11/9 JMRA GDPRセミナー

ESOMAR | 70
WORLD RESEARCH

Agenda

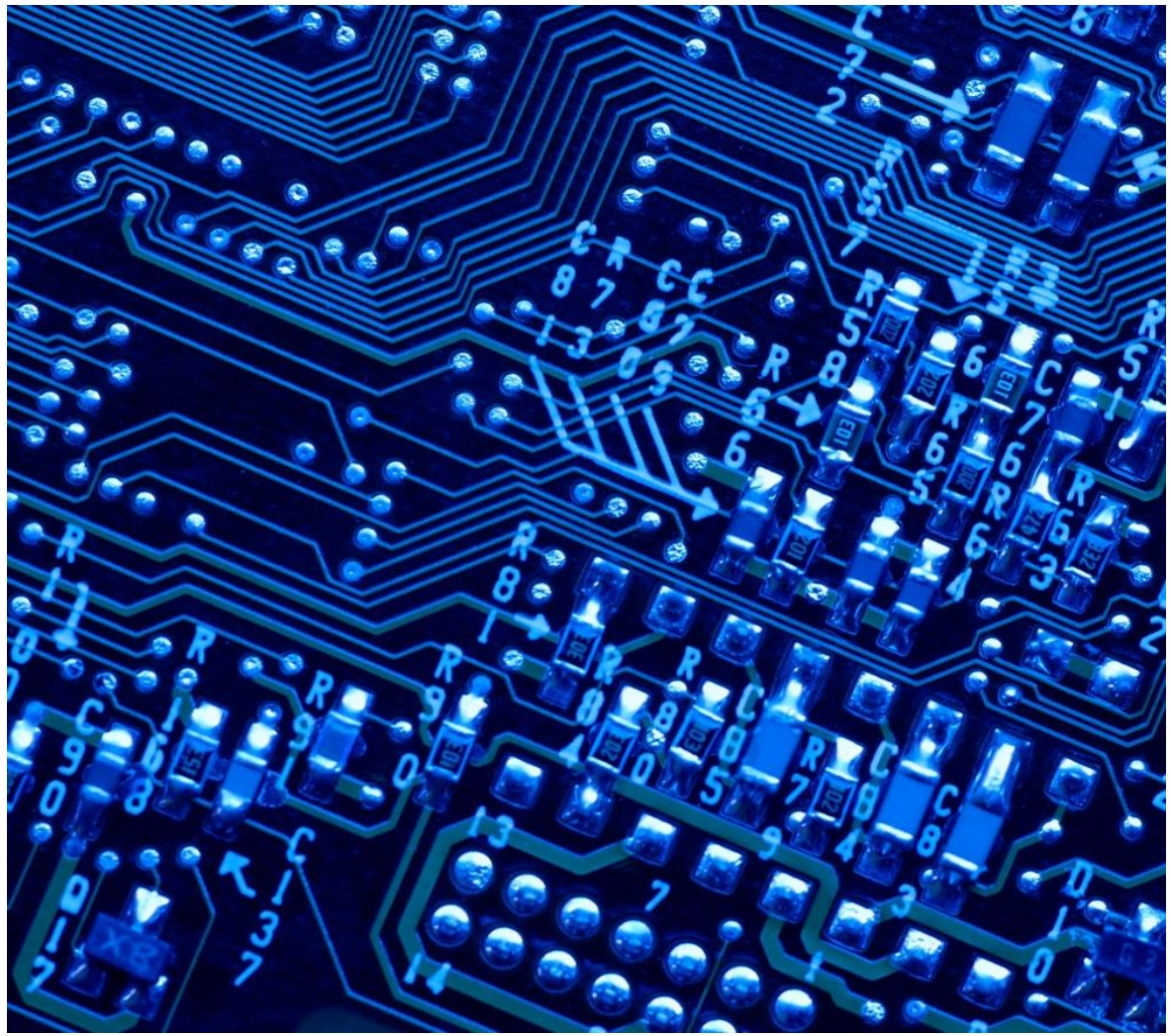
- GDPRに適合するための12のステップ

- トピックス：政策提言の強化（重要政策・規制への対応）
  - GDPRから派生した規制強化の動きへの対応
    （eプライバシー規制強化と、著作権制度改革）

