければ、それに越したことはない

- できるだけ個人データを扱わず、統計加工されたデータや、匿名化されたデータのみ扱うことにするのが望ましい
- IPアドレス等を含む個人データを重複チェック等に使用したとしても、**すぐに削除するか匿名化する手順にすればリスクは軽減**

＜参考＞ ISO20252の活用方法

- **残念ながら、現行のISO20252認証が直ちにGDPRの要求事項を満たすわけではないが…**
  - ESOMAR版のGDPR『行動規範』は、2018年中に完成予定
  - 改訂版ISO20252は、2018年11月発行目標
    ⇒ GDPR『行動規範』と改訂版ISOの内容はリンクするが、残念ながらそれがGDPR規制を全クリアすることには直結しない
  - しかし、GDPRの**文書記録管理**に信頼性を持たせる意義あり
    ⇒ 現在、おそらく2018年末時点でも、ISO以上の認証制度はない
    ⇒ 定期的なチェック、想定外の事故予防のためにも有効

- **ISO20252: 2018には、アクセスパネル管理とISO19731（デジタル分析／Web解析）も統合される**
  - 総合的な信頼性向上により有用　**（日本でも認証体制準備開始）**

2．GDPRへの基本的な対応策 ＝「同意」取得と記録管理

- **最大のリスク要因は、個人データの域外移転（に伴う事故）**
  - 「十分性認定」があっても、万が一「事故」が起これば致命的に

- **自社管理の調査を実施し、安全にデータを移転するには？**
  - **まず、集計結果（統計データ）のみを移転する場合は対象外**
  - **基本的には、データ主体の「明示的な同意」を取得**
    - **⇒ 記録の管理、適格な維持が重要に**

この詳細は『行動規範』待ちだが、当面は従来と同様の方法でOK

  - 他に、現地のグループ会社（子会社）が調査を実施する場合
    - ⇒ BCR: 拘束的企業準則の承認取得（日本では楽天、IIJなど）
      （ただし、中小企業には容易でない）
  - 他に、現地の提携先企業に委託して調査を実施する場合
    - ⇒ SCC: 標準契約の締結（EU当局指定の**各国語版**ひな型あり）
      （ただし、案件ごとに毎回届出や更新が必要＝容易でない）

3．そもそも、EU戦略をどう考えているか？

◆ 貴社の海外事業におけるEU市場の位置付けは？

- EU、US、中国、ASEAN…等の中での相対的重要性は？

  ⇒ 日本が十分性認定を得られる以上、「攻めるチャンス」ではある
  （重要顧客の戦略・方針も影響する）

- 現地で戦略的パートナーを得られるかどうかがポイント

  ⇒ 日本企業が単独で（日本から）オペレーションするのは無理（!?）

◆ 選択肢は「何もしない」～「積極投資」まで幅広い

- EUでのプロジェクト数が少ない場合、「何もしない」手もあり

  ⇒ 従来通り（日本のPマーク対応のみ）でも、乗り切れるはず
  ただし、業務の防衛的観点からは最低限の対応準備が望まれる

- GDPR対応が拡販の機会になり得れば、費用対効果の見極めへ

  ⇒ 現地で「有用な代理人 or 提携パートナーの探索」が可能か？

４．早急に検討しておいたほうがよいこと

1. 会社を代表するGDPR担当者の指名（少なくとも英語対応が必要）

- EU規制当局及びEU市民からの問い合わせ先として明示
  ⇒ 将来的には「EU域内居住のEU市民への委嘱」を考える

2. EU域内で扱うデータの棚卸、データフロー図の作成

- 収集・処理・移転される個人データの所在や使用法の精査(Scan)

