BUREN
LEGAL | TAX | NOTARY

アラート　ＥＵ一般個人データ保護規則は２０１８年５月２５日に施行

２０１２年１月、欧州委員会はデータ保護改革を開始しました。ヨーロッパのデータ保護の現在の法的枠組みはＥＵ指令（the Directive 95/46/EC、以下「指令」といいます）ですが、各加盟国で異なる形で国内法化されかつ実施されているため、データ保護の水準は各加盟国によってばらついた状態になっています。

データ保護改革は、現在加盟国で異なっている国内法制をＥＵ内のどこであっても適用される統一的な法制に替えることによって、データが処理される個人（以下「データ主体」といいます）の権利を強化することを目指しています。また、この改革は、１つの準則を提供することによって、ビジネスを規制する環境を単純にし、行政の負担を軽減することを目指しており、多国籍企業にとってはワン･ストップ･ショップの導入によりデータ保護の監督機関相互の連携が容易になります。

一般データ保護規則（正式名称：個人データの処理及び当該データの自由な移動に係る自然人の保護並びに指令の廃止に関する規則、以下「規則」といいます）は、２０１６年５月２４日に成立しており、その施行は２０１８年５月２５日です。ＥＵ規則は加盟国に直接に適用されるため、施行によりオランダを含むすべてのＥＵ加盟国に直ちに適用されます。また、規則が自動的に適用されるため、加盟国による国内法化は必要ではありません。その結果、現在適用されている指令は廃止され、指令を実施する加盟国の現在の国内法の代わりに、規則が適用されます。オランダ・データ保護法（オランダ名：*Wet bescherming persoonsgegevens*）については、すべてまたはその多くがオランダ議会によって廃止されることになります。このため、規則は自然人に対してだけではなく、ビジネスにとっても大きな影響を及ぼすものとなります。

オランダでは、規則により導入される今回の変更の一部をすでに実施しています。２０１６年１月１日、オランダ・データ保護法が改正され、オランダ・データ保護法制に大きな変更が加えられました。改正により、データ漏えいを報告する管理者の義務が導入され、オランダ・データ保護機関の執行権限が拡大されるとともに、データ保護機関に対してこの新しい義務に違反がある場合に違反者に罰則を課す権限が付与されました。これら近時のオランダ・データ保護法の改正は、規則の適用によって管理者および処理者の義務がより広範になることを想定したものです。以前の弊事務所の記事でより詳細な改正の情報を紹介していますので、ご参照ください。
(http://burenlegal.nl/nieuws/2016/10/31/alert-%EF%BF%BD-de-meldplicht-bij-datalekken-487)

適用範囲

規則の適用範囲は、いくつかの例外を除き、現指令に類似しています。

規則は、自動化された手段による全部または一部の個人データの処理およびファイリング・システムの一部を構成するまたは一部を構成することを予定している個人データの自動化された手段以外の処理に適用されます（第２条）。純粋な個人または家庭内の活動における自然人によるデータの利用などについては規則は適用されないなど、適用範囲にはいくつかの制限があります。

また、個人データの定義の大半は、指令の定義と同じです。識別された又は識別可能な自然人に関する情報は、個人データとされます。この個人を特定し得る方法として、オンライン識別子や位置データが加えられました（第４条）。センシティブ・データという特別の範疇についての定義には、遺伝データおよび生体識別データが含まれています。

適用範囲の重要な変更としては、規則が管理者のみならず処理者に適用される点です。規則は、また処理行為の記録と処理をしたデータを保管するなどの特別な法的義務を処理者に課しています（第２

８条、３２条）。さらに規則は、処理者により広範な責任を課しています。しかし、今回処理者に新しい義務が課せられるようになったからといって、管理者の義務および責任が免除されるわけではありません。管理者はなお、義務を有しており、処理者との契約が十全に規則を遵守したものとなるようにしなければなりません。

場所的範囲

データ保護準則の場所的範囲は、規則では特に広くなっています。

第一に、規則は、ＥＵ内の管理者または処理者の事業所の活動における個人データの処理に適用されます。ＥＵ内で個人データの処理がなされているか否かは問いません（第３条）。「事業所」の定義は、現指令の定義と同じで、事業所の法的形態に関わりなく活動が実際に行われていることを意味します。
第二に、規則は、（ａ）管理者または処理者が、ＥＵ内でデータ主体に対し、料金の支払いの有無にかかわらず商品またはサービスを提供する場合、または（ｂ）管理者または処理者が、ＥＵ内のデータ主体の行動を監視している場合に、ＥＵ内に事業所を持たない管理者または処理者にも適用されます。これらの活動をする場合、管理者または処理者は、ＥＵ内に代表者を指名する義務があります（第２７条）。