- 想定される質問と、現段階での回答

GDPRに適合するための12のステップ

ESOMAR Plus のナレッジシェア



推奨される 12 のステップ

1年以内にGDPRへの準拠を
達成するプログラム

GDPRに適合するための12のステップ

ESOMAR Plus のナレッジシェア

① 組織的対応
- ✓ 専門チームの編成と権限付与
- ✓ DPO（データ保護責任者）の任命

② 追跡可能な記録の管理
- ✓ プライバシー影響評価
- ✓ チェックリスト（テンプレート作成中）
- ✓ 定期的なレビュー

③ データフローの監査

④ 長期的なデータ戦略

⑤ 想定外の事態への対処

⑥ ユーザーの権利尊重・同意取得

⑦ セキュリティの確保

⑧ データ主体とのコミュニケーション

⑨ 危機管理計画

⑩ データチェーン全体での安全確保

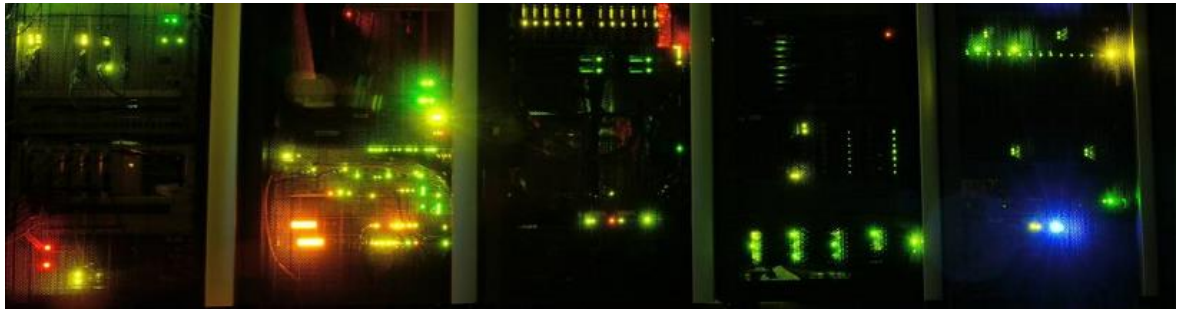
⑪ 第三国へのデータ移転
- ✓ 移転を可能にするための条件

⑫ プライバシー保護文化の醸成

ESOMAR | 70
WORLD RESEARCH

留意すべき重要な事項

GDPRについて

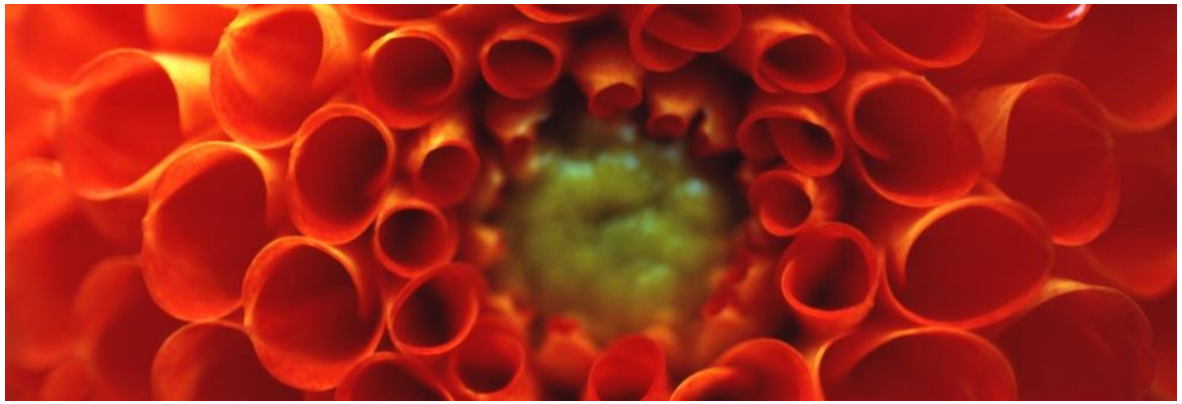


- すべてのEU加盟国に適用される
- EU内外の全企業に強制適用される
- 対象範囲は個人データ (直接的または間接的に本人が識別できるデータ)
- 違反した場合に巨額の金融負債が発生
  - ✓ 2000万ユーロまたは全世界売上高の4%（いずれか大きい方）