3. データ処理と移転の文書記録システムの整備

- 追跡可能な記録管理が必要、**ISO20252と連動させる**のがよい

4. DPO（Data Protection Officer）委嘱の検討（推奨事項）

- おそらく大多数の会社において義務ではないが、信頼性は高まる
  ⇒ 現実的な手段としては ESOMAR Plus の活用しかないが…？

5．対応必須となった場合の要求事項

ESOMAR Plus の活用ご検討を

◆ **以下、もしも本格的な対応が必要と判断された場合には…**

継続的かつ大量の域外データ移転を行っている（行う予定がある）場合

5. リスク評価（データ保護影響評価：DPIA）の実施

- 自社が行うデータ処理のリスク評価と対策立案

6. データ処理・移転の適法性根拠の確認

- 収集・処理は「同意」が前提、移転は「十分性認定」で

7. データ侵害時の対策立案

- 「72時間以内」の規定があり、これはかなり大変

8. データ主体の権利確保のためのシステム的対策

- データポータビリティ、忘れられる権利など

⇒ 現地のシステム委託事業者との協力・連携が不可欠

＜参考＞ ESOMARがEU当局との交渉を通じて得ている感触

- **本気で課徴金を課す腹積もりがあり、準備もできている**
- **しかし、施行初日からフル適用しようというわけではない**
  - GDPR施行から1～2年は、各国の執行状況をうかがう予定
  - 当面の関心は、FacebookやGoogleなどのIT大手に向いている
  - ただし、何の準備もしていなければ大変なことになるとの脅しも
    ⇒ 仮にすべては間に合わないとしても、努力を継続することが重要
- **ESOMAR版『GDPR行動規範』は認可の可能性が十分に高い**
  - よほどの事故でない限り『行動規範』の策定・認可までは猶予期間(?)と期待される

【ESOMARの担当：Kimさん】

6．よくいただくご質問について

① EU現地の提携先に調査委託する場合の契約書などは？

- SCCの英文ひな型は提供できるが、日本主導は考えない方がよい
  （欧州は多言語社会、英語版だけでは済まない。弁護士費用もたいへん）
- EU域内企業は法的にGDPR対応が必須、先方に合わせることで対応

② すでにEU域内でFGI を受託してしまっている場合の対処策は？

- 当面は、調査対象者からの明示的同意取得の徹底（書面内容は委託先に依頼）で大丈夫 （⇒『行動規範』公表後、英語版ひな型は検討予定）
- ただし、P14の 1.～3. には手を付けておくべき（何もしないのはマズイ）

③ 日本在住 or 滞在中のEU市民に調査する場合の対応策

- EU市民であっても、日本在住/滞在中の調査には日本法が適用される
- Pマークの規定に沿って同意を取得しておけばOK
  （そもそも、そんな個人データを取得する必要性があるかは「？」）

6．よくいただくご質問について

④ EU市民が混入し得るWeb調査を実施する場合の実務的対応は？

- 例えば英語版調査票があり、日本のサーバでIPアドレス等を管理する
  ⇒ 日本国内でチェック・加工する場合でもGDPR規制対象になり得る
  （英語版のみだとギリギリセーフかも？ 独語や仏語版もあるのならアウト）

⇒ Web調査で海外発のローデータを扱う必要がある場合には？

- まず、取り扱う「ローデータ」の定義・内容を明確に
  （住所や氏名の有無は当然として、他に個人特定につながる情報は何か？）
- 外国語版は実査時にポップアップを表示し、Cookie使用の承諾を得る
  （「うざい」が、他業界でも多用 ⇒ 回収率にどれだけ響くかは未知数？）
- マッチング等に**使用した後、速やかに削除する手順**とする
  ⇒ **手順書に明記**のほか、**削除した記録を確実に残していく**こと

※）仮に事故が起こってしまったとしても、規制に対応しようとしている（していた）姿勢が認められれば、制裁にまで発展する可能性は低くなる

7. ESOMAR Plus のご紹介

- **JMRAとESOMARのパートナーシップ契約に基づいて仲介**
- **ESOMAR会員向けのアドオンサービス（有料）**
  - まず、ESOMARの**法人会員加入**が前提

参考：
ESOMAR
法人会費 →

1EUR=@130円として、
約180,000円
～650,000円

常勤従業員数	基本価格	追加費用（本社以外の拠点国追加）
10人以下	EUR 1,400	
11～50人	EUR 1,800	+ EUR 500/国
51～150人	EUR 2,500	(1ヵ国につき1メンバー登録)
151人～500人	EUR 3,500	
501人以上	EUR 5,000	

