英国情報保護法の最新動向と IT 問題

（2014 年 9 月）

独立行政法人　日本貿易振興機構（ジェトロ）

ロンドン事務所

進出企業支援・知的財産部 進出企業支援課

本報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）ロンドン事務所がリテイン契約に基づき、現地のフィリップ・ロス法律事務所に作成委託し、2014年9月に入手した情報に基づくものであり、その後の法律改正などによって変わる場合があります。掲載した情報・コメントは作成委託先の判断によるものですが、一般的な情報・解釈がこのとおりであることを保証するものではありません。また、本稿はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本稿にてご提供する情報に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求め下さい。

ジェトロおよびフィリップ・ロス法律事務所は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的損害および利益の喪失については、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたか否かにかかわらず、一切の責任を負いません。これは、たとえジェトロおよびフィリップ・ロス法律事務所がかかる損害の可能性を知らされていても同様とします。

本報告書にかかる問い合わせ先：
独立行政法人　日本貿易振興機構（ジェトロ）

進出企業支援・知的財産部

進出企業支援課

E-mail：OBA@jetro.go.jp

ジェトロ・ロンドン事務所
E-mail：LDN@jetro.go.jp

JETRO

本報告書作成委託先：
フィリップ・ロス法律事務所

Koichiro Nakada
Partner & Head of Japan Business Group
Philip Ross Solicitors
koichiro.nakada@philipross.com
Tel: 07855 720 643

Yoko Nakada
Solicitor & Associate, Japan Business Group
Philip Ross Solicitors
yoko.nakada@philipross.com
Tel: 020 7596 8587
M:　07585 624 539

目次

英国情報保護法の最新動向と IT 問題

第１章　データ保護

1.はじめに

データ保護立法は、企業が個人から収集・保有・処理する個人情報に関して何をしてよいのか、また、何をしてはならないのかという点を特に規定している。

2.重要な立法

英国では、1998 年データ保護法（The Data Protection Act 1998）（以下、「1998 法」という。）により、データ保護に関する法が施行されている。

欧州連合における関連法令は指令 95/46/EC（以下、「データ保護指令」という。）に定められている。欧州連合の法令は常に見直され、EU 理事会による最新の布告はつい先日の 2014 年 6 月 9 日に発表された。この点は後述する。

データ保護立法の目的は、個人の基本的な権利と自由、特に個人情報の取扱いに関するプライバシーの権利を保護すると共に、欧州連合内における個人情報の自由な流れを容易にすることである。

この報告では英国における規制の運用に焦点を当てる。

この報告においては、イングランドおよびウェールズの法を英国法として説明する。スコットランドと北アイルランドでは立法について異なる取り決めがあるので別の規則が適用されることがあるが、一般的に言えば EU の立法に従っている。

1998 年法は、コンピュータ化されたデータだけでなく、手作業によるデータについてもデータ保護管理の枠組みを設立した。具体的には、個人情報がデータ保護原則に従って利用されるように確保し、個人情報の取扱いに一定の条件を付け、個人情報が要注意（sensitive ）と思われる場合に追加の保護措置を付加し、データ主体の権利を確立し、通知と強制手段の枠組みを確立した。

留意すべき点は、データ保護指令は最低限の基準を定めるものであり、従って、データの提供者（以下、「データ主体」（”data subjects”）という。）の権利、および、情報を管理する者（以下、「データ管理者」（”data controllers”）という。）に関する義務は、国ごとに異なるという点である。

3.「データ」の意味と関連表現

「データ」とは、以下のような情報を意味する。

(i)　ある目的のために与えられた指示に応じ、自動的に作動する装置によって取り扱われる情報；
(ii)　かかる装置によって取り扱う意図をもって記録された情報；
(iii)　関係資料整理システム（a relevant filing system）の一部として、または、関係資料整理システムの一部を構成する意図をもって記録された情報；

(iv) 上記のいずれでもないが、閲覧可能な記録の一部を構成する情報（例えば健康記録や教育記録）。

「データ管理者」（“Data Controller”）とは、単独またはほかの者と共同で、データを取り扱う目的および方法を決定する者（会社を含む）を意味する。

「個人情報」（“Personal Data”）とは、以下により識別できる生存する個人に関する情報である：

(i) 当該情報

(ii) 当該情報、および、データ管理者が所有し、または、所有する可能性があるその他の情報であって、当該個人についての意見の表明もしくは当該個人に関する当該データ管理者その他の者の意図の表示を含む情報

「データ取扱者」（“Data Processor”）とは、個人情報に関して、データ管理者に代わってデータを取り扱う者（データ管理者の社員を除く。）を意味する。

4.登録とデータ管理者

一部の小さな例外を除き、個人情報を保有し取り扱うすべての企業は、データ保護のために情報コミッショナー(the Information Commissioner)に登録する必要がある。この要件は、社員、顧客、納入業者などについてデータを保有しているほとんどすべての企業に適用される。手続きは比較的簡単で、取得され取り扱われる予定のデータの種類とかかるデータの利用目的の完全な詳細について書式に記入する。現在、費用が年 35 ポンドで、登録は毎年更新しなければならない。ほとんどの場合、更新は自動更新にする（例えば、更新料を支払うために年間自動引落を依頼している場合）か、または、情報コミッショナー事務局から毎年更新通知を送ってもらうことができる。

ほとんどの場合は、登録の更新は料金の支払い以外何もしなくても処理される。しかし、企業がデータを保有する目的を変更していた場合、または、現在の登録の範囲がなんらかの理由で変更され、もしくは、不正確であった場合、違反があったとされ、情報コミッショナーはそれを訴追することができる。

データ管理者に関する登録が情報コミッショナーの保管する登録簿に記載されない限り、個人情報を取り扱ってはならない。

しかし、個人情報が電子装置によって取り扱われることもなく、かかる取り扱いを行う意図を持って記録されることもない場合、この要件は適用されない。従って、単に会合で名刺を集めても、それはデータ取扱いには当たらない。しかし、名刺を集めた後、データベースまたはファイルに個人の詳細を記入することは、データ取扱の定義に該当し、従って、1998 年法の適用を受ける。

登録する必要のある組織が登録を怠った場合、刑事上の違法行為になる。訴追は治安判事裁判所に提起され、その結果、最高 5000 ポンドの罰金および担当役員に対する刑事責任が科されることがある。登録を怠った法律事務所が訴追され有罪判決が下された例も多々ある。

情報コミッショナー対 Feld Mackay and Donner 法律事務所事件

- Feld Mackay and Donner 法律事務所の上席パートナーは罰金 3150 ポンド、および登録懈怠の訴追費用として 3500 ポンドの支払いを命じられた
- 情報コミッショナー は次のように述べた。「*治安判事裁判所が届出懈怠の重大性を認識したことは喜ばしい。データ保護法の順守により、個々人の個人情報が安全、正確、最新であり公正に扱われることを保障することになる*」。
- 訴追は増加傾向にある

情報コミッショナー事務局から得られる明白な徴候によれば、かかる登録懈怠に対する訴追は今後も継続されることを示している。

5.データ保護原則（Data Protection Principles）

データの作成とデータ管理

1998 年法は、データ管理者が順守しなければならない 8 つのデータ保護原則を定めている。要約すれば、データ管理者は、データについて以下のことを確保しなければならない。