ESOMAR | 70
WORLD RESEARCH

2018年5月25日

まもなく、それは現実になる！

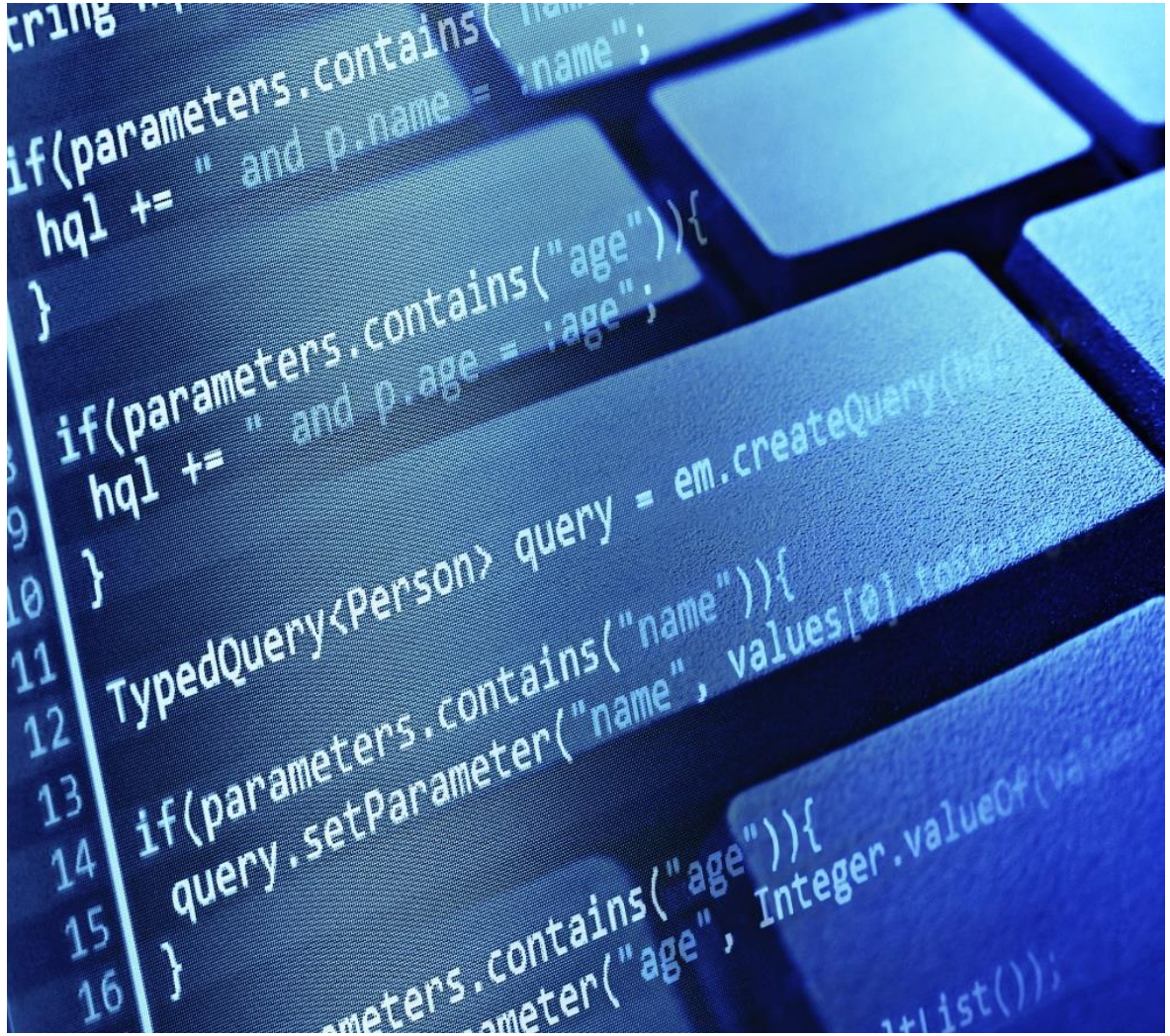


ESOMAR | 70
WORLD RESEARCH

ものごとを正しく理解しよう

GDPRの下で、すべてが可能になる

GDPRは、データ活用でできることを制限しようとしているのではない。
セグメンテーションからビッグデータ分析まで、すべてが実施可能。



ESOMAR | 70
WORLD RESEARCH

GDPRへの 適合のために、データの流れ(Data Flows)を知る必要がある

Step 1

オーケストラの統率者を保持することが重要

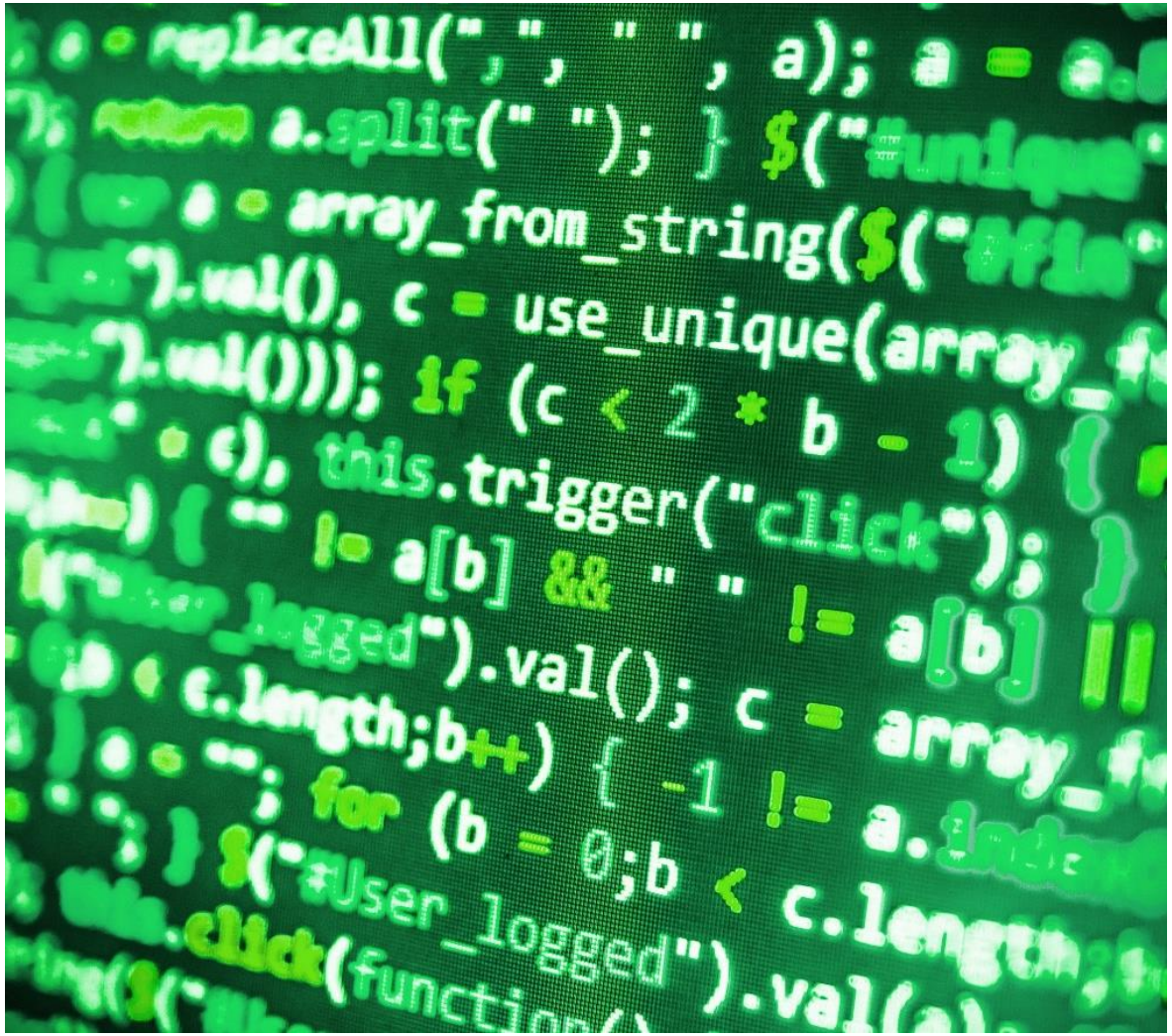
- **準拠対策をリードする多機能チームを組織:**
  - 上級幹部職（シニアマネジメント）
  - IT・情報システム
  - 運用・オペレーション
  - 人事・教育訓練
  - マーケティング
  - 法務
- **チームのすべての議論、結論、行動の記録を残す（追跡可能であることが必要）**

責任者は、EU内居住者が必要に

ESOMAR | 70
WORLD RESEARCH

Step 1

オーケストラの統率者を保持することが重要



- チームは、以下に明確な焦点をあてる:
  - ✓ リソース（経営資源）の決定と割当て
  - ✓ 長期的なデータ戦略の設定
  - ✓ データマップの決定
  - ✓ データ使用ポリシーのレビュー
  - ✓ 情報システムのレビュー
  - ✓ リスクアセスメントの実施
  - ✓ データの取扱いを含む契約の更新
  - ✓ データ侵害発生時の対応手順のテスト
  - ✓ データ主体とのコミュニケーション
  - ✓ 継続的な監査とレビュー

ESOMAR | 70
WORLD RESEARCH

Step 1

オーケストラの統率者を保持することが重要

「データ保護責任者(DPO)」の任命は重要で、ほぼ義務となる（小規模企業には免除あり）。

DPOは上級管理職でなければならず、経営陣に直接報告ができ、IT部門やCEOの機能から独立していなければならない。DPOは外部のサービス提供者に委嘱することもできる（⇒ ESOMAR Plusで紹介することも可：P29参照）

DPOの役割は、データ処理活動の記録を保存し、その実施状況を監視し、助言を与えることである。

DPOはまた、データ保護規制当局や世間一般との間のインターフェース役となる。

ESOMAR | 70
WORLD RESEARCH

Step 2

影響評価と記録することを学ぶ

GDPRは、データ管理者とデータ処理者に説明責任を求める

その達成のために、プライバシー影響評価（PIA: Privacy Impact Assessment）を実施し、細心の注意を払った記録を保持しなければならない

PIA記録の保持を義務付け（record keeping obligation）

ESOMAR | 70
WORLD RESEARCH

Step 2

影響評価と記録することを学ぶ

影響評価では、個人データの誤用、事故による漏洩、または侵害が生じた場合の、個人に及ぶリスクのレベルを特定する必要がある。

そのような事態が生じる可能性、どの程度起こり得るか、そして組織がその影響を緩和するための手段について特定すべきである。

テンプレート化を見越した PIAチェックリストを使用

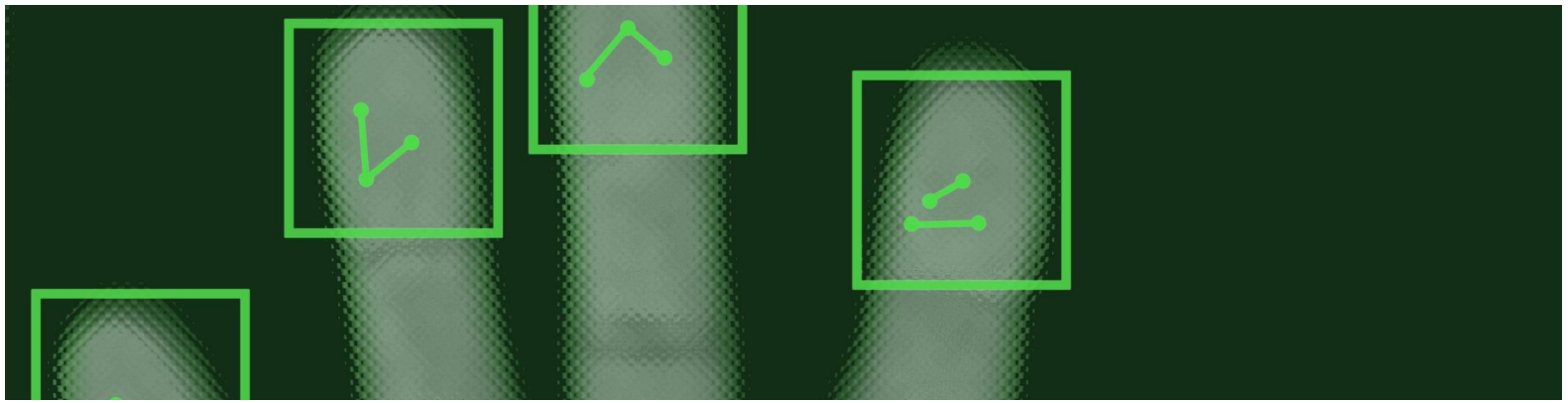
ESOMARのチェックリストが、影響評価の基礎として役立つ。

↓

2018年1月中には公表予定

それをテンプレートとして使用することで、各データ処理活動に対する重要な質問への回答を定義する。

あなたの回答と、実施した手法を文書化する。定期的なレビューも同様に重要となる！



ESOMAR | 70
WORLD RESEARCH

Step 3

データの流れを明らかにする監査

GDPRの説明責任原則は、以下を要求する:

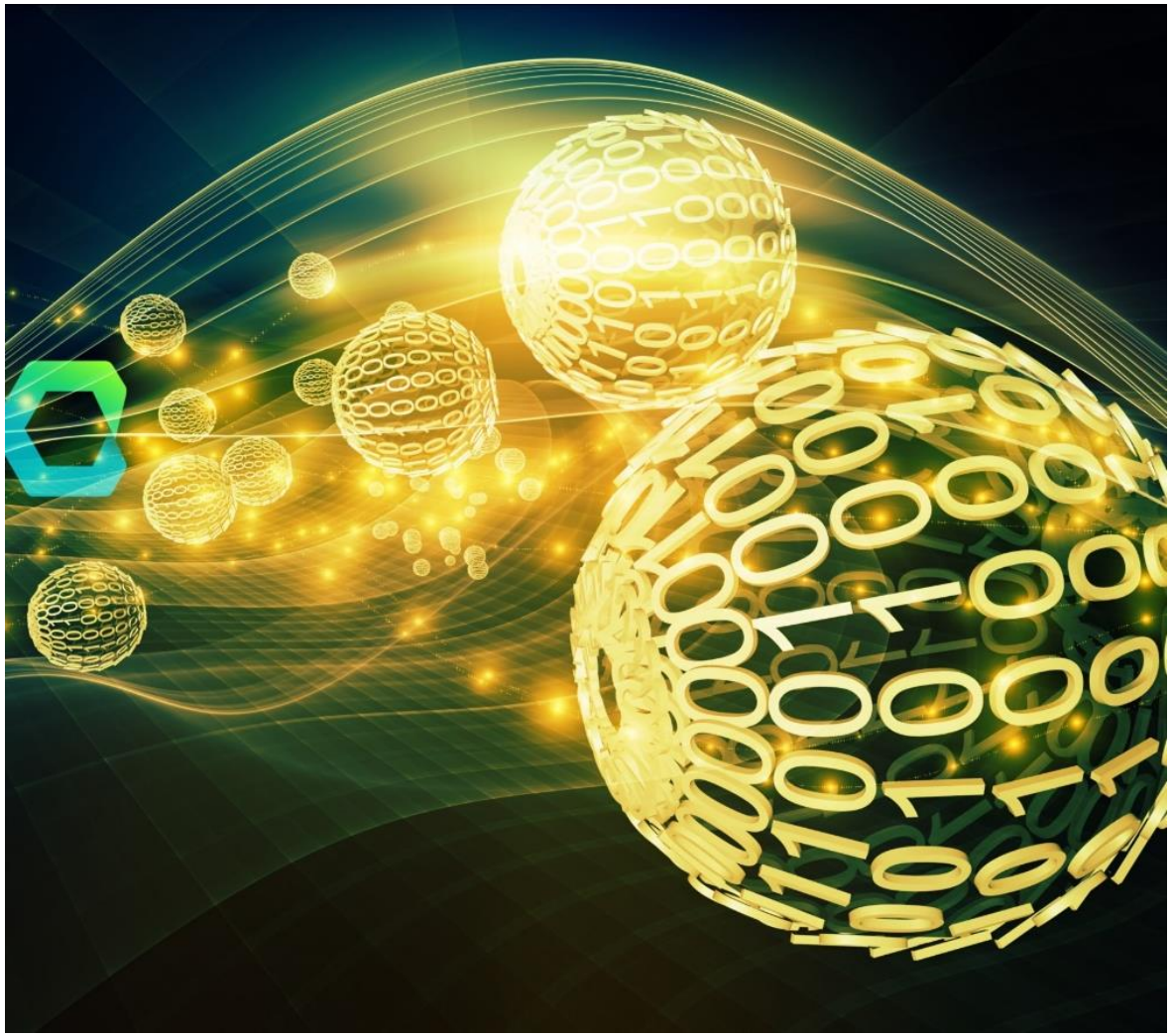
- どのようなデータが入ってくるか？
- どのようなデータが出ていくか？
- なぜそのデータが使用されるのか？
- そのデータは何に使われるのか？
- 誰がそのデータにアクセスするのか？
- そのデータは（他と）組み合わされるか？
- それはどれだけの期間保存されるのか？
- それはどのように削除されるのか？