- **具体的に、どんなサービスが受けられる？**
  - ESOMAR提供資料に沿ってご紹介

ESOMAR Plus のご紹介

ESOMAR

2018/06/18
GDPR Seminar 2: by JMRA

ESOMAR

ESOMAR Plus: あなたの GDPR コンプライアンスパートナー

ESOMAR Plusは、ESOMARの法人会員向けコンサルティングサービスです。貴社のニーズやデータ保護の準備段階に応じて、4種類の契約形態を提供します。

ESOMAR Plusは、一般データ保護規則（GDPR）施行にあたって、具体的なガイダンスを市場調査・インサイト・データ分析業界向けに提供するために開発されたサービスです。

GDPRは、ヨーロッパ内外においてEU市民の個人データを処理するすべての事業者に向けた、新しい要求事項を導入します。

ESOMAR Plus パッケージ：概要

DPO委嘱サービスは「アドバンス」以上

ベーシック（Basic）

- ESOMARが作成するガイダンスノート（指導メモ）及び説明資料へのアクセス；
- 精選された‘知識共有’ ウェブセミナー 4件；
- 実用的なテンプレート、及び貴社のコンプライアンスを証明するガイダンスを含む、ESOMARの「GDPRツールキット」；

価格：

法人会費の20%＋ EUR*1) 750～
（約97,500円*1)～）

*1) 1EUR=@130円で計算、以下同じ

アドバンス（Advanced）

- ベーシックパッケージに含まれる全ての特典；
- 日々の運営上の質問に対してお答えする、ESOMARの問合せ窓口への優先的アクセス；
- 貴社専用のGDPRのご紹介；
- 新しいESOMARガイダンスに関するアップデートを報告する専用ウェブセミナー；
- ESOMARの社内DPO（データ保護責任者）によるデータ保護指導サービス；
- 7点の無料改訂文書を含む完全版「GDPRツールキット（資料20点）」；

価格：

法人会費の20%＋ EUR 5,000～（65万円～）

ESOMAR

ESOMAR Plus パッケージ：概要

プレミアム（Premium）

- アドバンスパッケージに含まれる全ての特典；
- 貴社スタッフ向けに、データ保護と綱領のエキスパートが専用の研修プレゼンテーションを実施；
- 新しい基準や新たに発生している基準に関する貴社専用のアップデートウェブセミナー；
- 貴社のデータ処理活動、契約及び個人情報保護方針のスキャン（精査）；
- データ保護指導サービス；

価格：法人会費の20%＋ EUR 15,000～（195万円～）

アルティメット（Ultimate）

- プレミアムパッケージに含まれる全ての特典；
- 貴社スタッフ（最大50名）向けの複数日オンサイト研修 1回；
- 個人情報保護方針及び契約の詳細な監査；

価格：法人会費の20%＋ EUR 25,000～（325万円～）

アドバンス、プレミアム及びアルティメットパッケージへの追加可能サービス

1. **プロジェクト別コンサルティング**：スキャンの結果に基づいて、ESOMARは提言を実施するためにビジネスを支援できるエキスパートへのアクセスを提供します。費用は1時間当たり€250、またはプロジェクト毎に。
2. **データ保護責任者**：GDPR、ESOMAR綱領及びガイドラインに関するトレーニングを受けた外部弁護士を、ESOMARが外部データ保護責任者として提供します。費用は1時間当たり€300、またはプロジェクト毎に。