1. 公正かつ適法に取り扱われていること
2. 限定された目的のために取り扱われていること
3. 適切で、関連性があり、過剰でないこと
4. 正確であること
5. 必要以上に長く保管されないこと
6. データ主体の権利に合わせて取り扱われること
7. 安全であること
8. 欧州経済領域（European Economic Area）（すなわち、25 の EU 諸国およびアイスランド、リヒテンシュタイン、ノルウェー）以外の国であって、適切な保護の方策のない国には転送されないこと

6.インターネットに関する留意点

インターネットの普及とそれが現在のビジネス経営に与えた影響には、企業のデータ保護責任に問題を発生させるおそれがあった。その結果、今では多くの企業がプライバシーに関する正式な指針を作成している。かかる指針は、多くの場合企業のウェブサイトに表示されるが、その目的は、サイト上で集められる情報の種類、その情報の利用方法、個人がこのデータにアクセスする方法、および、そのデータを削除させるための手順に関して正式な説明を行うことである。プライバシーに関する説明には、ウェブ利用者の情報を守るために導入されているシステムに関する情報も記載されるのが通常である。現在、インターネットの内容は英国政府の規制を受けていないが、様々な自主的な行為規範が情報サービス提供業者(Internet Service Provider）により適用されている。

(a) データ収集とデータ保護通知

データ管理者は、データの取扱いが公正かつ適法であるように、データの取扱いに関して、データ主体に対して、例えば、出版やウエブ上での公開など一定の情報を表示して閲覧できるようにする必要がある。要求される情報は以下の通りである。

(i) データ管理者の身元
(ii) データ管理者が 1998 年法に関して代理人を指名している場合、その代理人の身元。
(iii)データを取り扱う目的
(iv) データ主体に関する取扱いを公正にするために必要となるその他の情報

これらの情報は、「データ保護通知」（a “Data Protection Notice”）と呼ばれ、データが取得される時、あるいは、それ以前にデータ主体に提示されなければならない。通知の目的は、データ主体が自分のデータの取扱いに同意する前に、情報に基づいた判断を下せるようにすることである。ウェブサイトを経由して会社に個人情報を提供する個人の場合、データ主体は、既存の顧客、情報を求める将来の顧客、ウェブサイトから商品を購入する人、および、ウェブサイト経由で競争入札に参加する人である。

データ管理者がデータ主体の同意に基づきデータを取り扱おうとする場合、上記の情報が同意のときにデータ主体に提供されていなければ、その同意は有効ではない。

データ保護通知は、申込書やデータ主体のサイン欄の横に表示するべきである。データ主体が権利を知らされた上で同意が適切に行えるように、通知が目立つように表示されていることが重要である。明確かつ正確な通知を表示しない場合、個人情報の取扱いが不公正、および/または違法とされることがある。
データ保護通知はしばしばプライバシーに関する指針の中に記載される。指針では個人情報の取得や利用に関する多くの事項（以下で詳しく扱う。）が扱われる。

(b) データ入力ページ

データが一定の方法で利用されることを拒否する選択権（オプトアウト（”opt out”））をデータ主体に与えるためにしばしば使われる一つの方法は、申込書に「 オプトアウト」のチェックボックスを置く方法である。一例としては、以下のようなチェックボックスの形をとり、データ主体が情報を受け取ることを望まない場合にはチェックマークを入れるというものである。

「□　弊社その他の優良企業の、興味をお持ちと思われる商品に関する詳細情報を受け取りたくない場合には、□に✓を記入して下さい。」

英国以外の一部の EU 諸国では、データ利用に関して「オプトイン（“opt in”）」による具体的な同意を要求している。 しかしながら、英国における情報コミッショナーの見解では「オプトイン」による同意（下例参照）が必要条件というわけではない。ただし、将来、ＥＵ委員会あるいは欧州裁判所が、「オプトアウト」方式を使って得たデータの取扱いは不公正かつ違法であるとの見解を取る可能性もあることに注意すべきである。多くの企業は、「オプトアウト」のほうが「オプトイン」方式より情報を取得できる機会が大きいとの理由から、「オプトアウト」方式を引き続き使用している。

「オプトイン」は次のような書式をとることがある。

「□　弊社商品の詳細を郵送で受け取りたい場合は□に✓を記入して下さい

□　弊社商品の詳細をＥメールで受け取りたい場合は□に✓を記入して下さい

□　関連商品またはサービスについて弊社以外の優良企業から郵送で情報を受け取りたい場合は□に✓を記入して下さい

□　関連商品またはサービスについて弊社以外の優良企業からＥメールで受け取りたい場合は□に✓を記入して下さい」

(c) プライバシーに関する指針

データ主体は、必ずプライバシーに関する指針の存在を知らせる必要がある。プライバシーに関する指針は、データを要求する前の段階で、指針を表示しているページにテキストやハイパーリンクを用いて利用者が常に簡単にアクセスできるようにしなければならない。リンクは間接的でもよいが、プライバシーに関する指針は明確に説明され、かつ、簡単にアクセスできるリンクでなければならない。

プライバシーに関する指針が読まれたこと、および、データ主体がデータを送付したときに指針に合意したことを確認する証拠として「チェックボックス（a “tick box”）」を表示するのが、多くの企業にとっては良い方法である。

一般的な基準として、プライバシーに関する指針には最低限 1998 年法に基づきデータ管理者が提供すべき情報がすべて提供されていなければならない。例えば、マーケティング活動や第三者への情報開示、海外への情報転送や「cookies(クッキー)」の使用に関する情報である。　ウェブサイトがクッキーのような、非表示のトラッキング装置を使っている場合には、プライバシーに関する指針はクッキーに関する章を設け、そこで、クッキーとは何か、なぜこのサイトはクッキーを利用しているのか、クッキーによりユーザに関するどのような情報が保管されアクセス可能であるのか、これらの情報には誰がアクセスできるのか、クッキーを拒否あるいは無効にしたい場合どうすればよいか、そうした場合に当該ウェブサイトの使用にどのような影響があるかなどを説明する必要がある。

プライバシーに関する指針はデータの取扱や利用に関する特定の状況に応じて作成するべきである。 かかる通知の表現には以下のような定型がある。

「（ご注文を）完了するためには、お客様から特定の情報をいただく必要があります。これらの情報がどのように使われるかに関して規定している弊社のプライバシーに関する指針（*）をお読みください。」

*この部分でプライバシーに関する指針の全文へリンクする。

データ主体がデータを送付する前に、以下のことを知らせるべきである。

「「続ける」ボタンをクリックすることにより、弊社プライバシーに関する指針（*）を読み、そこに規定されたようにお客様のデータを利用することに同意したことになります。」

*この部分でプライバシーに関する指針の全文へリンクする。

7.直接にデータを収集する場合の留意点

企業は個人情報を個々人が記入した申込用紙や、個人とのミーティングから収集することもある。

上記 3 に述べた情報保護原則は、コンピュータにファイルされたデータだけではなく、紙の記録に記載されたデータの収集にも適用される。従って企業は、個人が直接に記入する申込用紙にも、以下のような文章を記載した方がよい。

個人情報について

1. XXX 会社は、データ管理者として登録されています。
2. お客様から提供された個人情報は弊社データベースに保管されることがあります。
3. お客様からのご要望があれば、お客様に関してどのような情報を弊社が保有しているかをお知らせし、コピーをお渡しいたします（ただし、有償となります）。弊社が保有しているお客様に関する情報が不正確であると思われる場合には、ご連絡ください。訂正いたします。
4. 弊社が保有しているお客様に関する情報は機密情報として扱い、弊社内でのみ開示されます。
5. お客様の興味があると思われる弊社サービスについてお知らせをお送りいたします。ただし、お客様から不必要であると連絡をいただいた場合は、中止いたします。

