GDPR における企業・団体の法的責任

亜細亜大学
法学部教授　加藤　隆之氏

EU 一般データ保護規則（以下、GDPR）では、データを漏えいするなどの違反行為をした場合、1.民事責任、2.制裁金（行政が科す責任）、3.刑事責任という 3 つの責任を負う可能性がある。これは日本で交通事故を起こした場合、1.民事責任（損害賠償）、2.刑事責任、3.行政上の責任を負うのと同様である。GDPR については、この 3 本の柱で考えていくと問題点が見えてくる。

■民事責任

GDPR では第 82 条で民事責任の要件を①規則違反行為、②因果関係、③有形的又は無形的損害と定めており、日本の不法行為の要件とあまり変わらない。しかし問題なのは、どういう場面で損害賠償責任を負うのか、という点である。とりわけ、「損害」の概念に財産的損害を伴わない純粋な精神的な損害、例えば、不安や懸念（apprehension）、また、不快感（discomfort）などを含むかが不明確なことが問題だと考えている。この点について日欧どちらでも具体的な考察がなされていないため、どういう場合にデータ保護違反となり民事責任を負うのかについて、その輪郭が明らかになっていない。

また、GDPR 第 33 条、34 条では、「個人データの侵害行為があった場合、監督機関やデータ主体にその事実を通知する義務が存在するが、自然人の権利又は自由に対するリスクが生じそうにない場合にはその義務が免除」されている。つまり、リスクが生じそうな場合に通知しなければ GDPR 違反となるが、ここでいう「リスク」と「損害」の概念との整合性も考える必要がある。

日本では、個人情報保護法違反、プライバシー権侵害があった場合、不法行為による損害賠償請求（民法第 709 条）という法律構成をとるのが一般的である。しかし日本でも、権利侵害があっても損害がなければ損害賠償請求はできず、また、権利侵害と損害は同義ではない。この点について学説に争いはない。すなわち、個人情報保護法違反、データ保護法違反イコール損害賠償請求可ではないのである。ところが、この点について、個人情報保護法関連の研究者は、十分な研究をしているとはいえない状況である。

では民法上の「損害」とはいったい何か。財産上の損害が生じない精神的苦痛なども含まれるのか。早稲田大学講演会事件（最判平成 15・9・12）で最高裁は「秘匿されるべき必要性が必ずしも高いものではないが、自己が欲しない他者にみだりにこれを開示されない

という期待は保護されるべきであり、本件個人情報は、プライバシーにかかる情報として法的保護の対象となる」とし、「本件開示について承諾を求めることは容易であった」ことなどを理由として、プライバシー権の侵害であると判示した（ただし、第 1 審、第 2 審は不法行為の成立を否定し、最高裁も 3 対 2 の僅差での判決であった）。

学生に関するデータが個人情報であることは間違いないが、損害賠償請求を行うには損害が生じていなければならない。当日の警備上の理由から当該講演会に「参加する学生」の情報を警視庁に提供した場合、それにより「参加が妨げられたわけではない学生」が被った損害とはいったい何か。

個人情報を漏えいすることイコール損害発生ではない。現在の議論の中では、日欧ともにデータ保護法違反イコール損害賠償でいいのではないかという雰囲気があるが、その点をきちんと検討する必要がある。たとえば、長崎市内の公立小学校において、通知表の様式及び評定記載方法をめぐる校長会と教師との争いから、一部の学校では通知表が児童に交付されないという出来事が起きた。この時、Y がこの教師たちを批判したビラを配布し、そこに教師らの氏名・年齢・住所・電話番号を記載していたという事件（最判平成元年 12 月 21 日）では、記載されていた教師宅に脅迫電話がかかるなどの被害が生じた。最高裁は当該個人情報の頒布行為によって、私生活の平穏など人格的利益が侵害されたことを理由として、2 万円の損害賠償を認めた。

先の早稲田大学講演会事件では、差戻審で学生 1 人あたり 5,000 円の損害賠償が認められたが、いかなる損害に対して支払われたのか、また額として適切であったのかなど検討を要する課題である。損害の意味を突き詰めなければ、損害額の算定は困難であろう。

