

EUおよび英国における情報保護法の重要性

ロンドン・センター

本レポートは、2003年10月21日にジェトロ・ロンドンが主催した法務・労務セミナーにおいて、クリフォード・チャンス法律事務所が、情報保護法について講演した要旨を取りまとめたものである。

1. はじめに

英国および欧州諸国における情報保護法は、非常に複雑で、遵守するためにコストがかかるという指摘がある。しかし、現実には一般的評価より良い面と悪い面がある。個人情報保護に関連するいくつかの問題は、伝統的にやや誇張されてきた。反対に、人々は個人情報保護問題に直面した場合、視野の狭いとらえ方をする傾向があり、結果として、ある状況においては、情報保護法と同様に重要ないくつかの関連規則を無視することがある。本レポートでは、個人情報保護の基礎をなす法律自体の遵守について助言するとともに、ありがちな誤解や問題を明らかにすることを目的とする。

2. 情報利用を規制する法律

情報はいくつもの異なる形式をとるので、個人情報保護や情報利用に対する規制については、多数の異なる法律に定められている。これらの法律とは、例えば、個人情報の利用を規制する情報保護法、信任義務から生じる義務、人権法（一般的に個人のプライバシーを行政機関から保護する法律）、個人情報保持に関する契約上の制限、マーケティングやモニタリングに関連する分野ごとに特定の規則、知的所有権から派生する制限などである。従って、数多くの異なる規則がある程度重複して存在し、情報の利用を制限するということである。

しかし、これらの多様な法律の存在は、解釈・運用の面で伝統的に混乱を招いてきた。例えば、データベースにおける知的所有権（データベースの複写を防ぐために利用できる）と情報保護法上の権利（個人情報(personal data)の利用を制限する）を混乱して考えることがよくある。個人情報保護に関連する問題を取り扱う上では、関連する法律の範囲を正確に把握することが重要である。

3 . 情報保護法と関連法律

欧州の情報保護法の基礎となるものは、個人情報利用を規制するいくつかの EU 情報保護指令である。主要な EU 情報保護指令は、最近ではアイルランドで実施され、現在では、ほとんどの EU 諸国で国内法化されている。唯一、同指令の国内法化をいまだ完了していない国はフランスである。また、EU 域外においても、同様の法律が存在する。例えば、米国においては、金融サービスとプライバシーに関連する法律が存在する。

英国においては、主要な情報保護法に加えて、例えば、通信の監視制限やマーケティングの目的での電子通信システムの利用について分野ごとに特定の関連法律が存在する。この分野の法律のほかに、英国におけるインフォメーション・コミッショナー (the Information Commissioner) のような国内規制機関や、第 29 条特別調査委員会 (情報保護問題について欧州委員会に助言する EU 規制機関のグループ、95 年の情報保護指令 <Directive 95/46/EC> 第 29 条に基づいて設立) により発行された数多くの規制ガイダンスが存在する。従って、情報保護に関する問題を検討する場合には、主要な法律だけではなく、関連する規則やガイダンスについても目を向けることが重要である。

4 . 情報保護法が要求するもの

情報保護法は、個人に関する情報の利用という、大変広範囲でつかみどころのない問題について規制することを意図するので、非常に漠然とした文言で表現されている。同法は、遵守しなくてはならないいくつかの情報保護原則 (principles) を明らかにする。これらの原則により、以下のような要件が課せられる。

- ・ 通知： 誰がその者の情報を保持しているかについて、その個人に対して通知する義務がある (詳細は「5 . 通知」を参照)。
- ・ 公正な情報処理： すべての状況に鑑みて、情報の利用は一般的に「公正 (fair)」であることを確保する要件が存在する。情報処理が公正であることを証明するためには、例えば、関連する個人の同意を取得するなど、いくつかの条件のひとつを満足させる必要がある (詳細は「6 . 公正な情報処理」を参照)。
- ・ センシティブな情報： 「センシティブ (sensitive)」と定義される情報については、特に注意を要する。センシティブな個人情報とは、例えば、個人の健康、人種、宗教、政治的意見、前科の詳細、労働組合構成員であるかどうかに関するものである。
- ・ 正確性、比例性、情報の保持： 一般的に、情報の質の問題に関連する多くの原則が

Report 6.