紙ベースの申込用紙で収集されたデータをコンピュータに入力する場合には、データ主体にその旨を知らせる必要がある。

また、紙ベースの申込用紙の保管やミーティングを通して収集したデータの保管の方法に関しても留意する必要がある。これらの情報に不正アクセスできないようにセキュリティ対策を実施する必要がある。個人情報にアクセスできる社員を指定し、実施されているセキュリティ対策を守るよう研修を行う必要がある。例えば、申込用紙は、内容がコンピュータに入力されるまで、鍵のかかる安全なキャビネットで保管する必要がある。また、紙の申込用紙は、コンピュータに入力後、確実に破棄しなければならない。

第 2 章　IT の発展

1.クラウド（Cloud）

データ管理における最近の革新はクラウドである。クラウドの基本的な前提は、データを保有している第三者が外部的にデータ管理を行う場合、個人データは、企業所在地外のリモートサーバー上に保存され、データ使用者が望むときにはいつでもデータ管理プロバイダーが使用している適切なアクセスプロトコルによりアクセスすることができるということである。

問題は、これが企業のデータ管理に関する法にどのように影響するかである。データがイングランドやウェールズ以外の場所あるいは欧州以外の場所にあるリモートサーバーに保有されている場合、これによりこれらの地域で営業している企業は、データは 1998 年法あるいはデータ保護原則の対象外であると言うことができるのだろうか。

残念ながら情報コミッショナーの見解では、これによりデータ保護法令を回避することはできない。イングランドまたはウェールズで営業している場合、企業がどこか遠隔地でデータを保存していたとしても、それによりデータ保護法令の適用範囲外にはならない。データがイングランドまたは欧州で営業している企業で使用するためにアクセスされるならば、データ保護法令が適用される。

企業のサーバーがデータをどこに保存しているかは問題ではない。データが EU 内で営業している企業で使用されるならば、そのデータにはデータ保護法令が適用され、欧州またはイングランドで作成されその他の地域に転送されるのか、あるいはその他の地域で作成保管されるがイングランドまたは欧州にあるコンピュータ端末からアクセスされるのかにかかわらず、そのデータは下記の方法により処理されなければならない。EU 理事会が 6 月 9 日に行った布告では、将来、企業は、データ保護法令の順守と執行に関する権限を有するひとつの機関を相手にしさえすればよいようにするべきことが確認された。

2.データ処理の外部委託

このように外部のデータ取扱者を利用する場合、雇用主は、適切なセキュリティー対策が取り入れられ遵守されるように確保しなければならない。このために、利用者はデータ取扱者と書面による契約を結び、その中でセキュリティーを維持し、個人情報は委託元たる雇用主の指示に基づいてのみ取り扱われるよう確保する必要がある。外部のデータ取扱者を利用すると労働者の情報が欧州経済領域外へ転送されることになる場合、雇用主は転送に適切な根拠があることを確認しなければならない。データ取扱者は、個人情報の収集、取扱、保管に関して、データ管理者としての雇用主に適用されるのと同じ基準を遵守しなければならない。

また、契約社員や派遣社員が業務上個人情報を取り扱う場合、その契約社員や派遣社員は雇用主にとってデータ取扱者になる。社員記録やその他の個人情報を閲覧できるこれらのスタッフの信頼性については、同一レベルの閲覧権を持つ社員の場合と同様に完全な調査を行わなければならない。従って、これらのスタッフと書面による契約を結び、その中で指示がある場合に限りデータを取扱うことおよびデータを安全な状態にしておくことを確保する必要がある。

3.データの転送

データ保護第８原則は、個人情報は（インターネットで、直接本人から、または、その他の方法により収集されたものかを問わず）欧州経済領域以外の国や領域に転送してはならないと規定している。ただし、その国が個人情報の取扱に関して、テータ主体の保護と自由を保護するための適切な方策を施している場合にはこの限りではない。欧州委員会が欧州経済領域以外の国で個人情報に関する保護が適切であると認定している国は、スイス、ハンガリー、カナダおよびアルゼンチンである。アメリカと日本はこのリストに含まれていないことに注意すべきである。
従って、個人情報を日本などの欧州経済領域外へ転送する場合には、受取り側の国（おそらくほとんど日本であると思われるが）の情報保護のレベルに応じて個別に検討する必要がある。保護の適切性を評価するに際しては、以下の事項を検討する必要がある。

a) 情報の性質
b) データの源となる国
c) データ転送の最終目的地国
d) 情報を取り扱う目的と、取扱期間
e) 目的地国の法律、国際的な義務、その他関連する規約
f) 目的地国におけるデータ・セキュリティ対策

欧州経済領域以外の国へのデータ転送禁止には多くの例外があり、以下の場合に該当する欧州連合以外へのデータ転送にはデータ保護第８原則は適用されない。

(i) データ主体が転送に同意している場合
(ii) 転送がデータ主体とデータ管理者との契約の履行に必要である場合、または、データ管理者と契約を結ぶために必要な場合
(iii) 転送が、データ管理者とデータ主体以外の人の間の契約であって、データ主体の依頼により締結されるもの、または、データ主体のためのものを締結または履行するのに必要である場合
(iv) 転送が重大な公益のために必要である場合
(v) 転送が、法的手続き（または、将来の法的手続き）のためにもしくはそれに関連して必要である場合、または、法的権利を立証、行使もしくは防御するために必要である場合
(vi) 転送がデータ主体の死活にかかわる利益を保護するために必要である場合
(vii) 転送が、公的登録簿上の個人情報の一部であり、かつ、かかる登録簿の閲覧条件が、転送後当該データが開示される人、もしくは、その可能性がある人によって、満たされている場合
(viii) 転送が、情報コミッショナーによりデータ主体の権利と自由の適切な保護措置を確保しているとして承認される種類の条件により行われる場合
(ix) 転送が、データ主体の権利と自由の適切な保護措置を確保する方法で行われているとして情報コミッショナーによる承認を受けている場合

多国籍企業の場合、データ転送しようとする場合のうち少なくともその一部は以上の例外に該当すると思われる。典型的な理由としては、転送について社員の同意を得ている、データ転送について顧客から書面による同意を得ているなどである。転送が例外に当たらない場合、データ保護に関するグループ内の規則がグループ全体を通して適切であり、各グループ企業および各社員によって厳守されていれば、グループ内の国際的なデータ転送について承

認を得ることができる場合がある。承認は情報コミッショナー事務局から取得する。日本で現在導入された厳格なデータ保護立法を考慮すれば、かかる承認が得られる可能性は大きい。

4. 2014 年時点における変更点と追加の指針

2014 年 6 月 9 日、EU 理事会は EU 貿易圏外で企業が個人情報を移転する方法に影響を与えると思われる新規則について合意に達した。

データ保護

ルクセンブルクにおける会合において、EU 各国の法相と内相は、データ移転に適用される規則について、および新しい一般データ保護規則案の地域的な範囲について合意に達した。ただし、規則案の残りの論点の文言についてまだ合意に達していないが、同案は現在の EU データ保護法に対する幅広い改革を導入することになると思われる。各国の法相と内相は、これら規則の最終的な文言について欧州議会で交渉が始まる前に、法案の文言について合意しなければならない。

EU 理事会は、法改正について部分的なコンセンサスしかないにもかかわらず、合意の達成には「すべての事項が合意されるまでは何も合意されたことにはならない」（“nothing is agreed until everything is agreed”）という基本原則に基づく必要がある旨を確認した。

