<English follows Japanese>

2016 年 6 月 27 日

Brexit が個人情報保護に及ぼす影響

執筆者：ロッケ・モーレルおよびローナン・ティグナー

英国で実施された直接国民投票の結果、僅差で EU 離脱（「Brexit」）への賛成が反対を上回りました。しかし、Brexit 実施の手続きには時間がかかる見通しであり、依頼者の皆様の業務にどのような影響が及ぶかについても、今後徐々に明らかになっていくものと思われます。モリソン・フォースターの Brexit Task Force は全てのオフィスを横断的に連携させ、依頼者の皆様にとって関心の高い問題に対応したサービスをその時々に応じて提供してまいります。また、特に重要なテーマについては、MoFo Brexit Briefing を発信していく予定です。皆様のニーズに合わせたサポートをご提供できるよう努めてまいります。

短期的には変化はない

英国は当面は EU 加盟国の地位に留まる。したがって、データ保護指令（「本指令」）及び e-プライバシー指令は、現在英国の国内法において実施されている形のままでの適用が継続される。2018 年 5 月には本指令に代わって EU 一般データ保護規則（GDPR）が施行される予定であり、それまでに、GDPR の施行に伴う変更を反映するために e-プライバシー指令が改訂されることになっている。英国の EU 離脱が実現するまでに移行期間は終了する見通しであるため、英国が正式に EU を離脱する前に GDPR が施行される可能性も十分に考えられる。

GDPR は EU 規則という形式を採っており、全ての EU 加盟国に直接的に適用されるため、英国が同規則を国内法として実施するために何らかの手続きを踏む必要はない。また、英国が EU を離脱する前に、改訂後の e-プライバシー指令の国内法化を余儀なくされる可能性も十分に考えられる。データ移転に関する EU の規則は EU 域内における個人情報の移転には適用されないため、英国が正式に EU を離脱するまでは、英国と他の EU 加盟国間のデータ移転は現状のまま継続される可能性がある。

英国の EU 離脱後に変わること

英国が EU を離脱すれば状況は変わる。すなわち、英国が EU を離脱した時点から、GDPR は英国ではもはや適用されなくなる。ただし、（e-プライバシー指令を含む）EU 指令を国内法化した英国の法令は、それらの法令が改正または廃止されるまで引き続き効力を有する。したがって、GDPR のデータ移転規則上、英国は「第三国」として扱われることになる。そうなると、一定の条件を満たしている場合を除き、EU 域内で設立された事業者は、対象と

なるデータについて「十分な保護措置」を講じている場合に限り、例えば英国のような第三国に個人情報を移転することが可能となる。

英国が要求される「十分性認定」を取得するための選択肢としては以下の 3 つが挙げられるが、このうち採用される可能性が最も高いのは 3 つ目の選択肢である。

• 欧州経済領域（EEA）の参加国となる： 英国は、EEA 協定の調印国となることにより、（ノルウェー、リヒテンシュタインおよびアイスランドと同様）欧州経済領域（EEA）の参加国となる可能性がある。その場合、EEA 協定第 7 条に基づき、英国は 4 つの自由に関連する EU の法令（GDPR を含む）に直接的に拘束されることを受け入れなければならない。人の移動の自由等、Brexit 支持者に不評な多くの EU のルールに従うことを約束しなければならなくなるため、ノルウェー、リヒテンシュタインおよびアイスランドが採用したこの方式を英国政府が選択する蓋然性は低いと考えられる。

• スイス方式： スイスは、EU または EEA のいずれにも加盟していない（ただし、スイスは EU と二国間合意を締結しており、単一市場への参加は認められている）。スイスは本指令による拘束は受けないものの、国内法において本指令を完全に施行しており、かかる事実に基づき、欧州委員会から「十分性認定」を受けている。同国は既に、GDPR が施行された場合にはこれを反映すべく国内法を改正し、十分性認定を維持する方針を表明している。また、スイスは欧州司法裁判所（ECJ）の管轄には服していないものの、ECJ の判例法は同国の法制度にも重要な影響を及ぼしている。例えば、ECJ が EU／米国間のセーフハーバー協定を認める欧州委員会の決定を無効と判断したことを受けて、スイスもまた、同国と米国間のセーフハーバー協定は同国から米国へのデータ移転を容認する十分な法的根拠にはならないと宣言した。EEA 参加国になるという選択肢と同様、スイス方式を採用する場合にも、英国は EU の規則の決定プロセスに参加する権限を持たないまま、今後施行が予定されている GDPR のほか、データ保護に関する EU の法規制をそのまま採択することを義務付けられることになる。人の移動の自由等、Brexit 支持者に不評な多くの EU のルールに従うことを約束しなければならなくなるため、スイスが採用したこの方式を英国政府が選択する蓋然性は低いと考えられる。