存在する。これらの義務は非常に一般的な性質のもので、伝統的にこの点に関する義務に従業員に通知するという、一般的な情報保護原則により取り扱われてきた。例えば、情報の収集と利用は、個人がその詳細を提供した際の期待に比例し、また、その期待を反映するものでなくてはならない。

- ・ 登録： 関連する情報の利用について、情報保護規制機関であるインフォメーション・コミッショナーに通知する義務が存在する。英国では、この義務は形式的なものだが、フランスなどでは問題となる場合がある。
- ・ 安全管理： いかなる情報処理に関しても適切な安全管理対策を確保する一般的な義務が存在する。この義務は情報処理を外部委託する場合にも考慮する必要がある。
- ・ 情報の国際移転に対する制限： 欧州経済領域（E E A , E U 15 カ国 + ノルウェー、アイスランド、リヒテンシュタイン）外への個人情報の移転については、数多くの複雑な制限が存在する（詳細は「13. 情報の国際移転」を参照）。

5 . 通知

個人情報処理する会社は、個人（「データ・サブジェクト(data subjects)」と呼ばれる）に対して、その者の情報が処理されているということを知らせる義務がある。特に、「データ・コントローラー(data controller)」である会社は、個人に対して、その身元、情報処理の目的（例えば、サービスの提供やマーケティングのため）、その他関連する情報（例えば、情報の受取人である第三者や情報の国際移転）について通知しなければならない。

この通知義務の実施には、いくつもの実際上の困難が伴う。例えば、会社が個人情報を取得しても、その個人に対して正式な通知をだすことが不可能な場合が数多くある。そのような場合には、会社は、関連する情報の利用は自明であり、従って明示的な通知を出す必要はないという見解をとるであろう。

6 . 公正な情報処理

いかなる情報の利用も「公正(fair)」でなくてはならない。公正な情報の利用を確保するひとつの方法は、個人の同意を取得することである。そのような同意は、すべての場合に明示的なものである必要はない（例えば、行動により暗示されることもできる）が、そのような同意が有効であるためには、合理的にみて明らかであり、「自由な意思に基づき、特定のものであり、かつ情報に基づく（freely given, specific and informed）」同意でなくてはならない。

Report 6.

同意が得られない場合、会社は、情報保護法（および情報保護指令）に規定される別の条件である、「利益のバランスの条件(balance of interest condition)」に依拠することを望むかもしれない。これは、情報処理が雇用者の正当な利益であり、かつ、関連する個人を不当に侵害するものではない場合に、会社が情報を処理することを許可するものである。しかし、例えば、従業員に関する情報の利用や開示が、その個人を不当に不利な立場に追い込まなかったと証明することが特定の状況においては困難であるかもしれないという問題点がある。

従って、雇用関係において、会社は情報の利用が公正であることを示すその他の方法を採用するかもしれない。例えば、新しい従業員からは同意を取得（新しい従業員に関しては比較的容易である）し、他の場合には「利益のバランスの条件」に依拠するというものである。

ただし、情報が「センシティブな個人情報(sensitive personal data)」と定義される場合、「利益のバランスの条件」に依拠することはできず、すべての同意は「明示的な(explicit)」ものでなくてはならない。従って、実務上、雇用者はセンシティブな個人情報の収集は最低限にとどめるべきで、従業員もこれを明確に理解していることが重要である。

7 . 情報保護が問題となる典型的な例

情報保護が問題となる典型的な例は以下のような場合である。

- ・ 雇用関係において将来の、既存の、あるいは退職した従業員の情報が保持される場合
- ・ マーケティングの目的で顧客のデータベースが保持される場合
- ・ 電子メールなどの通信履歴の保管および記録
- ・ ビジネス上の通信の監視。特に従業員による電子メールの利用の監視
- ・ 情報の国際移転。特にグループ企業内での移転およびサービス提供者である第三者への移転

8 . 雇用関係

従業員に対して、彼らの情報がどのように処理されたかを通知することが重要である。通常、雇用契約、応募書類および情報保護原則を記す書類にて通知することになる。また、すべての場合において、従業員の情報の利用は公正なものでなくてはならない。公正さを確保するひとつの方法は、従業員の同意を取得することである。

しかし、既存の従業員から同意を取得することは困難である。なぜなら、手続き上の煩雑

Report 6.