大手教育出版企業の顧客情報流出事件では、子、保護者の氏名、住所、電話番号、性別、生年月日に関する情報が流出し、賠償額は 1 世帯あたり 500 円である。流出した個人情報がどのように使われるか不明で、具体的な損害も不明であるが、企業側からみれば約 3,000 万人に対し総額 150 億円の賠償となった。つまり、「損害とは何か？」を明確にしないと、企業は「損害」の意味がわからないまま莫大な負担を強いられる可能性がある。

■制裁金（行政上の制裁）

制裁金を公的団体に科したとしても、その金銭の出所は結局のところ税金であり、その実効性に乏しいという批判があるため、GDPR では、制裁金対象団体は民間団体と定めている。

制裁金を科すか否かの決定に際しては、第 83 条 2 項で考慮すべき事項を広範に定めているが、制裁金対象の違反行為が広汎すぎる。GDPR における制裁金の 3 大特徴は、広汎性、曖昧性、高額性といえる。制裁金対象の違反行為は、極めて多岐にわたる（広汎性）。

また、制裁金対象行為の規定についてであるが、曖昧な部分が残されていることも多い（曖昧性）。たとえば、第 31 条の監督機関との協力に応じない、懈怠すると制裁金の対象であるが、その内容は曖昧である。第 17 条の「忘れられる権利」の削除義務がいかなる場

合に生じるか、その判断は困難なこともあろう。だが、これらの義務に違反した場合、2,000万ユーロ又は全世界年間売上高 4 パーセント以下の制裁金が科される可能性が生じる。なお、忘れられる権利のケースでは、削除を求めた者からの要請に誤って応じた場合、情報元から民事上の不法行為責任を追及される可能性もある。

さらに、列挙された違反行為に対して、常に制裁金が科されるわけではないとしても、制裁金額が高額であるため、企業にとっては脅威である（高額性）。たとえば 2016 年のグーグルの年間売上高（予想）は、8 兆円規模なので、そのうちの 4%となると最高 200 億円までの制裁金を科すことも可能となる。さらに、損害賠償責任と刑事責任すら追加される可能性もあり、他の権利とのバランスが懸念される。

ところで、第 83 条 9 項では、制裁金を科す制度を採用していない場合、他の制度で代替することを認めている。たとえばアイルランドでは、制裁金をデータ保護コミッショナーが科すことについて、憲法上の制約があり、現在でもコミッショナーは制裁金を科す権限はない。実は GDPR にはこうした例外規定が多数存在しているが、この点に関する情報提供が乏しい。また、これで本当に EU 全体で実効性を持つことができるのか、疑問が残るところである。

制裁金を科す際の考慮事項

制裁金は、監督機関の是正措置と共に科すことも可能であるが、次の事項を考慮して制裁金を科すか否かについて決定しなければならない（2 項）。

(a) 当該取扱いの性質及び目的並びに影響を受けたデータ主体の数及びデータ主体の受けた損害の程度を勘案した当該違反行為の性質、重大性及び期間。
(b) 当該違反行為の故意又は過失の特徴。
(c) データ主体の受ける損害を軽減させるために当該管理者及び取扱者がとった行動。
(d) 第 25 条及び第 32 条に従って管理者及び取扱者が実施した技術的及び組織的対策を勘案した当該管理者及び取扱者の責任の程度。
(e) 当該管理者又は取扱者による関連する以前の違反行為。
(f) 当該違反行為の是正及び違反により生じ得る悪影響軽減のためになす監督機関との協力の程度。
(g) 当該違反行為によって影響を受ける個人データの種類。
(h) 当該違反行為が監督機関へ知らされた方法。特に管理者又は取扱者が当該違反行為を通知したか否か、もし通知したのならその範囲。
(i) 同じ事項に関して、当該管理者又は取扱者に対して事前に第 58 条第 2 項で定められた措置が命じられていた場合、それら措置の遵守。
(j) 第 40 条によって承認された行動規範又は第 42 条による承認された認証メカニズムの遵守。
(k) 当該違反行為から直接又は間接を問わず得られた財政上の利益又は避けられた損失のように、当該事案の状況に該当する悪化又は軽減要素。