「規則では、合法的なデータ移転を行うために利用できる 3 つの経路が定められている」。

1. 「第三国がデータ保護の点で「適切である」（‘adequate’）と欧州委員会が認めた場合。これは、例えばしっかりしたデータ保護法令やデータ保護機関が整備されているというような一定の条件―これは規則に規定されている―が満たされていることを意味する。

2. 適切な保護措置が存在している場合。例えば、データ保護機関により承認を受けた拘束力のある企業ルールなどがある場合。

3. データ移転を必要とする明確に定義された具体的な状況がある場合。例えば、税務調査や競争法違反に関する調査など。

「適切な保護措置」要件（the ‘appropriate safeguards’ requirement）を満たすために企業にはいくつかの選択肢がある。その中には拘束力のある企業ルール（binding corporate rules (BCRs)）に同意することなどがある。BCRs はデータ保護機関による承認を受けたもので、「共同の経済活動に従事する事業グループまたは企業グループ」（“group of undertakings or group of enterprises engaged in a joint economic activity”）内でのデータ移転の方法がどのようなものかを定めたものである。

法的に拘束力のある企業ルールにおいて定める必要のある点には、個人情報の取扱いに関する法的根拠やデータの安全を確保するために備えられている措置のようなデータ保護原則が移転されるデータにどのように適用されるのかなどがある。

「適切な保護措置」要件を満たすためには、EU 外に個人データを移転する企業は、欧州委員会の承認を受けた標準契約約款を利用したり、第三国における個人データの移転先と合意したデータ保護に関する契約条項について規制機関から認可を受けることができる。

規則では、重大な公益事由がある場合のような特定の場合に命じられる法定外のデータ移転も認められている。

限定的な例外のひとつに、「データ管理者が正当な利益を追求するために必要な場合であって、それがデータ主体の利益や権利、自由に優先する」場合に企業が個人データを移転する権利がある。

しかし、この権利を行使できるのは、データ移転が「大規模または頻繁ではない」場合で、データ管理者が「そのデータ移転行為または一連のデータ移転行為をめぐる状況をすべて評価し、その評価にもとづいて個人データの保護に関する適切な保護措置を提供した」場合に限られる。

新しい一般データ保護規則案の地域的な範囲について合意に達した際に、EU 各国の法相内相は、EU 外に本社のある会社も、EU 内に本社のある企業と同様、新規則の順守を強制できる点について意見が一致した。

各国大臣により合意された条文によれば、「本規則は、EU で設立されていないデータ管理者が EU 内に居住するデータ主体の個人データを取扱う場合であって、その取扱いが次のことに関連している場合に適用される。EU 内のデータ主体に対する物品またはサービスの提供。これはデータ主体の支払いが必要であるかどうかを問わない。およびデータ主体の行動の監視。これは当該行動が EU 内で行われる場合に限る」。

各国大臣は、新しい法的枠組みによりデータ保護を規制するために、「ワン・ストップ・ショップ」方式（'one stop shop' mechanism）の計画について議論した。ワン・ストップ・ショップ制の原則は、企業は、法令順守と法執行の問題に関して EU 内のひとつのデータ保護機関のみを相手にすればよいというものである。

新しい EU データ保護指令案の目的は次のとおりである。

1. 基本的な市民の権利や自由、特にプライバシーの権利の保護を改善する

2. データの自由な移動を保護する

現行規則の主な修正点は次のとおりである。

（1） EU 内の規則の統一と簡素化

- EU 規則がすべての EU 加盟国に同じように適用されるように国内法制における不必要な「規則」を改正すること
  - 従来は、各加盟国の立法により規則の執行においていくらか違いがあった

- 企業の運用上の負担（運用手続きを含めて）を簡素化すること
  - 企業がすでに EU 内のデータ保護機関のひとつから承認を受けている場合、他の国の機関の追加承認を受けずに当該企業が活動できるようにする制度の導入

- EU 加盟各国のデータ保護機関の間での円滑な協力を確保する仕組みの確立

- EU 加盟国の各データ保護機関が、他の加盟国のデータ保護機関からの要請があれば、調査などで協力できるようにする制度の導入

(2) 個人情報保護を強化するための規則の制定

- 個人情報の保護に対する個人の権利を強化すること
  - 消去できる権利（当該個人からの要請があれば、ウェブ上にアップロードされた個人情報を削除する義務の導入）
  - データ可搬性（Data portability）（個人がプロバイダーを変更した場合に、当該個人によってアップロードされた情報を当該個人に引き渡すよう企業に強制する規定）
  - 個人情報を取得する過程で必要な同意は明示的でなければならない旨を規定することなど

- 個人情報の取扱いについての企業の説明責任を強化すること
  - プライバシー・バイ・デザイン（企画・設計段階からのプライバシー配慮）の原則（Principle of Privacy by Design）（新サービス導入の前にプライバシー保護対策について考慮しなければならないという要件の導入）
  - 個人情報を処理する際におけるリスク負担の評価を必要とする要件
  - 「データ保護担当役員（“Data Protection Officer”）」を選任する義務（250 人超の従業員のいる企業などはこの義務を負う）

- 個人情報に関するセキュリティーを強化すること
- データ保護に関する個人の権利行使方法の改善
  - EU 加盟国におけるデータ保護機関の独立性と権限の拡大。行政および司法による救済の促進。

5.その他の事項

情報コミッショナーは、データの取扱いに影響する問題について、175 ページのガイダンスを提出している。IT 関係者はこのガイドを入手するよう推奨する。このガイダンスは IT の新しい発展に対処するのに必要なデータの取扱いに関する変更点について述べている。新たな技術的発展があるたびに、情報コミッショナーが対処すべき新たな問題も生じているのである。

第 3 章　強制措置

1.強制措置

情報コミッショナーは英国内における 1998 年法の順守を推進している。データ管理者が上記の８つの原則のいずれかに違反していると情報コミッショナーが判断した場合には、コミッショナーは以下の通知をデータ管理者に送付する。

a)　特定の措置の停止
b)　すべての個人情報または通知で特定された個人情報の取扱いの停止、あるいは特定の目的、期間、方法での取扱いの停止

この強制通知の順守の懈怠は刑事上の違法行為であり、罰金が科される。有罪判決が下された場合、会社だけではなく、違法行為を行ったと認定された会社の取締役、役員またはマネージャーにも罰金が科される点は、注意すべきである。

第 4 章　スタッフに関するデータ保護

1.雇用主の法的義務

個人情報が雇用主により収集・使用・保有される場合には、雇用主は当該情報が不適切に使用・配布されることがないように当該情報を保護する責任を負う。

2.被用者の法的権利

個人の詳細が保有・利用されている場合には、その個人は、正確にどのような情報が保有されており、また、なぜ保有されているのかを知る権利がある。

3.被用者データの規制

この点は、1998 年法のほか、同法に関連する雇用慣行データ保護綱領(Employment Practice Data Protection Code (DP Code))に定められているが、同綱領の目的は雇用主がプライバシー、データ保護の保障措置、および、個人情報に関する秘密保持の維持をすべて真剣に考える社風を発展させるようにすることである。

同綱領は、推奨される行為、雇用主が従うべき重要なポイントと可能な行為を定めている。それぞれ以下の点を扱う 4 つのパートがある。

- 募集と採用
- 雇用記録
- 職場における行動監視
- 健康診断

雇用主は、前述した８つの情報保護原則に従って社員の個人情報を取扱い処理しなければならない。外部のデータ取扱者を利用する場合、その者も雇用慣行データ保護綱領第 2.14 条による要件を遵守しなければならない。