管理者および処理者の責任

管理者は、個人データの安全を確保し、適切なデータ保護方針を実施するために、適切な技術的・組織的な措置を講じなければなりません。管理者は、処理が規則にしたがって行われていることを証明できなければなりません（第２４条）。

「プライバシー・バイ・デザイン」に関する条項は、個人データを利用する新しいビジネスの方法やサービスで管理者が上記の措置を実施することを求めています。「プライバシー・バイ・デフォルト」は、顧客が新しい製品を購入したりサービスを受けたりする場合に、最高度のプライバシーの設定が自動的に適用されることを求めています。このため、最高度のプライバシーの設定を適用するについて、データ主体の側の行為は必要とされません（第２５条）。

プロファイリングを含む自動化された決定に対し、データ主体は異議をとなえることができます。データ主体は、データ主体に対し法的効果を生じさせ、著しい影響を及ぼす、自動化された処理にのみ基づく決定の対象とならない権利を有しています（第２２条）。

データ処理がデータ主体の権利と自由に高い危険を生じさせるような場合（第３５条）、その処理の前にデータ保護影響評価が実施されなければなりません。この影響評価は、監督機関と協議の上実施されなければなりません。

データ主体を大規模に規則的・組織的に監視したり、または大規模に特別な種別のデータを処理したりする企業は、データ保護担当者を指定する義務があります（第３７条）。

同意

すべてのデータ処理は、データ主体の明確な同意に基づかねばなりません（第７条）。データ主体の同意は自由になされなければならず、特定され、十分な情報を知らされた上でなされ、不明確でないものでなければなりません。管理者は、同意があったことを証明できるようにしなければならず、データ主体は、同意を撤回する権利を有しています。

執行

国内監督機関（ＳＡ）は、規則の遵守を執行する職務を担います（第５１条）。各ＥＵ加盟国には、現在、データ保護機関があります。オランダでは、この機関はオランダ・データ保護機関（ＤＰＡ）といいます。現在のデータ保護機関が、新規則のための監督機関に組織変更されると思われます。

データ保護の不遵守に対する制裁金は、現在は国ごとで異なっていますが、規則によって決定されることになり、最大で２０００万ユーロまたは全世界の年間売上高の２－４％のいずれか高い方の額になります。

ワン・ストップ・ショップ

企業が多くの国に事業所を持ち活動をしている場合、様々な国内監督機関が同企業に適用される法的枠組みについて異なった解釈をする可能性があります。このリスクを避けるために、新規則の下で、いわゆる「ワン･ストップ･ショップ」が導入されました。多国籍企業については、ＥＵ内の主要な事業所の場所に応じて「第一監督機関」が指定されます。第一監督機関は、他のすべての監督機関と協議し、協力します。　（第６０条）　関連監督機関が決定に同意したならば、第一監督機関は、同決定を採択し、同決定はすべての関連監督機関を拘束します。管理者または処理者は、ＥＵ内のすべての所在地において、同決定を遵守しなければなりません。

データ漏えいの報告義務

データ漏えいを報告する一般的な義務は、オランダではすでに２０１６年に導入されており、新しい枠組みの下でもその多くが維持されます。データ漏えいがあった場合、すべての事案が、監督機関に報告されなければなりません。管理者は、不当に遅れることなく、可能であれば、漏えいを認識した後７２時間以内に漏えいの報告をしなければなりません。７２時間よりも遅く報告をする場合には、遅延の理由も付さねばなりません。漏えいがデータ主体の権利及び自由を脅かすようなものである場合には、漏えいをデータ主体に報告する義務があります（第３３条）。処理者は、漏えいを可能な限り早く管理者に通知する必要があります。監督機関に対する報告には、個人データの漏えいの性質、データ保護担当者の氏名及び連絡先詳細、予測しうる結果の説明を含めなければなりません。

その他留意点

規則は、ＥＵ全土の統一的なデータ保護の枠組みを導入するものです。しかし、加盟国は、義務を追加したり、国内監督機関に他の職務を付与したりすることができます。また、民事訴訟は国内裁判所で取り扱われるので、おそらく既存の国内判例法体系の中で、規則が適用され理由が付されることになります。

実務の観点からは、企業では仮名化または暗号化のような技術的な保護措置および有効なプライバシー方針を含むプライバシー遵守の枠組みを適切に確保することが重要です。さらに、規則を遵守しながら処理を行っていることを証明する書類を保存しておくことも重要です。