これは、すべての機能について通知される必要がある（⇒ EU市民に対して）。

ESOMAR | 70
WORLD RESEARCH

Step 3

データの流れを明らかにする監査

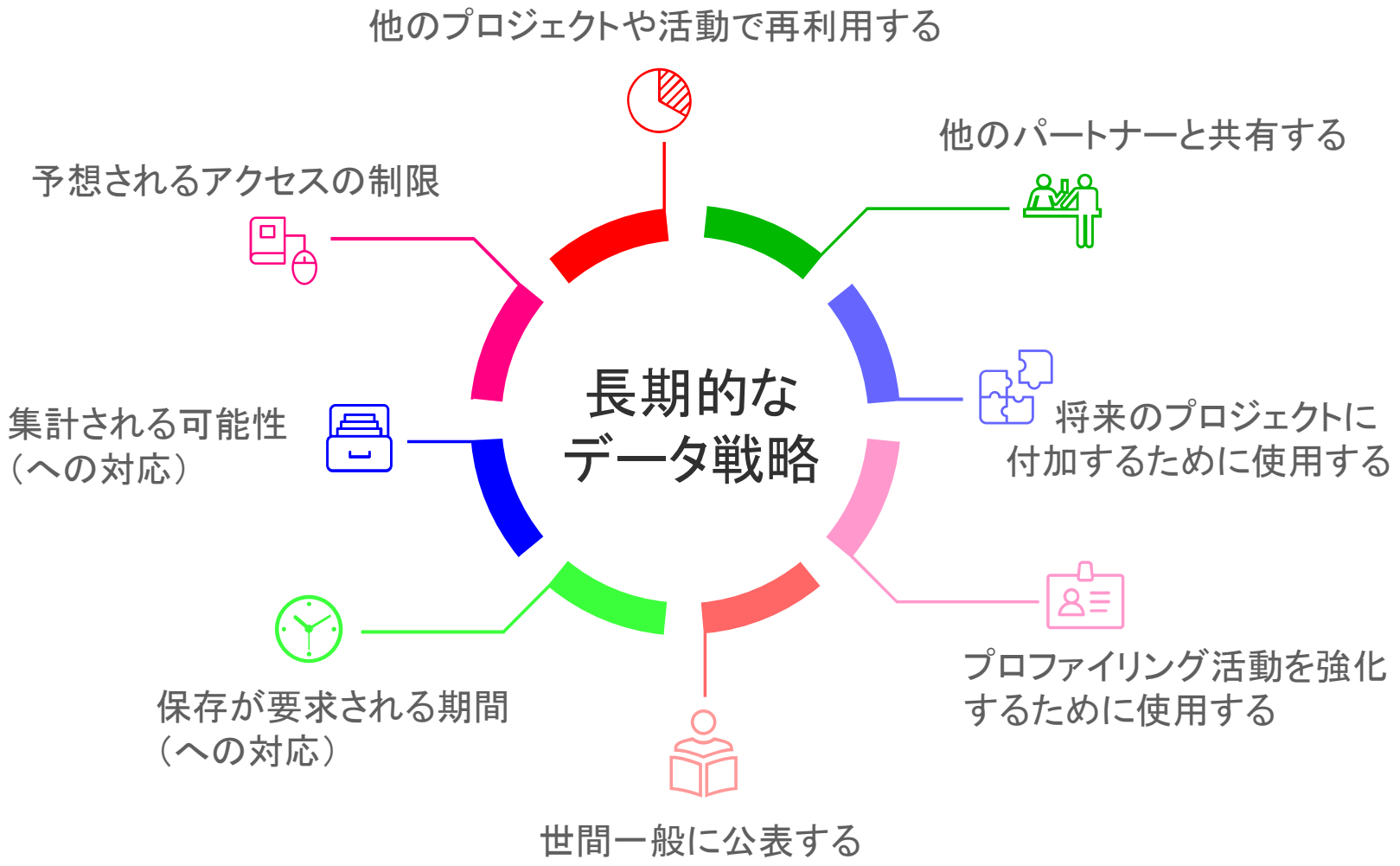


監査の結果記録を常に保存しておくことが、データ保護当局に準拠していることを証明する必要がある場合に重要となる。

ESOMAR | 70
WORLD RESEARCH

Step 4

将来のデータ使用について考える



ESOMAR | 70
WORLD RESEARCH

Step 5

将来のデータ使用について考える

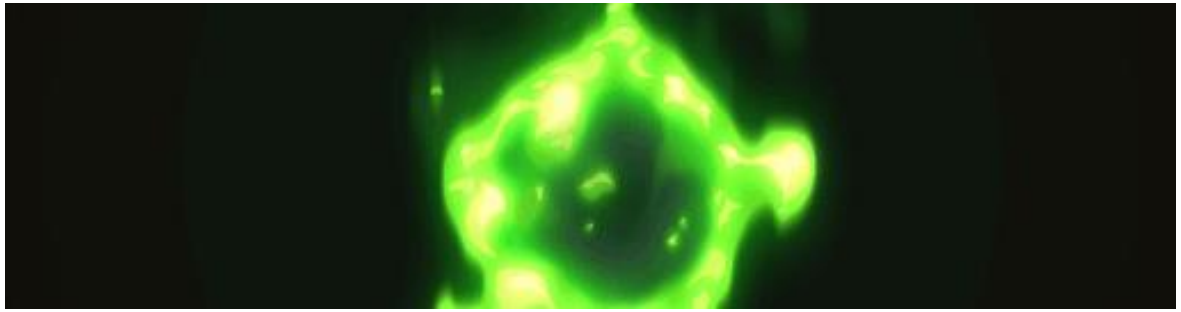
事前情報に関するGDPRの特別な要求事項を達成するためには、想定外の事態についても考慮しておくべきである。

ESOMAR | 70
WORLD RESEARCH

Step 6

ユーザーの権利を有効なものにする

- GDPRは、データ主体のデータ管理権を強化することを目指している。
- 従って、使用されるサービスやツールは、特に同意を使用する時に、ユーザーの権利を有効にしなければならない。
- ユーザーに対して、彼らの権利と、それをどのように効果的に使用するかを通知することが求められる。



ESOMAR | 70
WORLD RESEARCH

Step 6

ユーザーの権利を有効なものにする

システムは、さまざまな権利を幅広く行使するために更新される必要がある。

ほとんどの権利には、満たされるべき一定の条件が課されている。

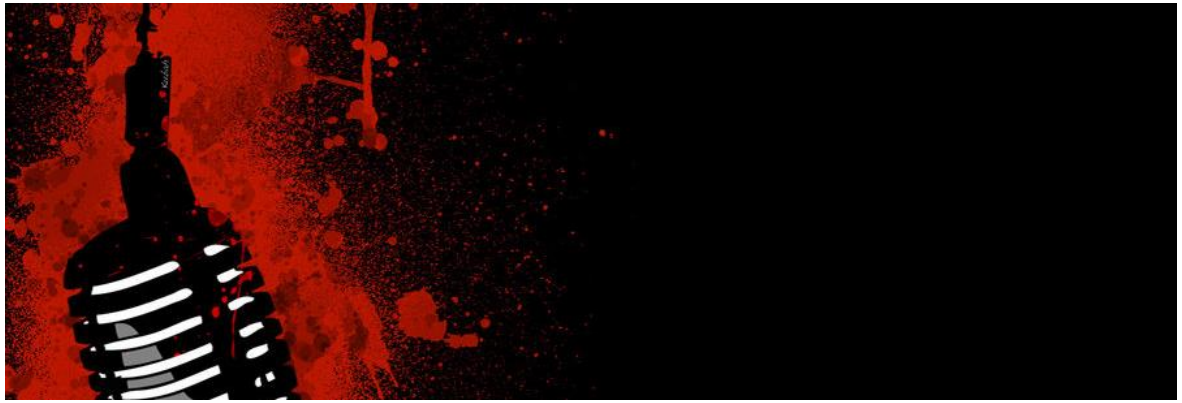
ESOMAR | 70

Step 7

ひたすらコミュニケーションをとる

データ主体への事前通知がカギとなる。
以下について知らされる必要がある:

- （調査機関の）身元情報
- 誰にデータが共有されるのか？
- データはどのくらいの期間保存されるか?
- 苦情を申し立てる、または同意を撤回することを含む、（データ主体の）権利