ESOMAR

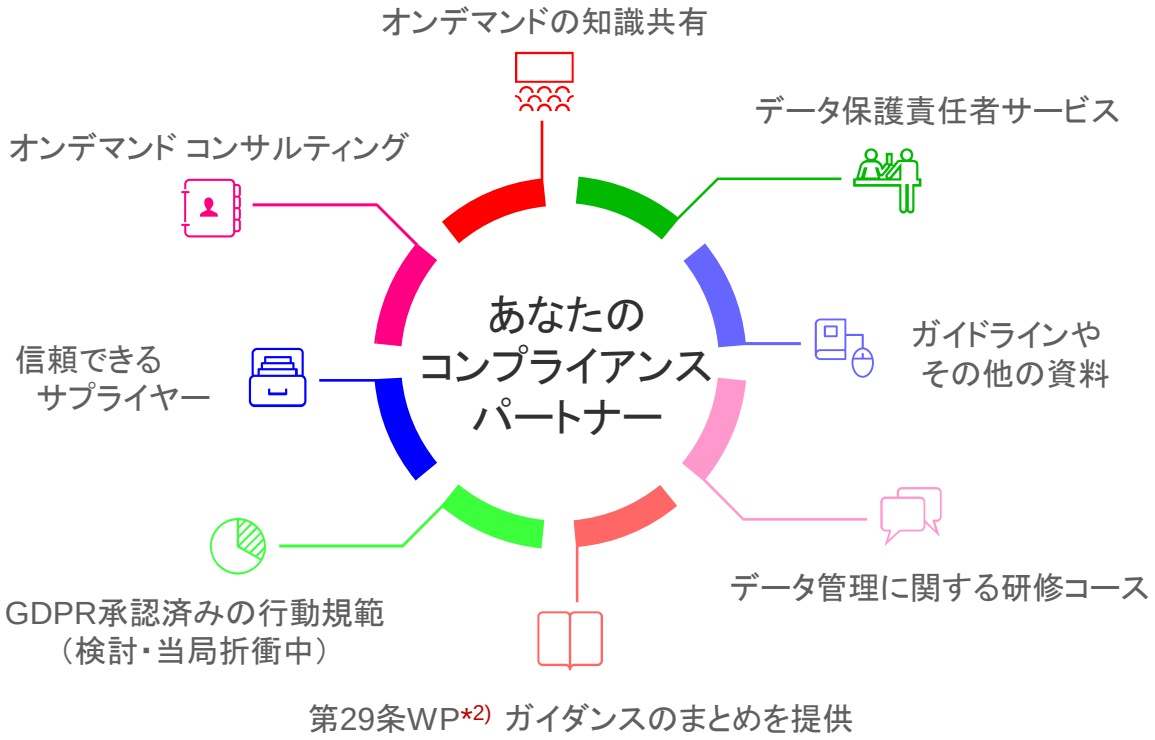
ESOMAR Plus

幅広い製品やサービスを通して貴社のコンプライアンス向上を図ります。

詳細及び正確なお見積もりをご希望の場合は、こちらまでご連絡下さい。

professional.standards@esomar.org

お待ちしております！



*2) GDPR以前の規制であるEUデータ保護指令の第29条に基づく作業部会と、その部会が発した文書類を意味する。

協力: JMRA

＜参考＞ ESOMAR Plus の実際

- **Basicでは基礎知識と基本テンプレート等の入手**
  - 名称を貴社名に置き換えれば基本的な文書体系が完成
- **Advancedで「貴社専用」窓口、DPOサービス委嘱可能に**
  - 継続的なGDPR対応のためにはここから(？)
- **Premiumで貴社内データや契約の「Scan（精査）」サービス**
  - 本格対応が必要と見込まれる場合、ここまで行かないと(？)

    ⇒ ESOMAR『Research World Connect』最新記事（6/12付）を参照
    https://rwconnect.esomar.org/why-a-scan-either-conducted-by-esomar-or-someone-else-is-key-to-getting-gdpr-right/
    - 最初の重要なタスクは、組織の「データマッピングスキャン（精査）」
    - スキャンを通じて①データ処理の見える化、②できていないことの確認、③改善のための優先課題を抽出 ⇒ GDPR対応の「地図」を作成する
    - トップラインだけでも1日、レポート提出までにまる1週間必要

＜参考＞ JMRAとしての今後の打ち手（案）

◆ ESOMAR Plus の関連サポート

- 資料翻訳、質問対応等（社内資源の限られる会員社向け個別対応）

◆ 対外的アピールの検討（日本国内の顧客や関連事業者向け）

- ある程度の対応方針が明確化した段階での「声明」発表など

  ⇒ 「十分性認定」発効や『行動規範』草案公表等のタイミングか？

- クライアント向け「GDPR勉強会」
  開催または個別サポート

※）最終的には、ESOMAR版『行動規範』の公表（年内の見込み）をお待ちください

<Q&A>

あなたの中に未来がある。

一般社団法人 日本マーケティング・リサーチ協会