さに加えて、何らかの理由で同意を拒否する従業員がいるかもしれないからである。さらに、従業員に同意を拒否するという現実的な選択の余地がない場合に、そのような同意の有効性に疑いが生じるであろう。このため、多くの会社は情報保護に関する同意を新しい従業員に対しては要求するが、既存の従業員に対しては要求しない。ただし、特にセンシティブな情報（例えば個人の健康に関する情報）を収集する場合はこの限りではない。

注意しなくてはならない点は、従業員の情報の利用に関して問題となるのは情報保護法だけではないということである。特に、雇用者は、従業員の情報の利用はより大きな雇用法の問題を生じさせるかもしれないということを確認する必要がある。例えば、雇用者と従業員との間の信頼と守秘義務が雇用契約の中に暗示的に含まれる。さらに、明示的な守秘義務が従業員に約束されたかもしれないし、人権問題も生じる。英国の人権法(the Human Rights Act)の下では、個人は、「個人および家庭生活を尊重する権利(right to respect for private and family life)」を有する。これは、例えば雇用者が従業員の行動を監視しようとする場合、問題となるかもしれない。

9 . マーケティング

企業は、個人に対してダイレクト・メールを送付する場合、それらの個人から同意を取得することが情報保護法の下で要求されるかどうかについて厳格であるとはいえない。いかなるダイレクト・メールの送付にも同意が必要であるというのは、よくある誤解である。

実際には、通常、情報保護法の下では、マーケティングのために個人の情報を利用する意図があるということに関連する個人に通知する必要があるが、マーケティングのために個人の事前の同意は必要としない。一般的に、ダイレクト・マーケティングに關与する多くの会社は、個人に対して「オプト・アウト(opt out)」することを提供する。情報保護法の下では、宣伝資料を受け取ることを拒否する絶対的な権利が存在する。従って、郵便による個人対象のマーケティングや、企業顧客や既存の顧客に対するマーケティングに関して事前の同意を取得しなければならないという一般的な要件は存在しない。

しかし、新しい電子マーケティング規則によれば、電子メールやテキスト・メッセージなどの電子的な方法により、ビジネスの既存の顧客ではない個人に対してマーケティングを行う場合、事前の同意を必要とする。従って、このような種類のマーケティングを予定している場合、あらかじめ明確な（「オプト・イン(opt in)」するという）同意を取得することが重要である。電子マーケティングに関する新しい英国の規則は、2003年12月11日に施行された。同様の規則が他の欧州諸国でも適用され、プライバシーと電子通信に関するEU指令を実施する。

10 . 電子マーケティング

EU 電子通信情報保護指令(the Electronic Communications Data Protection Directive)は、会社に対するダイレクト・マーケティングを規制する規則については正確に規定していない。同指令は、自然人以外の申込者(つまり、会社)の正当な利益は十分に保護されなくてはならないと述べるにとどまる。英国においては、現在の法案はこの問題についてはふれていない。その結果、この問題は、英国のインフォメーション・コミッショナーなどの管轄規制機関によるガイダンスの対象となるであろう。

マーケティングに関する上記の解説は、すべて情報保護問題に関連するものである。しかし、電子商取引や遠距離販売および通信の監視に関する規則など、適用される法律の下にその他の通知や同意の要件が存在するかもしれないということを覚えておく必要がある。例えば、英国の電子商取引規則は、すべてのダイレクト・マーケティングが、ダイレクト・マーケティングであるということを明確に示すことを要求し、遠距離販売に関する規則は、契約成立の詳細、契約取消手続きおよび価格について、個人に明らかにすることを要求する。また、様々な広告基準や同様の要件が存在する。従って、情報保護規則を孤立して考えてはならない。

また最近では、欧州第 29 条特別調査委員会が、欧州ダイレクト・マーケティング連盟(FEDMA : Federation of European Direct Marketing Associations)によるダイレクト・マーケティングに関する実施規範を承認したことも覚えておく必要がある。従って、ダイレクト・マーケティング活動を開始する以前に、同規範を検討する必要がある。

11 . 情報の保持

情報保護法の下では、個人情報に「必要以上に長い期間保存してはならない(must not be kept for longer than necessary)」。しかし、この義務は非常に曖昧に表現されているので理解することが困難である。個人情報をどの位の期間保持することが「必要(necessary)」であろうか。その答えは、実際には情報保護法ではなく、様々な目的で情報が保持されることを要求するその他の多様な規則による。例えば、雇用法、税法、契約法あるいは金融規制法により書面を一定期間保持する義務が存在する。それは、例えば投資者に与えられた助言を証明するためである。また、将来、訴訟に利用するという商業的な理由で情報の保持を望むかもしれない。情報保持に関するすべての問題は非常に複雑であり、情報保護義務はこの点に照らして検討する必要がある。

Report 6.