• 完全十分性認定方式： 英国は、独自のデータ保護法令を実施し、自国の法制度が EU のデータ保護法が定める基準に照らした評価において「十分」であることを認定するよう欧州委員会に対して要請することが考えられる。一見すると、この選択肢は好ましい選択肢であるように思われる。なぜなら、この方式によれば、（GDPR を巡る交渉において同国が主張していたとおり）英国は取引を円滑に進めるために一部のルールを緩和することが可能であるからである。しかし、英国が自国と EU 間のデータ移転をスムーズに継続できるよう、EU 離脱後速やかに十分性認定を取得したいと考えるのであれば、GDPR に近似した規定の導入を余儀なくされる可能性が高い。それ以外の方法を採ろうとすれば、英国が早期に十分性認定を取得する可能性が遠のくおそれがある。なぜなら、EU は、英国が EU 加盟国に対して有利となる、またはある種のフォーラムショッピングを可能にするようなルールの緩和には当然反対すると考えられるためである。したがって、英国の情報コミッショナー オフィス（ICO）が、英国のデータ保護基準は GDPR と同等のものにならざるを得ないとの声明を既に発表したことも驚くには値しない。注目したいのは、英国がかねてからデータ保護の必要性を訴えてきた国であり（例えば、英国では、本指令が採択される 10 年以上も前に法整備がなされている）、プライバシー法令に対する認識も国民の間に深く浸透しているという点である。また、英国は、欧州評議会条約第 108 号（データ保護に関する主要な原則を規定）および「欧州人権条約」（「ECHR」、第 8 条においてプライバシー権を規定）を批准しており、欧州人権裁判所の管轄にも服している。更に、ICO は「グローバルなプライバシーの執行に係るネットワーク（GPEN）」のメンバーでもある。GPEN は、国境を越えた情報共有と世界のプライバシー監視機関による国境を越えた執行における協力の強化を目的とした機関である。これらはすべて、英国の十分性を示唆するものであるといえる。ただし、Schrems 事件において ECJ が下した近時の判決は、英国にも影響を及ぼす可能性があることを指摘しておきたい。Schrems 事件の判決において、ECJ は、（端的にいえば）米国諜報機関の権限は、厳格な必要性審査の原則および比例性の原則に照らして、国家安全保障の目的に対する手段として容認される範囲を超えており、また、個人は自己のプライバシーを保護する十分な法的救済手段を有していないため、欧州市民のプライバシーが十分に保護されているとはいえないとして、セーフハーバー協定を遵守している米国企業へのデータ移転を認める同協定を容認するとした欧州委員会の決定

は無効であるとの判断を示した。諜報機関が過度に強力な監視権限を有しているとの懸念は、英国の諜報機関にも当然に当てはまる。英国の調査報道協会（Bureau of Investigative Journalism）や複数の市民権保護団体が提起し、現在欧州人権裁判所で係属中の 3 つの事件のほか、英国諜報機関の一般的な監視権限が欧州人権条約第 8 条に違反しているとの申立てについての判断が下されれば、今後の見通しがより明確化するものと考えられる。

結論

短期的に見れば、英国が EU 加盟国でなくなるまでは何も変わらず、データ移転もこれまでどおりに行われる可能性がある。

英国が「十分性認定」を得るために 3 つの方式のうちいずれを選択したとしても、結果的には英国の個人情報保護法令は、近く施行される GDPR 等の EU のプライバシー規則に沿ったものとなるであろう。

今後企業が取るべき措置

• Brexit 後に英国が実施するデータ保護法令の内容にかかわらず欧州委員会は「十分性認定」を行うと思われるが、EU 脱退の時点において認定がなされているとは限らない。そのため企業は、標準契約条項（SCC）の締結など、EU 域内から英国へのデータ移転に関して別の取決めを用意する必要がある。データ管理者とデータ処理者は、拘束的企業準則（binding corporate rules（BCR））を導入して、グループ内データ移転に関する「適切な保護措置とする」こともできる。いずれにせよ、Schrems 事件の判決を受けて、欧州委員会の十分性認定に、また、新たな枠組みである「EU 米国間プライバシー・シールド」の条件については EU と米国の交渉の成行きに左右されるのを避けるため、企業が BCR を実施する方向に動き出している様子がうかがえる。

• ビジネスにおいて GDPR に基づく要件を実施するまでの準備期間を考えれば、英国内の企業は引き続き GDPR の施行に向けた準備を進めることが推奨される。上記のとおり、最終的に英国は GDPR に酷似した規則を実施すると思われるからである。また、EU 加盟国の市民に商品やサービスを提供し、またはその言動をモニタリングする英国の企業のデータ処理活動に今後も GDPR が適用される可能性があることに留意すべきである。中央データ処理システムを運用する営業所を他の EU 加盟国内に有する英国の企業にも同様のことがいえる。