個人情報とは、当該情報、または、雇用主が保有しているまたはその可能性のあるその他の情報から特定できる個人に関する情報である。個人情報には以下のものが含まれることがある。

- 給与の詳細
- 病気および出勤記録
- 相続人/受益者の氏名を記した通知書
- 年次人事評価記録
- 銀行口座の詳細

従業員に関する意見、当該従業員に関する雇用主やその他の人の意思の表示も含まれる。

以下のようなデリケートな問題であると判断される個人情報が取り扱われる場合は、特別な保護が与えられる（1998 年法第 2 条）。

- 人種的民族的出自
- 政治的な意見、宗教的信仰、その他の類似の信念
- 労働組合の加入未加入
- 肉体的または精神的健康
- 性生活
- 違法行為の実行またはその嫌疑、または、実行した違法行為もしくはその嫌疑に関する手続き、および/または、かかる手続きもしくは下された判決の処分。

以下のように情報が個人を特定できない場合は、保護の対象外となる。

- 名前や肩書きなど個人を特定できる情報が使用されていない一般的なレポート
- 資料整理システムの一部ではない手作業によるファイル
- 匿名の個人に関するレポート

4. データ主体閲覧請求

すべての従業員には、当該本人に関して雇用主がどのような情報を保管しているかを知る権利がある。これは、データ主体閲覧請求権（subject access）として知られている。雇用主が保有している情報には、健康状態や病歴、懲戒および研修、勤務評定、メールや面接の記録などが含まれていることがある。従業員は、将来・現在・過去の雇用主に対して、書面で、当該個人雇用主/組織により取り扱われている個人情報のすべてのコピーを請求できる。雇用主は、1 つの依頼毎に最高 10 ポンドの手数料を請求できる。（この請求は最近の雇用法改正と共に増える可能性がある。）

推奨される行為として、雇用主は以下を行うべきである。

- データ主体閲覧請求を受付け、請求から 40 日以内に回答できるように従業員に関する情報を検出できるシステムを構築すること
- 情報が受領権のある人のみに与えられるようにするために、データ主体閲覧請求を行っている者の身元を確認すること
- 第三者の身元に関する情報のうち、どのような情報を留保するのが合理的かについて判断を下すこと
- マネージャーおよび組織内の関係者に対し、従業員からのデータ主体閲覧請求に従ってどのような情報が開示される予定であるかを知らせること
- 開示される情報は理解しやすく、情報源を記載し、また、コピーするのに不釣合いな労力がかからない限りで可能であれば、ハードコピーで渡すようにすること。不釣合いな労力に定義はないが、費用、費やす時間、難しさ、雇用主の規模などが考

慮される要因となる。不釣合いな労力が必要な場合でも、その他の形式で閲覧させなければならない。

- 第三者（通常は、他の従業員）を特定できる情報をすべて削除すること。例えば、その従業員について苦情が申し立てられた場合、苦情申立書類を開示すると、苦情を申し立てた人が特定されてしまうことがある。この場合には、雇用主は苦情を申し立てた人の名前を削除すればよいが、それでもまだ第三者を識別できる場合もある。雇用主は、従業員の閲覧権と第三者のプライバシーに関する権利のバランスをとらなければならない。情報が開示されることに第三者が同意しているか、または、第三者の同意がなくても、いかなる場合でも閲覧請求に応じることが合理的である場合には、雇用主は情報開示を行わなければならない。

社員に関する個人情報を記載している文書であって、その情報が以前は電子的に作成されていても、今ではもはや電子的な形式ではなく紙ベースでのみ保有されている場合、かかる文書を開示する義務は雇用主にはない。同様に、関連資料整理システム（a “relevant filing system”）に保有されていない情報も開示する必要はない。

ある社員に関する個人情報および「関連資料整理システム（a “relevant filing system”）」とは何かという問題は、*Durant 対金融サービス庁*事件[2003 年]において控訴院により検討された。

開示できる個人情報に関して、控訴院は、かかる個人情報には、当該個人が単に間接的に触れられているのではなく、その焦点として含まれていなければならないと決定した。従って、以下の例の情報は、通常、個人情報にならない。

- 他の個人情報と関連していない箇所で単に触れられた個人名
- 個人が公的な資格でビジネス会議に出席した場合に、その議事録に偶然述べられたその個人の出席
- その人に送信またはコピーされたことだけを示している書類やメール上に現れている個人の名前で、その中に当該個人に関する他の情報はない場合

手作業によるファイルに関する「関連資料整理システム（’relevant filing system’）」の解釈に関して、控訴院は、「関連資料整理システム」とは、検索の開始時に、データ主体閲覧請求を行う個人の個人情報になりうる特定の情報がそこに保有されているかどうか、またもしそうならば、どのファイルの中にそれが保有されているかを明確に示すために、ファイルが構造化されているまたは参照されるようになっている資料整理システムであると判示した。

手作業による資料整理システムが「関連資料整理システム」であるかどうかを判断するための基準は「臨時秘書テスト（the “temp test”）」であるということも示された。すなわち、臨時に雇用した秘書が、その会社の資料整理システムに関する詳細な知識なしに、ある個人に関する特定の情報を抽出できるかどうかというテストである。従って、多くの手作業によるシステムは関連資料整理システムでないと思われるので、これらのファイルに保有されている情報はデータ主体閲覧請求により開示する必要はない。

第５章　スタッフの行動監視

1.概説

現代のビジネスにおいて、スタッフの行動監視は、ますます重要かつ争われている問題となってきている。

通常の業務の中で、ほとんどの雇用主が単純な観察または点検に基づくある程度のスタッフの行動監視を行っている。例えば、スタッフによって定期的に利用される電話回数などである。これは一般的な管理行為の一部であり、ほとんどの場合、法的問題の原因にはなりえない。

しかし、論争の的となっているのは、自動的で電子的な手段による侵害的な手段によるスタッフの行動監視を行うという傾向である。例えば、電話の監視、E メールの傍受、ときには有線テレビによる行動監視などである。

一般的に、行動監視は侵害的だとみなされる。従業員が、職場でもある程度のプライバシーがあり、私生活を秘密にしておくことができるという期待を持つことは正当である。従って、行動監視の結果としてこれらの期待にそむく影響があれば、それは、社員のプライバシー侵害の程度と行動監視から雇用主が得られる利益とを比較して正当化されなければならない。具体的に行動監視を規定する法令や規制とは別に、行き過ぎた明らかに侵害的な形の行動監視は、場合によっては、プライバシー尊重を求める権利を個人に与える 1998 年人権法第 8 条（Article 8 of the Human Rights Act 1998）に違反し、また雇用主が負っている黙示的な信頼・信用義務に違反する場合がある。

法令

- 1998 年データ保護法（Data Protection Act 1998）
- 1998 年人権法（Human Rights Act 1998）
- 2000 年捜査権限規制法（The Regulation of Investigatory Powers Act 2000）
- 2000 年電気通信（正当なビジネス慣行）（通信傍受）規制法（Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000）
- 2011 年プライバシーおよび電気通信（EC 指令）（改正）規則（The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011）。その後、第 15 条において、社員が送受信する通信を閲覧する雇用主の権利を改正した。