従って、書面および情報の保持に関する問題の取り組み方としては、まず関連する書面と情報およびそれらの情報の保持を要求する法的義務を明らかにすることである。そのあとで初めて、個人情報が必要以上に長い期間保持されないよう確保し、そのために適切な記録保持および削除に関する原則を実施するという、情報保護の観点から取り組むべきである。

1 2 . 通信の監視 - 情報保護法との関連

通信の監視は、その過程で会社が特定の個人の情報を収集することになるので、情報保護上の問題が生じる。通信の監視を必要とする申し分なく正当な理由が存在する。例えば、ITシステムが適切に機能していることを確認するため、会社の原則や手続きの遵守を確保するため、詐欺を予防あるいは発見するため、一般的に規則の遵守のためなどである。一方で、情報保護法はそのような監視が度を越えたものではないことを要求し、雇用法や人権法の下に個人はプライバシーや守秘義務の権利を有するであろう。従って、法は会社が監視を行うことを禁止しないが、監視が目的に比例し、注意深く、そして組織立った方法で行われることを要求する。

一般的に、監視は合理的であれば許可される。監視が行われるかもしれないということを従業員に通知することが重要である。また、監視を行う者にはこの分野における権利義務について理解し、その義務の範囲を超えて他人の通信を不適切な方法で監視する場合には、リスク（潜在的に個人的な刑事罰を含む）に直面するということを理解させることが重要である。

また、国により監視に関する規則が異なることにも注意する必要がある。例えば、英国では、監視が行われるかもしれないということを通知するだけでよい。しかし、フランスでは、一般的に、個人の同意が裁判所の命令がなければ個人的な通信を監視することはできない。イタリアやドイツでは、監視活動を開始する以前に、地域の労使協議会の許可を取得することが必要かもしれない。

1 3 . 情報の国際移転

情報保護法で特に懸念されるひとつの分野は、情報の国際移転に関する制限の問題である。EUの情報保護法は個人情報の欧州経済領域（E E A）外への移転を制限するが、一定の条件を満足すれば情報移転は許可される。例えば、個人の同意がある場合や、移転された情報を保護する「適切な保護措置(adequate safeguards)」を準備する場合などである。これ

Report 6.

らの「適切な保護措置」の例としては、EU により承認された「標準契約条項(Model Contract Terms)」が挙げられる。さらに、国際商業会議所のような様々な機関がその他の条項を提案している。しかし、これらは規制機関により正式に承認されていない。

米国と EU は、米国への情報移転のための「セーフ・ハーバー条項(safe harbour)」について同意したが、これにはいくつかの欠陥があり、理想的な解決方法とは言えない。

また、2003 年初めに、第 29 条特別調査委員会は、原則として「国際移転のための拘束力のある企業規則(binding corporate rules for international transfers)」の使用を承認する書面を発行した。これにより、会社が国際的に移転された情報が適切に保護されることを確保する企業グループ内の原則を準備することが予想される。ただし、これらの原則により、個人が関連するグループ会社に対して行使できる法的権利を与えられることが条件となる。言い換えれば、そのような原則には法的実効力がなくてはならない。

上記に加え、スイス、ハンガリー、ガーンジー諸島およびアルゼンチンなどの国・地域が「適切な保護措置」を提供すると正式に認められた。これは、かなり任意的なリストである。日本には情報保護法が存在するが、EU により「適切な保護措置」を提供するとは正式に認められておらず、EU の官僚的な煩雑な手続きを考えるとそのような承認が得られるまでには相当の期間を要するであろう。

従って、情報の国際移転の問題に取り組む場合、会社は同意が得られない場合に、「適切な保護措置」を確保することのできる方策を明らかにするべきである。特定の状況に適用されるその他の限られた条件も存在する。例えば、訴訟に関連して法的権利を保護するために情報移転が必要な場合などである。しかし、これらの条件が適用される場合は非常に少ない。

14 . 結論

上述のように、情報保護法遵守に取り組むためには、会社はまずそのビジネスフローの中で情報がどのように収集され、利用され、あるいは開示されるかについて考察しなくてはならない。関連する情報が特定の個人についての「個人情報(personal data)」である限りにおいて、情報保護法の問題が生じるかもしれない。

しかし、情報の利用を制限する雇用法、金融サービス規則、税法、守秘義務、契約義務などから生じるその他の影響も考察する必要がある。情報保護法は重要であるが、特定の事例において適用される唯一の法律ではないかもしれない。従って、情報保護法遵守については「全体論的な(holistic)」取り組みを採用し、すべての義務について同時に検討することが重要である。