ESOMAR | 70
WORLD RESEARCH

Step 7

ひたすらコミュニケーションをとる

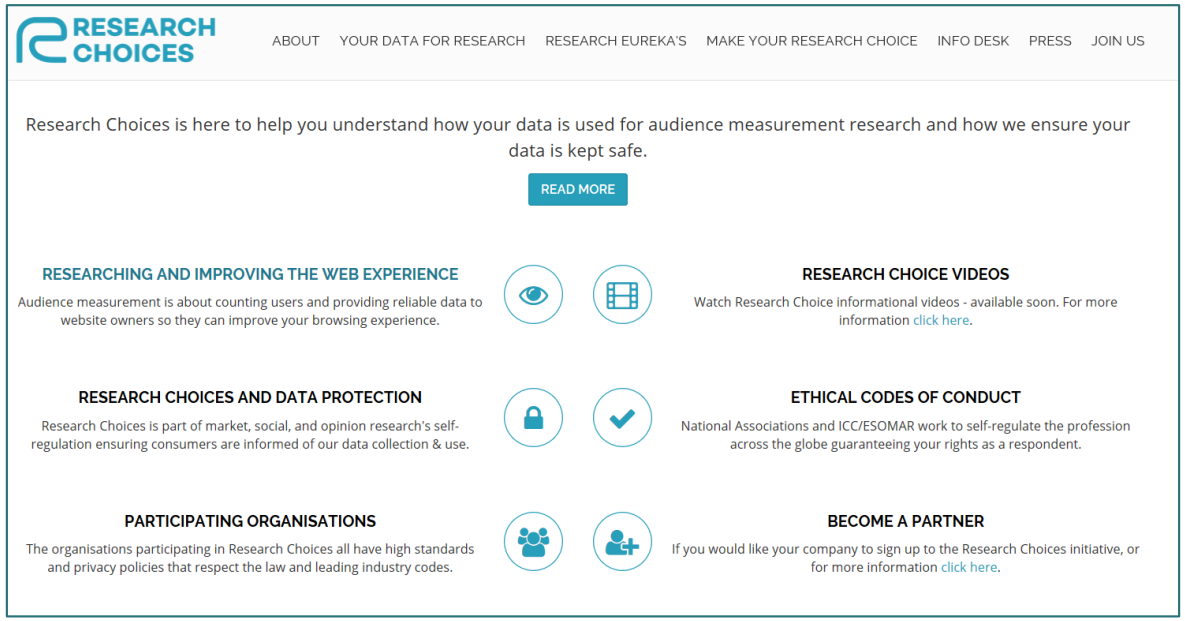
あなたと、あなたのデータ処理活動に対する信頼を構築するために、以下が重要となる:

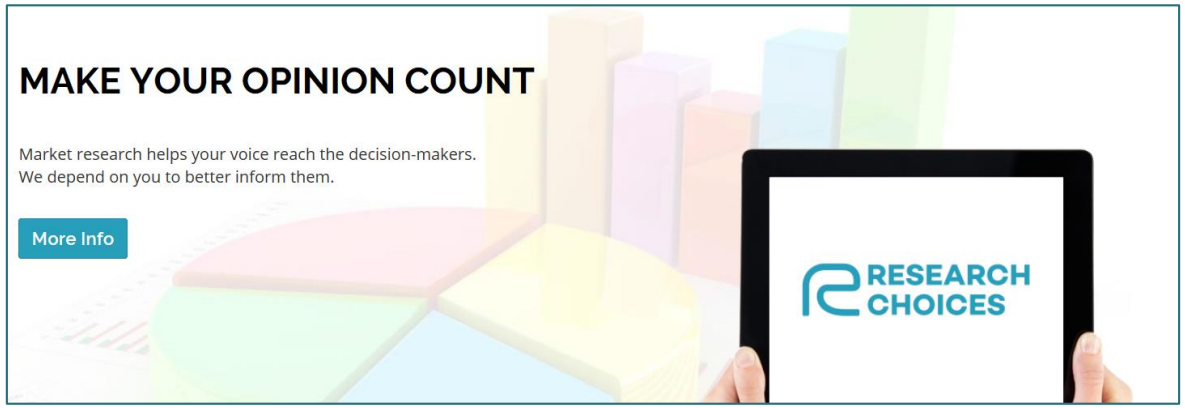
- 簡潔で、ポイントを突いていること
- 透明性があること
- 理解しやすいこと
- 簡単に見つけられること
- ターゲット層に対して適切であること

ESOMAR | 70
WORLD RESEARCH

Step 7

ひたすらコミュニケーションをとる





情報は、多様な形式で提供することができる。

“Research Choices”はオンライン調査のための透明性確保運動であり、あなたのコミュニケーション戦略の一部を構成することができる。

業界共通の慣行を説明する動画も提供。

↓

http://www.researchchoices.org/

ESOMAR | 70
WORLD RESEARCH

Step 8
安全性を保つ

データの侵害を回避し、説明責任を負うことは、データセキュリティ原則の履行を要求する。

- システムと人材がカギになる
- セキュリティの穴を特定し、閉じる
  - ✓ 物理的に、またはデジタル的に
- 脅威に対する抵抗力をテストする

ESOMAR | 70
WORLD RESEARCH

Step 9

データの侵害に備えた危機管理計画

- GDPRでは、（事故が生じた場合に）72時間以内にDPA（当局）に通知することを要求している
- データ侵害が生じた場合、すみやかにその原因と対応策を調査できなければならない
- 追加的な是正処置について、DPA と連絡を取り合うことになる
- ユーザーにも連絡を取ることになる可能性を考慮しておく必要がある
- これは急いで決めるべきではない（慎重に検討）

かなりタフな要求事項？

Step 10
データチェーンの課題

あなたと二次契約業者は、データチェーンの中でデータを安全に保持する責任を負う。
従って、契約で役割を明確にし、パートナーがあなたと同じ重要原則を遵守することを、定期的に確認することがより重要になる。

ESOMAR | 70
WORLD RESEARCH

Step 11

第三国へのデータ移転

従来のデータ指針と同様に、第三国へのデータ移転は厳しく規制され、次のような場合にのみ実施できる:

- データ主体が同意している
- 適切性（十分性）が認定されている国への移転
- SCC（Standard Contractual Clauses）締結済み
- BCR（Binding Corporate Rules）取得済み
- （各業界による）行動規範に則っていること

