protiviti
Face the Future with Confidence

2018年2月15日ウェブセミナー「EUにおける一般データ保護規制（GDPR）の概要と対応のポイント」 ご質問とプロティビティの回答

No.		頂いたご質問	Protiviti回答
1	適用範囲	EU域外（日本やアジア）に居住する自然人も対象になるのでしょうか。	EU域外に居住する自然人が、出張や旅行時にEEA域内で取得された個人データは、GDPRの適用対象となります。
2	適用範囲	EU域内に居住する日本人（EUへの出向者）は、GDPR対象になるのでしょうか。	対象になります。
3	適用範囲	出張などで、EU域内で、交換した「名刺」を、日本帰国時に持ち帰った場合は、域外への移転、域外での取得に該当するのでしょうか。	データ化して域外へメール転送されるなどしない限り神経質になる必要はないと思われます。また、域外での取得には該当しません。
4	適用範囲	代理店経由でなく国内の事業所で個人データ（氏名・住所・パスポートNo・CRカードNo等）をEU圏内の個人客より取得する場合にも適用されるのでしょうか。	EU所在者がホテルやレストランをオンライン予約する場合などは、GDPRの域外取得に該当し得ます。 パスポート番号やクレジットカード番号は機微情報に該当しますので、本人からの明示的な同意取得を確実にされることをお勧めします。
5	取得の妥当性	現在、英国の小規模現地法人（子会社）より、緊急時の連絡用（安否確認等）に氏名・性別・年齢・連絡先（TELormailアドレス）を取得しているが、「正当な利益」の主張は可能でしょうか。	EU現地法人の社員の個人データ取得が、グループや組織の運営において、また労務管理上も必要であると認められる場合は、正当な利益であることを主張することが可能であると思われます。
6	取得の妥当性	親会社として、英国現地法人の子会社の内部監査を行う際、取得資料に現地社員の勤務データ等が含まれる場合がある、このような場合、親会社としての「正当な利益」を主張できますでしょうか。	主張できると考えます。 GDPRの制裁金が課せられる場合、親会社を含むグループ企業全体での世界売上げが基準となることが予想されるため、親会社としてグループ全体のコンプライアンスを確認する責任と権限を正当に有すると考えてよろしいのではないでしょうか。 上記に加え、監査計画書の中で監査目的と個人データの取得（勤務データ）の関係性・妥当性を述べておくことをお勧めいたします。
7	対応内容	日本国内に本社がある企業から、EEA域内のグループ会社に出向しているメンバー（=EEA域内在住者）も対象になるかと思います。 具体的にはどの程度の対応が必要なのでしょうか。 法令上の特例として明示的な本人同意を取得することで対応済みとしてよいでしょうか。	社員の個人データを取り扱う上での対応という前提でご回答いたします。 個人データの利用目的を本人に明示して、オプトアウトなどではない明確な同意（本人のサイン等）を取得しておかれることをお勧めします。なお、利用目的についてはGDPRに対応した内容となっているかを再確認されることをお勧めします。
8	体制・役割	GDPR対応のプロジェクト体制において、グローバルカンパニーの場合、どこがイニシアチブをとるべきなのでしょうか。（欧州側の会社なのか、日本の会社なのか）	個々の企業の管理方針や業務内容等によって異なります。 EUにおいて活発にビジネスを展開されているのであれば、EUにおける主要な拠点を定め、そこでイニシアチブを取る体制の方が、当該国の監督機関との連携や報告等が一番円滑に行えると考えます。EUでのビジネス展開がそれほど活発ではない場合は、日本の本社等でイニシアチブを取られる企業も多くみられます。 企業グループのガバナンス体制の構築方針（日本本社からの集中統制、各地域HQへの積極権限移譲等）と合わせることも肝要です。
9	体制・役割	内部監査部門の事前の役割の説明がありました。ややセカンドラインが担当すべき業務が入っていたように聞こえましたが、もう一度、監査部門の「事前」の役割についてご説明頂けないでしょうか。	個々の企業により内部監査部門の位置づけが異なりますが、コンサルティング的な役割も担える環境であれば、これまでの監査を通じたグループ内の各種統制状況の理解、評価のスキル等を活用し、GDPRの対応準備の整備状況の評価や、リスク・コンプライアンス・倫理に関する専門知識の提供等を通じて対応を支援することが可能と考えられます。