社員の行動監視はいかなる種類であれ明らかに微妙な問題であり、雇用主は慎重に対処する必要がある。雇用主が電話の会話を聞くことや E メールを閲覧するという考え方に社員が憤慨するのは当然である。従って、行動監視指針の実施は、その導入の前に、あるいは現行の手順を実質的に変更する前に、従業員か従業員の代表と協議して決定すべき問題である。

明らかに、社員の行動監視の程度は、業務の種類が異なれば変わるものである。業務上微妙な機密情報を受領・利用する専門的サービス、IT サービスおよび金融サービスにかかわ

る業種は、例えば、肉体労働の業種と比べてよりいっそう高い程度の行動監視を正当化できるだろう。

一般原則として、行動監視の目的は、企業、規制機関または顧客の真正の必要性と明確に関連があると確認できなければならない。行動監視システムは、その必要性を満たし、その必要性に比例するように個別具体的に計画されなければならない。不当、不必要、過度の行動監視は、ほとんどの場合で合法的とはなりえない。

2.データ保護綱領（The Data Protection Code）―推奨される慣行

データ保護綱領は、社員の通信を監視する決定に関して好ましい推奨される慣行を雇用主のために定めている。好ましい慣行として、雇用主は、以下のことを行うべきである。

- 行動監視の目的を明確にする。これは、行動監視が行われる前に確認すべきである。雇用主は、単に監視のために監視する、あるいは製品やサービスを利用する顧客が要請しているからという理由だけで従業員を監視することは、それを正当化ができないのであれば、行うべきではない。
- 選ばれた特定の方法が、行動監視により得られる利益によって正当化されると認められること。これもまた、行動監視開始前に確認すべきである。
- 従業員が行動監視の性質、範囲、理由を認識しているかを確認する。ただし、（例外的に）秘密裡の行動監視が正当化できる場合は除く。これはどのような行動監視が行われ、なぜ行動監視が必要とされるのかの理由を従業員に知らせることを含む。
- 情報を閲覧できる人を最低限に抑えること。可能であれば、閲覧は人事部のような特定の部門で働いている関連のある責任を負う者に限定すべきである。行動監視によって獲得された個人情報の閲覧は制限されなければならない。さらに、そのような閲覧ができる者は機密保持やセキュリティーの要件を順守し、必要に応じて適切な研修を受けなければならない。
- 収集された情報は他のいかなる目的にも使用してはならないことを保証する。ただし、そうすることが明らかに各従業員の利益になる場合、または、合理的に見て雇用主が無視できないと思われる行為がそれにより明らかになる場合はこの限りではない。
- 情報が各従業員に不利な影響を与える場合、何らかの不利な措置がとられる前に、その情報を見て、例えば、その情報について説明や異議などの申し立てをする機会を与えることを保証する
- 従業員が自分に関して保有されている情報を閲覧する権利は損なわれないこと、および、行動監視システムがこの要件を満たすことができることを確認する

3.法令

– 2000 年捜査権限規制法（The Regulation of Investigatory Powers Act 2000 ）

捜査権限規制法は通信の機密保持を保護し、公共または民間の電気通信システムにおける伝送中の傍受を規制する法的な枠組みを設立した。捜査権限規制法の主要な目的は、警察が E メールやインターネット通信を閲覧し、登録情報へのアクセスを取得できるようにすることだった。しかし、捜査権限規制法の規定の中には、社員の通話、E メール・メッセージ、インターネットのアクセス状況を監視する雇用主にも適用されるものもある。

捜査権限規制法第 1 条は、「合法的な権限なく、公共または民間の電気通信システムによる伝送中の通信を故意に傍受することは違法である」と規定している。

捜査権限規制法が扱う範囲は以下の通りである。

- 通信の傍受
- 通信データの取得
- 侵害的な捜査方法
- 暗号化されたデータへのアクセス

捜査権限規制法はまた、民間の電気通信ネットワークに関する違法傍受に対する別の民事責任を規定している。それにより、事実上、送信者と受信者双方に、違反についてシステム運営者に対して損害賠償を請求する権利が与えられる。

捜査権限規制法の下では、雇用関係において、以下の場合に、雇用主が通信を傍受する「合法的権限」がある。

1. 傍受の理由が、2000 年電気通信（正当なビジネス慣行）（通信傍受）規制法（the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*）の範囲内である場合。
2. 送信者および受信者 (あるいは受信予定者 or intended recipient) 双方が傍受に対して明示的に同意している場合。

*2000 年電気通信（正当なビジネス慣行）（通信傍受）規制法*は、ビジネスに関連する広範な状況で社員の通信を傍受する権限を与えているが、それでも雇用主は行動監視開始前に社員の同意を得ることがきわめて望ましい。これは疑念の余地を払拭し、あらゆる種類の通信の行動監視を会社が行っていることを誰に対しても明瞭にする。ほとんどの場合、雇用主は社員の雇用契約書に行動監視についての適切な同意条項を盛り込んでいるが、そのような条項が含まれていない場合には、別途、同意書が署名されることがある。いずれの場合でも、同意の証拠を示すために書類に社員の署名がなければならない。行動監視指針の詳細を記載したスタッフハンドブックだけに頼るのは雇用主にとって十分ではない。

– 2000 年電気通信（正当なビジネス慣行）（通信傍受）規制法（Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000））

2000 年電気通信（正当なビジネス慣行）（通信傍受）規制法（以下、「電気通信規制法」という。）第 1 条で、雇用主は従業員の通信を傍受することは、原則として違法行為であるとされているが、電気通信規制法で定められた特定の状況下においては、雇用主は通信を傍受する合法的な権限を有する。

基本的な点では、電気通信規制法は、企業のビジネスネットワークにおける社員通信の一定の傍受を正当と認めている。このような傍受は、もし電気通信規制法がなければ 2000 年捜査権限規制法で禁止されるものである。電気通信規制法の全般的な目的は、通信の監視が電気通信規制法およびヨーロッパ人権条約を遵守して行われることを保証することである。本質的に、電気通信規制法は企業が送信者、受信者または電話をかけてくる者の承諾なしに通信を傍受し、監視し、記録することが合法となる多くの場合を定めている。しかし、同法は、指令 2002/58/EC 第 5 条に定められたデータの取扱いとプライバシーに関する規則の範囲内で許される傍受のみを許している。

電気通信規制法は、社員が既に同意した傍受には適用されない。かかる傍受は捜査権限規制法で禁止されていないからである。

2000 年電気通信（正当なビジネス慣行）（通信傍受）規制法

電気通信規制法によれば、社員だけでなく、社員に電話をかけてくる者や E メールを送信する個人に対しても傍受が行われることを通知しなければならない。この問題に対処する一般的な方法は、以下のようなものである。

(i) 自動的に録音されている電話メッセージが流され、電話をかけてくる者全員に通話が監視されている可能性があることを告げる
(ii) すべての送信されるメールに、受信する通信が組織によって監視されているという趣旨の記述をつける
(iii) 通信文や営業資料にその趣旨の警告を印刷する

電話をかけてくる者や通信者に、通信が監視されていることを通知しなければ、プライバシーの侵害について損害賠償を求める民事訴訟が提起されるおそれがある。

– **1998 年データ保護法（Data Protection Act 1998 ）**

雇用主が社員の通信監視から得られた情報の記録を保管する場合、この情報は 1998 年データ保護法に定義される「個人情報（“personal data”）」となる。同法は、紙ベースの書類で保有されるデータ、コンピュータシステムに蓄積されるデータまたは E メールによって処理されるデータに適用される。従って、このようなデータはデータ保護法の規定に従って取り扱われなければならない。雇用主は、従業員が監視によって収集された自分たちについての情報のコピーを取得する権利があることを認識しておかなければならない。