ESOMAR | 70
WORLD RESEARCH

Step 12

社内のプライバシー保護文化の醸成

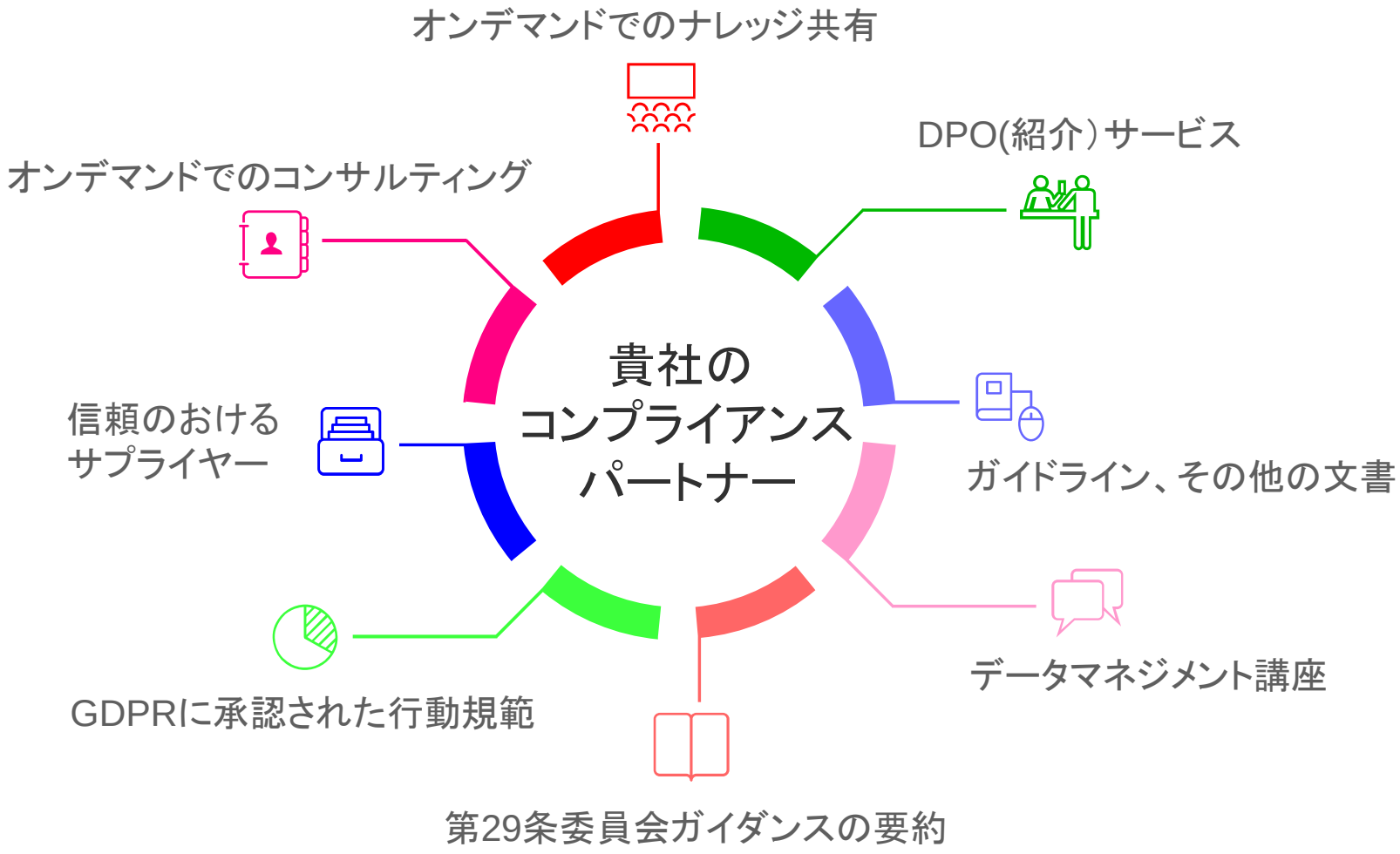
これはDPO（データ保護責任者）に一任された仕事ではない

チームメンバー（＝社員）全員のコミットメントが要求される

利益だけでなく、リスクにも常に気を配った文化が要求される

ESOMAR Plus*)

幅広い製品やサービスを通じて、どのようにコンプライアンスを強化するか？



*)ESOMARが会員に提供する
オーダーメイドの
コンサルティング・サービス
↓
https://www.esomar.org/utilities/esomar-plus

（参考）SERENE*) プロジェクトのご紹介

*) Self Regulation Engine の略

・自主規制に取り組む各国の協会が、共通する課題に対処するためのクラウド型プラットフォーム。規制当局および公衆一般に向け、透明性と有効性をアピールする。

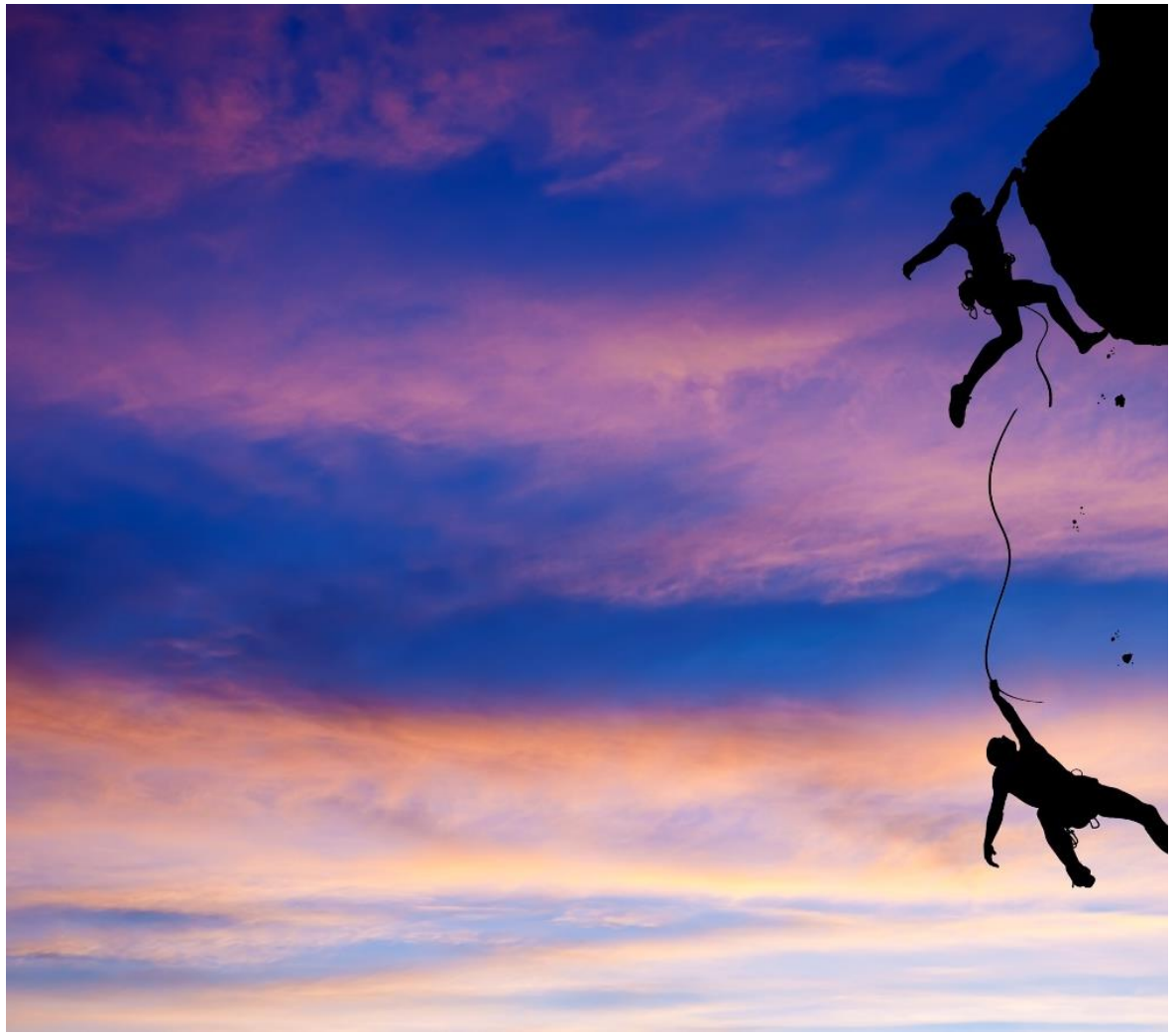
・各協会のWebサイトやポータルサイトを通じて簡単にアクセスでき、苦情申し立て（受付）や回答提供が可能。

・グローバルな知識データベースの構築や、事例ファイルの相互転送なども可能。

重要なポイント

覚えておいていただきたいこと

- 施行日までの時間は限られている。GDPRがあなたの組織に影響を及ぼすことは避けられない。
- マルチな専門性を持ったチームを編成し、12のステップを掘り下げることを通じて作業を進める。
- 認知・自覚、強い関与、モニタリング、経営資源配分、テストの実施、倫理観向上がこの実践を牽引する。
- ESOMARはESOMAR Plusを通じて、コンプライアンス体制強化を支援するために幅広いサービス体制を構築していく。



ESOMAR | 70
WORLD RESEARCH

Questions?