• ICO は、多くの場合、データ保護監督機関（DPA）として BCR の承認を主導してきたが、EU 離脱後は、DPA として主導的役割を果たす権限がなくなる。したがって、ICO を主導 DPA として BCR を整備する企業は、主導 DPA として役割を果たしてもらえるよう他の EU の DPA に交渉を申し入れなければならない。BCR の承認申請のために主導 DPA およびその共同責任者を選任する必要がある企業は、この点を考慮すべきである。

ご質問等がある場合は遠慮なくお問い合わせください。

コンタクト:

ロッケ・モーレル
44 (20) 79204054
lmoerel@mofo.com

ローナン・ティグナー
32 (2) 340-7358
rtigner@mofo.com

または

brexit@mofo.com

モリソン・フォースターについて:

モリソン・フォースターは優れた実績を誇る世界的な法律事務所です。クライアントには大手金融機関、投資銀行、Fortune 100 企業、テクノロジー・ライフサイエンス関連企業等が名を連ねています。*American Lawyer* 誌の A-List に過去 12 年間連続で選ばれただけでなく、*Fortune* 誌が「働きたい全米トップ 100 企業」として当事務所を挙げています。モリソン・フォースターの弁護士はクライアントのために最良の結果を出すことに全力を注ぐ一方で、より強固な事務所となるべく各弁護士の個性を失わないよう配慮しています。詳しくは、当事務所のウェブサイト（www.mofo.com）をご覧ください。

本稿は一般的なもので、ここに含まれる情報はあらゆる事案に適用されるものではなく、また個別の事案に対する具体的な法的アドバイスを提供するものでもありません。過去の結果が今後も同様に当てはまることが保証されているものではありません。

27 June 2016

Brexit: Data Protection Implications

By Lokke Moerel and Ronan Tigner

The United Kingdom has voted by a narrow majority to leave the European Union ("Brexit"). But the process of Brexit will take time, and the implications for our clients' businesses will also unfold over time. Our MoFo Brexit Task Force is coordinating across all of our offices and working with clients on their key concerns and issues, now and in the coming weeks and months. We will also be providing MoFo Brexit Briefings on a range of key issues. We are here to support you in any and every way that we can.

No changes in the short term

For the time being, the UK remains a member of the EU; and the Data Protection Directive ("Directive") and e-Privacy Directive as currently implemented in UK law continue to apply. The Directive will be replaced by the EU General Data Protection Regulation (GDPR) in May 2018, and in the coming period the e-Privacy Directive will be updated to reflect the changes that the GDPR will bring. Given the time that will elapse before Brexit actually occurs, it may well be the case that the GDPR will come into force before the UK formally exits the EU.

As the GDPR has the form of an EU regulation, it will be directly applicable in all EU Member States, and no steps need to be taken by the UK for it to be implemented in the national law of the UK. Further, it may well be the case that the UK will have to implement the amended e-Privacy Directive into UK law before Brexit takes place. Until the UK formally exits the EU, data transfers between the UK and the other countries in the EU may continue to occur because the EU data transfer rules do not apply to transfers of personal data within the EU.

Changes after Brexit

The situation will change when UK leaves the EU. From that moment on, the GDPR will no longer be applicable in the UK. The national laws implementing EU directives (including the e-Privacy Directive) will, however, remain in force until they are amended or repealed. Thus, the UK will

become a "third country" under the data transfer rules in the GDPR. In this case, personal data can only be exported by a business established in the EU to a third country, such as the UK, if there is an "adequate level of protection" for such data, unless certain conditions have been met.

There are three options under which the UK may obtain the required "adequacy status", with the third being the most likely:

• Becoming an EEA member: The UK may (like Norway, Liechtenstein and Iceland) become a member of the European Economic Area by becoming a signatory to the EEA Agreement. Under Article 7 of the EEA Agreement, the UK would still need to accept being bound directly by relevant EU laws relating to the four freedoms, including the GDPR. This option is unlikely to be pursued by the UK government in the form adopted by Norway, Liechtenstein and Iceland, in view of the fact that the UK would need to agree to be bound by many of the rules of the EU which have been unpopular with Brexit supporters, including the free movement of people.

• The Swiss solution: Switzerland is not part of the EU or EEA (although it has bilateral agreements with the EU allowing access to the single market). Although not bound by it, Switzerland has fully implemented the Directive into its domestic legislation and, on this basis, has received an "adequacy finding" from the European Commission. Switzerland has already indicated its wish to update Swiss legislation to reflect the application of the GDPR and retain its adequacy status. Also, although Switzerland is not subject to the jurisdiction of the European Court of Justice (ECJ), the ECJ's case law has had a significant influence on Swiss legislation. For instance, after the ECJ struck down the EU-US Safe Harbor Decision of the Commission, the Swiss also declared that the Swiss-US Safe Harbor did not provide a sufficient legal basis for exporting data from Switzerland to the U.S. As with becoming a member of the EEA, the Swiss model would require the UK to adopt the GDPR as it stands now and any further EU legislation on data protection, without having any right to participate in EU rule-making. This option is unlikely to be pursued by the UK government in the form adopted by Switzerland because it would entail the UK agreeing to be bound by many of the rules of the EU which have been unpopular with Brexit supporters, including the free movement of people.