制裁金対象の違反行為

（a）1,000 万ユーロ又は全世界年間売上高 2 パーセント以下の制裁金（4 項）
①管理者及び取扱者による次の条文の義務違反行為
・8 条　情報社会サービスに関する子どもの同意に対して適用される条件
（Conditions applicable to child's consent in relation to information society services）
・11 条　識別を要求しない取扱い（Processing which does not require identification）
・25 条　データ保護・バイ・デザイン及びバイ・デフォルト
（Data protection by design and by default）
・26 条　共同管理者（Joint controllers）
・27 条　EU 域内に拠点のない管理者又は取扱者の代理人
（Representatives of controllers or processors not established in the Union）
・28 条　取扱者（Processor）
・29 条　管理者又は取扱者の権限下における取扱い
（Processing under the authority of the controller or processor）
・30 条　取扱い活動の記録（Records of processing activities）
・31 条　監督機関との協力（Cooperation with the supervisory authority）
・32 条　取扱いのセキュリティ（Security of processing）
・33 条　個人データ侵害の監督機関への通知
（Notification of a personal data breach to the supervisory authority）
・34 条　データ主体への個人データ侵害の通知
（Communication of a personal data breach to the data subject）
・35 条　データ保護影響評価（Data protection impact assessment）
・36 条　事前協議（Prior consultation）
・37 条　データ保護職の指名（Designation of the data protection officer）
・38 条　データ保護職の地位（Position of the data protection officer）
・39 条　データ保護職の職務（Tasks of the data protection officer）
・42 条　認証（Certification）
・43 条　認証機関（Certification bodies）

②認証機関による次の条文の義務違反行為
・42 条　認証（Certification）
・43 条　認証機関（Certification bodies）

③監視団体による次の条文の義務違反行為
・41 条 4 項　承認された行動規範違反に対する監視団体の適切な措置
（41 条、Monitoring of approved codes of conduct）

（b）2,000 万ユーロ又は全世界年間売上高 4 パーセント以下の制裁金（5、6 項）
次の条文の違反行為
・5、6、7、9 条における、同意の条件を含む基本的取扱い原則
・12～22 条におけるデータ主体の権利
・44～49 条に従った第三国又は国際機関の取得者への個人データ移転
・9 章に基づき採択された加盟国の国内法の義務
・取扱いに関する 58 条 2 項による監督機関の命令の不遵守、又は 58 条 1 項に違反してアクセスの提供を履行しないこと

■刑事責任

GDPR 第 84 条では、第 83 条による制裁金を欠く場合には罰則が必要と規定している。しかし、上記の通り制裁金に関する条文は多岐にわたっており、それ以外の場合とは何を指すのかが不明である。これほど巨額な制裁金を科すにも関わらず、刑事責任については各国裁量というのはバランスが取れていないようにも思われる。

■まとめ

① 民事責任については、損害概念のとらえ方いかんでは、責任を負うべき範囲が、非常に広汎になる可能性がある。
② 制裁金については、対象行為が広汎に過ぎることに加え、高額に過ぎる。
③ 刑事罰については国家間で一貫性がない。

これにより、EU 域内に拠点を持ち、EEA 域外に EU 市民の個人データを移転するなど GDPR の適用を受ける企業は、何をしたらどういう罰則が科されるのか予見しづらく、過剰な対策をせざるを得ない傾向にあるのではないだろうか。確かに、高額な制裁金を科される可能性がゼロではないが、これだけ高額な制裁金を科すに際しては、十分な事前説明や反証の機会等のプロセスを経ることも想定されることである。

一番考えなくてはならないのは、プライバシー権と個人情報保護との関係を明確にし、なぜプライバシー権が重要で、最も保護される領域は何かについての原理的考察を行うことだと考える。たとえば英米の判例法は、パッチワークでプライバシー権を十分に保障しないといわれているが、そこに意味はまったくないのか。今一度、何が我々の権利で一番保護されなければならないものかという点から考える必要があるのではないか。

個人情報保護についても、基礎理論の研究がなされないままに保護に対してのみ対応に追われ、いかなる個人情報保護違反行為に対し、民事制裁、刑事制裁、行政上の制裁金制裁が妥当なのかを決する「価値基準」を育む機会が持たれなかったのではないだろうか。

欧州に学ぶことは多いが、わが国自身の足元も見つめ、企業活動や社会全体にプラスになるかという視点も持ったうえで議論する必要を感じている。たとえば、今回のわが国の個人情報保護法の改正では保有個人情報が 5,000 件以上を対象とするという要件が撤廃されたが、これは EU による十分性審査を念頭に置いたものであっただろう。ところが、GDPR は逆に小・中規模事業者には別に配慮すると規定をいれているところがある。EU に若干振り回されすぎてしまったという印象を受けている。