– **1998 年人権法（Human Rights Act 1998）**

1950 年ヨーロッパ人権条約第 8 条（Article 8 of the European Convention on Human Rights 1950）は、人権法に組み込まれているが、「すべての人が、自分の個人生活および家族生活、家庭ならびに通信に対する尊重を求める権利がある」と定めている。

社員の行動監視と第 8 条が矛盾する可能性は容易に推測できる。企業の正当な営業上の要求と社員のプライバシーを守る権利との平衡を保つのは、簡単なことではない。それにもかかわらず、このような状況で人権侵害を主張して訴訟を起こすと脅されることは多いが、訴訟が成功するのはまれである。

4.情報と同意

電気通信規制法の下で行動監視を合法的に行うためには、雇用主は傍受が行われていることを将来の利用者に知らせるべくあらゆる合理的措置を講じていなければならない。この点は個人の雇用契約に記載されることが多いが、社員に通知するにあたってはスタッフハンドブックあるいはインターネット・E メール取扱指針の記述でも十分である。例えば、以下のようなものである。

「当社は社員が使用する電話、E メール、インターネットの監視に関する指針を採用しました。監視は 2000 年電気通信（正当なビジネス慣行）（通信傍受）規制法により認められた業務上の目的のためにのみ行われる。従って、こちらからかける電話、先方からかかってきた電話、送受信した E メール、仕事中にアクセスしたインターネットサイトは管理職に

よって傍受されることがあることをご承知下さい。指針や規則の完全な詳細は社員ハンドブックに記載されています。」

しかし、電気通信規制法によれば、社員だけでなく、社員に電話をかけてくる者や E メールを送信する個人に対しても傍受が行われることを通知しなければならない。この問題に対処する一般的な方法は、以下のようなものである。（ⅰ）自動的に録音されている電話メッセージが流され、電話をかけてくる者に通話が監視されている可能性があることを告げる、(ⅱ）すべての送信されるメールに、受信する通信が組織によって監視されているという趣旨の記述をつける、(ⅲ)通信文や営業資料にその趣旨の警告を印刷する。

重要なのは、（電気通信規制法で要求されているように）傍受が行われる可能性があることを利用者に**通知**することと、利用者の**同意**を得ることの違いについて明確にしておくことである。同意が必要とされるのは行動監視の目的が電気通信規制法の範囲に含まれない場合である。

社員に会社の行動監視指針を通知した後は、雇用主は、以下の業務上の目的または状況のいずれかがあれば、社員の同意の有無にかかわらず、電気通信規制法に基づき社員の通信を合法的に傍受、監視、記録することができる。

1. 業務に関係する事実が存在するかどうかを立証するため。これは、一般的に、電話や E メールによって業務を行う会社や、取り交わされた契約条件に関して証拠を提出する必要がある場合に関係する。
2. 業務に関連する規制や自主規制の慣行または手続きを遵守しているかどうかを確認するため。この最も一般的な例は、例えば、FSA 規制を遵守している金融機関が通話を記録するというものである。
3. 社員が雇用主の通信システムを使用して達成あるいは達成すべき水準を確認または証明するため。（これは一般的にスタッフの教育や顧客サービスに関連する）
4. 国家安全保障のため。
5. 犯罪の防止や捜査のため。
6. システムの不正使用の調査や捜査のため。
7. システムの効果的作動を確保するため。ウィルスに感染する危険性やその他「ハッキング」のようなシステムに対する脅威を調べるためにコンピュータシステムを監視することは正当である。

さらに、受信した通信が雇用主の業務に関連しているかどうかを判断するためである場合、監視は許容されるが、記録は許容されない。しかし、監視の最中に通話や E メールの内容が雇用主の業務に無関係で、個人的あるいは私的な性質のものであることが明らかになった場合は、それらは電気通信規制法の範囲外になるので、雇用主は通常明らかに個人的な受信・送信メールの内容を開いたり読んだりしてはならないことに注意しなければならない。しかし、そのような通信が非合法であったり、会社の指針に違反したりする事柄を含む可能性があると会社が考えるのが合理的であれば、それらの通信は「業務に関連する（“relevant to the business”）」と言える。これは、通信が、例えば、機密情報、ポルノその他の不快な内容、中傷的な記述を含む場合に起こりうる。

5.秘密裡の行動監視

秘密裡の行動監視とは、相手に気づかれないように行動監視を行うことであるが、例外的な状況においてのみ正当となる。例えば、従業員に行動監視が行われていると通知すると、

国家安全保障、犯罪の防止や捜査、犯罪者の逮捕や告発、あるいは税金や公租の賦課が害される場合である。行動監視に関する一般的な規則を遵守するための要件だけでなく、特定の好ましい慣行の推奨もある。

民間調査機関を使用するなら、雇用主は調査員が雇用主の義務に従って行動するように契約上要求されているかどうかを確認しなければならない。

好ましい慣行として、雇用主が行うべきことは以下の通りである。

- 通常、上級経営陣に秘密裡の行動監視を認めるよう要求する。正当化されるためには、犯罪行動や業務上の過誤を疑う根拠があり、関係する従業員に通告すると、その防止や捜査が妨害されるということを上級経営陣が納得しなければならない。
- 秘密裡の行動監視は厳密に対象が限定され、制限された特定の時間枠の中で行われることを保証する。関係者の人数も同様に制限されるべきである。
- 秘密裡の行動監視は、従業員がプライバシーが守られていると思うことが合理的な領域、例えば、個人オフィス内やトイレ内などで使用されないことを保証する。例外的にそのような領域を監視する必要がある場合は、警察と連携する意思がなければならない。
- 入手した情報の開示や閲覧を制限する明確な規則があることを保証する。入手した情報は秘密裡の行動監視のためにのみ使用されなければならないし、収集された他の情報は破棄されなければならない。ただし、それが、合理的に考えていかなる雇用主でも無視できないと予想できる情報を明らかにしている場合は、この限りではない。

私生活の尊重を要求する権利（1988 年人権法第 8 条）も、雇用主が行う秘密裡の行動監視に影響を及ぼす。*Robert McGowan 対 Scottish Water 事件(2004 年)* では、ある社員が出張呼び出し（call-outs）や勤務時間に関してタイムシートを偽造しているのではないかと雇用主が疑って、その社員を「スパイする」ために秘密の監視カメラが使用された場合、それは、私生活に対する尊重を要求する権利（1988 年人権法第 8 条）を侵害するものと推定された。しかし、決定的要因は、行動監視をする際の雇用主のとった措置が社員の違反行為疑惑に見合ったものであったかどうかであると判示された。この訴訟では、社員の違反行為疑惑が生じたため雇用主は問題を調査せざるをえなかったということ、および、監視の目的は当該社員が自宅を出て勤務先に向った回数を立証することであるが、これは彼のタイムシートの正確さやその他の点に影響を及ぼすこととなるので、秘密裏の行動監視は雇用主がその資産を守るために行わざるをえなかった調査の根本にかかわり、それゆえに不相応ではなかったということが判示された。

ROBERT A MCGOWAN 対 SCOTTISH WATER 事件 (2004 年)

