2019年7月11日
JIPDECセミナーレポート

GMOグローバルサインにおける国際法対応とAPEC CBPR取得の経緯について

GMOグローバルサイン株式会社
内部監査室長＆ Data Protection Officer　木戸　啓介　氏

GMO グローバルサインは、様々な基本システムに組み込まれているパブリックルートの証明書を発行している。もともとはベルギーの国民 ID プロジェクトの一環で、日本でいうところのマイナンバーの証明書を発行する認証局として設立された。その後、2003 年に GMO グループ傘下に入り、2006 年より GMO グローバルサインとして日本でサービスを提供している。2012 年には国内 SSL サーバ証明書の市場シェア 1 位を獲得し、2019 年第一四半期の速報値ではシェア 50%を越えている。また、現在は IoT 関連の事業も展開しており、証明書に関しては API 経由で IoT 用証明書の高速大量発行サービス等も行っている。

CBPR 認証取得の動機

グローバルサインは、欧州 2 か国を含む世界 10 か所に拠点がある。電子証明書の受注データは一旦日本に送られ、そこから認証設備を持つシンガポールまたはロンドンを介して証明書が発行されるため、サービス上、個人データの越境移転は避けられず、GDPR 対応が必須であった。

当時は、GAPP と言われる一般的なプライバシーポリシーの雛形をベースとしていたが、GDPR 対応が必要となった時点で規程類はすべて GDPR 準拠に変更し、さらに SCC と将来を考えた BCR 承認取得の 2 段階で対応する方針を立てた。組織体制としては、Data Protection WG を組織し、Data Protection Officer（DPO）の下、各拠点の責任者（社長）を Data Protection Manager（DPM）に指名し、DPO への報告はすべて DPM 経由とする体制を取った。これは、GDPR では管理者（グループ CEO）にすべての責任が帰するため、確実に実施される形をとる必要があったためである。

BCR 承認取得上の課題として、期間・費用の問題、さらに EU 当局とのやりとりに備え精度を可能な限り高めておく必要があった。何か効率的な方法がないか検討していたところ、CBPR 取得に向けて各国法制度の一番厳しい要求事項に合わせて対応していくことで、結果として BCR 申請から承認までの期間短縮が望めるという話を聞く機会があり、まずは CBPR 取得を目指すこととした。

実際に CBPR の審査を受けると、自分たちの目とは異なった視点での指摘があり、対策の完成度を認識し、さらに精度を高めることができるという点で意義を感じた。また、CBPR は取得コストも非常にリーズナブルであり、証明書も出してもらえるので、うまく活用した方がよいと考える。

グローバルサインのポリシー管理体制

認証局であるグローバルサインには、元々、認証局専門のポリシー管理体制（Policy Authority）があり、ここが認証局関連ポリシーを管理していた。そこに新規に Data Protection Officer を設置し、プライバシー関連の内規や対外的なプライバシーポリシー、緊急時の対応計画を策定し、それを Policy Authority が作成する関連ポリシーに実装させるという形を取っている。

CBPR 認証のメリット

CBPR 認証のメリットとしては、日本の改正個人情報保護法や北米を含む APEC 域内での法令準拠性を確認できる点が挙げられる。当社が発行する電子証明書の記載内容は、基本的には公開情報であり、そこに含まれる個人情報も公開情報となる。保護が必要な個人情報の大部分はコンタクト情報であり、当社にとっては従業員の個人情報の方が、保持している項目から見ても、また EU 従業員のプライバシーへの意識の点からもシビアに対応する必要があった。

このため従業員の個人情報の取り扱いにつては、GDPR に合わせて同意を適法根拠としない形で整備を進めた。日本の改正保護法でも適法となるよう、個人情報の取り扱いの通知・公表と責任窓口の明示の上、社内教育で周知徹底している。なお社内教育受講の証として、教育内容を理解した旨の表明と、ポリシー遵守誓約の署名を取っている。

国際的に保護法強化の動きがある中で、実際の対応においては、コストパフォーマンス、第三者監査による精度向上、さらに継続的な監査の仕組みによる準拠性確保が重要課題となる。その点で、CBPR は一つの対応策となるという感想を持っている。

その他（EU GDPR 留意点）

最後に、GMO グローバルサインの DPO として活動する中で、特に留意が必要と感じている点をお伝えしたい。

まず、経営トップのサポートに関しては、GDPR38 条、39 条に経営トップの関与が明記されているので、DPO をサポートしないこと自体が GDPR 違反となるということを説明

すれば理解・協力を得ることができる。

また、従業員情報の取り扱いに関しては、安易に同意に依拠することは非常に危険である。同意（＝consent）は個人の自由な意思によるもので、かつ撤回が可能なものと定義されている。会社と従業員は立場が対等ではないので、同意の有効性に疑義が残る。同意ではなく入社時の契約書等で明確にしておくことがベストであるが、雇用契約書に記載がない場合は、雇用契約の遂行に必要な正当な権利行使として、法令に基づく要求項目と合わせて、従業員に通知・公表することをお勧めする。

十分性決定に関して誤解しやすい点としては、決定後であっても GDPR28 条で管理者が処理者に処理を委託する際には法的に相手を拘束することが求められているため、SCC（またはそれに相当する手続き）は必要となることに留意した方がよい。

また GDPR で罰せられるのは、漏洩そのものに対してではなく、GDPR の要求事項に違反している場合なので、準拠していればペナルティという点に関しては恐れる必要はない。ただし、処理者が違反した場合は管理者がその責任を負うことになるので、契約で拘束した上で監督することが重要となる。

当社が対応で感じた点が、各企業の GDPR 対応の参考になれば幸いである。