• Full adequacy finding: The UK implements its own data protection laws and requests the Commission to issue a decision that its legal regime is "adequate" when assessed against the standard set by EU data protection law. At first sight, this seems the preferred option because it enables the UK to relax some of the rules in order to facilitate trade (as it advocated in the negotiations over the GDPR). However, if the UK wishes to obtain a quick adequacy decision to continue to facilitate data transfers between the UK and the EU also upon exit, it will likely have to implement provisions that are close to the GDPR. Any other approach could set the UK back in getting a quick adequacy decision. The EU may well be averse to any softening of the rules that would give the UK an advantage over EU Member States, or enable some sort of forum shopping. It is therefore not surprising that the UK Information Commissioner's Office (ICO) has already issued a statement that UK data protection standards would have to be equivalent to the GDPR. We note that the UK has been a long-standing advocate of data protection (e.g., it had a law more than 10 years before the Directive was adopted) and there is solid public awareness of privacy laws. The UK has further ratified Convention 108 (which sets core principles for data protection) as well as the European Convention on Human Rights ("ECHR" – which, in article 8, provides for the right to privacy), and the UK is subject to the European Court of Human Right's competence. The ICO is a member of the Global Privacy Enforcement Network (GPEN), intended to strengthen cross-border information sharing and co-operation in cross-border enforcement among privacy authorities around the world. This all seems to point into the direction of adequacy. We highlight, however, that the recent Schrems judgment of the ECJ may also have implications for the UK. In

the Schrems judgment, the ECJ invalidated the decision of the Commission that approved the Safe Harbor Framework facilitating data transfer to U.S. companies that adhered to this framework, because the privacy of European citizens was not considered to be adequately protected (in short) because the powers of the U.S. intelligence services went beyond what was strictly necessary and proportionate to the protection of national security and individuals did not have adequate means of judicial redress to protect their privacy. The concern that the intelligence services have overly broad surveillance powers may well also apply to the UK intelligence services. More clarity may come from three cases pending before the European Court of Human Rights, which were instigated by the UK Bureau of Investigative Journalism and a number of civil rights organizations, and claim that the generic surveillance powers of the UK intelligence services violate Article 8 of the European Convention on Human Rights.

Conclusions

In the short term, until the UK ceases to be a member of the EU, nothing changes and data transfers may continue as they currently do.

Whichever of the three options the UK follows to obtain the adequacy status, the end result will be UK data protection legislation which is very much aligned with the upcoming GDPR and other EU privacy rules.

Next steps for businesses

• While it is expected that the Commission will eventually confirm "adequacy status" for whatever data protection laws the UK puts in place post-Brexit, it is possible that this may not have been done at the precise time of exit. This situation would require businesses to put in place alternative data transfer arrangements for transfers from within the EU to the UK, such as the entering into of standard contractual clauses (SCCs). Controllers and processors can also "adduce appropriate safeguards" for their intra-group transfers by adopting binding corporate rules ("BCRs"). In any case, in the aftermath of the Schrems judgement, we see a trend of companies moving to implement BCRs in order to be less dependent on the adequacy decisions of the Commission and the negotiations of the EU and US in respect of the terms of the new Privacy Shield.

• Given the lead time it takes to implement the GDPR requirements into business processes, the advice to businesses in the UK is to continue their GDPR readiness programs. As indicated above, the rules that the UK will ultimately implement in all likelihood will closely resemble the GDPR. Note further that the GDPR may continue to apply to the data processing activities of UK companies where they offer goods or services to citizens in other EU countries, or otherwise monitor their behavior. The same will apply to UK companies with offices in other EU countries operating central data processing systems.

• The ICO has acted as the lead data protection authority ("DPA") in approving BCRs in many instances. After the exit, the ICO will no longer be authorized to act as lead DPA. Companies with BCRs where the ICO is lead DPA will therefore have to approach another EU DPA to act as their lead DPA. Businesses applying for BCRs and having to select a lead DPA and co-leads should be advised to take this into account.

Please do not hesitate to call with any question or concern you have. We're here to help.

Contact:

Lokke Moerel
44 (20) 79204054
lmoerel@mofo.com

Ronan Tigner
32 (2) 340-7358
rtigner@mofo.com

or

brexit@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 12 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.