- 雇用主が秘密裡の行動監視を行うことは、1950 年ヨーロッパ人権条約第 8 条に基づく社員の個人生活や家族生活に対する尊重を要求する権利を侵害するものではなかった。事実によれば、このような行動監視は不相応ではない。
- McGowan 氏が偽造したタイムシートを提出した疑いに基づいて、雇用主である Scottish Water は秘密裡の行動監視を行うと決定した。
- その後、雇用主の懲戒手続きに従って McGowan 氏は解雇された。
- McGowan 氏は、不当に解雇されたこと、および、行動監視は 1950 年ヨーロッパ人権条約第 8 条に基づく社員の個人生活や家族生活に対する尊重を要求する権利を侵害したことを主張した。

  判決：Scottish Water は公社であり、実質的には犯罪行為であることを調査していた。行動監視は Scottish Water が会社の資産を守るために行わなければならない調査の核心であった。行動監視は外的な理由あるいは気まぐれな理由で行われたものではなく、不相応ではなかった。

- この事件は次の事件の事実と比較すべきである。

COPLAND 対 UK 事件 (2007 年)

- 原告は継続教育学校（further education college）で秘書として働いていた。学校には行動監視指針は定められていなかった。7 か月間、電話、電子メール、インターネットを利用しているときに、原告は雇用主によって監視されていた。
- 行動監視の表向きの目的は、原告が自らの個人的な利益のために雇用主の設備を過度に利用しているかどうかを確認するためであった。欧州人権裁判所は、雇用主の行為は、欧州人権条約第 8 条に基づく原告のプライバシー権を侵害したと決定した。

第 6 章　雇用契約におけるデータ保護

1.契約規定

雇用主は、雇用契約またはスタッフハンドブックや指針の中にデータ保護に関する規定を含めておくべきである。その理由は、雇用主が個人情報に関して行うかもしれない行動がデータ保護立法に反しているおそれがあっても、もし社員が特定の方法でデータが利用されることについて同意を与えている場合は、かかる行動は一般的に許されるからである。

例えば、雇用契約には次のような文言の同意を含める必要がある。

1998 年データ保護法に関して、本契約の履行に関連するすべての目的のために、当社に提供された個人情報を保有し取扱うことに対して同意する。かかる目的には以下のものが含まれるが、それらに限られない。

こうして、その後に様々な目的を規定する。例えば、人事記録の管理と維持、給与その他の報酬・手当の支払いと調査、社員記録の維持など。

同様に、雇用主が社員による電子メール、電話、その他の通信を監視するつもりならば、具体的な同意が必要である。社員が署名した 雇用契約にこの趣旨の規定があれば、それが具体的な同意となる。

2.雇用推薦状（Employment References）

近年、会社と個人に相当な混乱を引き起こしている話題は、雇用推薦状の提供に関して法律はどうなっているかという点である。

雇用推薦状に関しては多くの考慮要因があり、推薦状を与えるべきかどうかは今回のセミナーの範囲外である。

それにもかかわらず、ある雇用主から将来の雇用主に向けて推薦状が出された場合、データ保護に関係する点は、情報コミッショナーが実務ガイドラインを発行して明らかにされた。

個人には自分について保有されている情報であってデータ保護法の適用があるもののコピーを請求する権利がある。個人が自分について書かれた推薦状のコピーを要求した時、推薦状は秘密のまま提供されるものであるという理由で、多くの雇用主はこれを拒否している。

同法の規定によれば、会社が社員に関して与えた秘密推薦状のコピーを当該社員が雇用主に要求した場合、会社はこれを社員に提供する義務はない。その趣旨の例外が同法に規定されているからである。

しかし、その推薦状の受取人は同じ扱いにはならない。会社が採用候補者に関して推薦状を受け取った場合、その推薦状には閲覧に関する通常の規則が適用され、それによれば、個人は、会社が当該個人に関して保有している文書の閲覧を請求できる。閲覧請求権により、個人は自分について保有されている情報を閲覧することができるが、他の人の意見など、秘密裡に提供された他の人に関する情報については必ずしも閲覧できるとは限らない。

会社が受け取った推薦状に「親展（“In Confidence”）」と表示されている場合、当該会社はその推薦状に含まれている情報が実際に機密であるかどうかを検討する必要がある。会社が、雇用開始日、欠勤記録などのような個人にとって既知の事実情報を保留することは賢明ではない。しかし、推薦者によって提供された意見情報は機密にしておくことができる。このような状況では、会社は、自分の意見を機密として扱ってもらうことについての推薦者の利益と、自分について何が言われているかを知ることについての個人の利益とを比較考量すべきである。

あらゆる場合において、その情報を見たいという請求に応えることが合理的かどうかを検討する時には、会社は以下の要因を考慮する必要がある

- 機密保持に関する明示的な保証が推薦者に与えられているかどうか
- 同意を保留することについての推薦者側の理由
- 推薦状が個人に与える潜在的現実的効果
- 推薦状は正確かつ真実でなければならず、かつ、推薦状を閲覧できなければ、個人は推薦状の正確性に異議を唱えることができないという事実
- 好ましい雇用慣行では、社員はその弱点を知らされているはずであるという点
- 推薦者に対する危険

また、企業は、推薦者の身元を秘密にしておくことが可能であり賢明であるかどうかも検討する必要がある。

ほとんどの場合、推薦状を与えるよう依頼される雇用主は、現在、提供する情報は意見情報ではなく事実情報に限るようにという助言を受けている。「*スミス氏は当社に 2001 年 1 月 1 日から 2005 年 12 月 31 日まで働いていた。彼の役職名は財務管理者（financial controller）だった。当社には彼の清廉と能力を疑う理由はない。*」というような事実の推薦状ならば、会社に問題をもたらす可能性は低い。

しかし、雇用主は、退職する社員との友好的な解決を容易にするだけのために推薦状に不正確な情報を記載しないように注意しなければならない。これは、雇用法上の請求や、推薦状を信頼すると合理的に予想される者からの損害賠償請求を引き起こす恐れがある。

3.結論

この報告の目的は、データ保護とスタッフに関するビジネス上の問題に関する規制の現状について概観することである。

マーケティングや顧客管理に関するデータの規制には別の規則が適用される。この点は、2003 年電子商取引（EC 指令）規則（the Electronic Commerce (EC Directive) Regulation 2003）により扱われる。

電気通信システムのプロバイダーは、顧客を保護するための特別な規則に服する。英国の関連法令は 2003 年通信法（the Communications Act 2003）に規定されている。

電気通信サービスやその設備におけるプライバシー権とデータ保護の調和を定める指令 2002/58/EC など、様々な規則が EU において制定されている。この指令に基づき、重要な規則が以下の法令に定められている。

2004 年プライバシーおよび電気通信規則（EC 指令）（改正）規則（The Privacy and Electronic Communications Regulations (EC Directive) (Amendment) Regulations 2004）

2011 年プライバシーおよび電気通信規則（EC 指令）（改正）規則（The Privacy and Electronic Communications Regulations (EC Directive) (Amendement) Regulation 2011）

最近では、通信セキュリティー違反の報告を定める EU 規則 611/2013 がある。この規則は 2013 年 8 月 25 日から施行され、セキュリティー違反が生じた国の国家データ保護機関（the National Data Authority）に対して、違反の発見から 24 時間以内に違反を通知するよう求めている。

影響を受ける個人または主体（法人）にできるだけ早く通知しなければならない。各場合における通知の書式は、同規則の補足規定 1 および 2（Annex 1and 2）に定められている。銀行、公的機関、その他の企業がデータ保護違反について最近メディアで発表するようになったことは、これらの規定の効果の一例である。

このようにデータ保護規制は現代の企業の行動様式に根本的な衝撃を与えるので、企業は法令順守を常に確保するために法の発展に遅れずについてゆくことが極めて重要である。