Let’s Stay in Touch:

Kim Leonard Smouter

Head of Public Affairs and Professional Standards

public.affairs@esomar.org

On Linked In | @esoGOV on Twitter

※）本セミナー＆資料に関する
お問い合わせはJMRA事務局まで

ESOMAR | 70
WORLD RESEARCH

注）本セクションには未確定事項を多く含んでいます

トピックス：政策提言の強化

重要政策・規制への対応

（GDPRから派生した規制強化の動きへの対応）

ESOMAR | 70
WORLD RESEARCH

政策提言の強化
重要政策・規制への対応 ①

特に重大

eプライバシー規制強化

- ePrivacy制度改革・規制強化
  - オンライン視聴・行動測定と電話調査に重大なリスク発生
  - 対象：クッキーを用いた受動的視聴測定、承諾されていない電話、そしてクッキーに類似したすべての技術
  - 罰則：GDPR と同様の2,000万ユーロまたは年間売上高の4%
- 対策・活動:
  - 関係団体との連合組織の設立
  - 4本の意見表明書提出、ePrivacy委員会との会合

特に重大

著作権制度改革

- 著作権制度改革:
  - テキストおよびデータマイニング規制を免除させる機会が失われるかも
  - 対象：学術目的のみが免除理由に（＝商業目的は認められない？）
- 対策・活動:
  - EFAMROと共同で1本の意見表明書を起草委員会宛てに提出
  - 幅広い調査団体との連携

世論調査への規制

- 世論調査の危機：
  - 多くの市場 (Latam, Africa, 欧州) が、世論調査の法規制強化危機に直面（Brexit投票、米大統領選の影響）
  - 結果が投票に影響を及ぼす、または「間違う」ことを恐れて
- 対策・活動:
  - 懸念を解消するための、世論調査に関するQ&Aの発行
  - 戦略とポジショニングを含む、ターゲットを絞った政策提言のサポート

ESOMAR | 70
WORLD RESEARCH

政策提言の強化
重要政策・規制への対応 ②

特に重大

eプライバシー規制強化

"Cookie Directive"
とも言われている

- クッキー（類似技術を含む）の利用制限に焦点を当てており、重大な支障を生じる恐れあり
  - 特に、オンライン上の視聴・行動測定（Audience mesurement）と、電話調査（セールス電話を締め出す意図）
  - ダイレクトマーケティングと同じ扱いになりかねない状況
  - 「クッキー利用承諾のポップアップを出す」ことで同意を得る方向性（仏、蘭、独、英BBC放送など）
    - ブラウザごとにポップアップを出し、承諾を得る方針だが・・・ ⇒ 承諾率が心配？ 国によって規制が異なる？

- 協会員で調査目的であることの申請、ポップアップ対策等により、何とか規制を回避できる可能性
  - ESOMAR、EFAMROを含む関連12団体（連合）による働きかけの途上
    ⇔ 年内に最終法案公表か？ ただし、すぐには決まらないだろう（＝ さらにロビー活動の余地）
  - 意見表明書原文は、⇒ esomar ⇒ Position Statement on ePrivacy Regulation で検索可

ESOMAR | 70
WORLD RESEARCH

政策提言の強化
重要政策・規制への対応 ③

特に重大

著作権制度改革

- オンライン上のコメント収集＆利用を認めない方向であり、重大な支障を生じる恐れあり
  - 学術調査目的以外の、いわゆる「ソーシャルリスニング」でのテキストマイニング利用が認められない可能性大
  - 現段階で、見通しはかなり厳しい状況で不透明
  - 「学術調査と同様」であることを訴えて、商業目的調査にも「免除」を要請している途上
    - ESOMARとEFAMROから、具体的な条文修正案を提出（済）

- 決着は、来年3～5月くらいまでずれ込む見込み
  - 意見表明書原文は、⇒ esomar ⇒ Position Statement EU Copyright Reform で検索可

ESOMAR | 70
WORLD RESEARCH

想定される質問と、
現段階での回答

想定される質問と現段階での回答

Q1：日本の市場調査会社が、EU域内の同業者に外注して調査プロジェクトを実施した場合に、追加分析等のために回答結果のデータセットを入手することは可能か？

A1：可能である（事前同意が取れていればもちろん可能だが、そうでなくとも・・・）

- データが匿名化（Anonymized）されている場合：個人データにはあたらないので、当然可能
- データが仮名化（Pseudonymized）されている場合：
  - 識別子（identifiers）については提供されないはずであり、結果データのみであれば可能

匿名化データのイメージ：

Code	性別	年代	居住国	職　業	・・・
00001	男	20代	フランス	公務員	・・・
00002	女	30代	ドイツ	専業主婦	・・・
00003	男	40代	スペイン	自営業	・・・
:	:	:	:	:	:

仮名化データのイメージ：

Code	性別	生年月日	Postal Code	職　業	・・・
10231	男	19881024	75009	警察官	・・・
30052	女	19810213	10115	専業主婦	・・・
42813	男	19700831	28039	青果商	・・・
:	:	:	:	:	:

想定される質問と現段階での回答

Q2：日本の市場調査会社が、EU市民を対象としたオンライン調査を実施する場合に、事前に参加者の同意を取れば日本国内のサーバを使用することは可能か？

A2： 可能である

- ただし、明白な同意と、それを証明する記録が必要（同意クリックのデータ記録など）

Q3： 現在、日本政府はEUとのデータ移転認証（＝十分性の認定）を獲得するために努力しているが、欧州側から見てその実現可能性はどうか？

A3： 有望と見られている： おそらく、次に認証される最初の国々のグループに入るだろう

- ただし、新しい要求事項や条件、時期などについては何とも言えない

（注： EUと米国の間では、単発的だが Privacy Shield 制度が発効しており、データ移転が可能）

想定される質問と現段階での回答

Q4：現実問題として、日本を含むEU域外の市場調査会社が、何らかの違反を理由にEU当局から訴追される可能性はどの程度ありそうか？

A4：ケースバイケースだが、おそらく最初の1～2年は大丈夫であろう

- 施行当初は規制・制度の周知期間となり、Best Effort でやっている限り告発まではいかない（？）
- 規制当局も、（罰金を多く取れる？）大型案件や、より悪質な案件に注力するはず
  - 一般に、市場調査会社（ESOMAR綱領を遵守しているはず）が悪質な違反をする可能性は低いと思われ、また案件も大型になるとは想定しにくい

Q5：具体的には、何をどう準備していけばよいのか？

A5：ESOMARで準備している『GDPR行動規範』の遵守を

- この年末までにドラフトを作成する予定
- そこから議論に入り、2018年末までには効力を発効させたい