2016 年 11 月

Strict New Rules Under the EU Regulation on Personal Data Protection beginning *May 25, 2018*

An important new law, **European Regulation 2016/679** [i] on personal data protection, also known as the General Data Protection Regulation **(**the **"GDPR"),** was passed on **April 27, 2016** and will apply from ***May 25, 2018***, repealing the previous Directive 95/46/EC, in order to provide increased and harmonized protection for personal data within the European Union (EU). As a result, all EU members will share a single and common legal framework with respect to data security.

The GDPR creates numerous legal obligations and **onerous fines of up to *20,000,000 Euros*** *or* ***4% of an organization's total worldwide annual turnover,*** whichever is higher, in case of non-compliance, and will be applicable not only to companies within the EU but also to those in **Japan** as long as they target European consumers.

The European Practice Group of Kitahama Partners herein provides answers to certain commonly asked questions, and also provides certain practical recommendations, in order to enable readers to understand and prepare for this important new European law which will have global implications.

1. When applicable?

The GDPR takes effect on May 24, 2016, will apply from **May 25, 2018,** and is directly applicable to all EU member states without implementing national legislation.

厳格化する EU 新個人情報保護規則法制 2018 年 5 月 25 日に施行

欧州連合（EU）における個人情報の保護の強化統一のため、個人情報保護に関する新しく重要な**EU 規則 2016/679**[i]（以下、「GDPR」といいます。）が **2016 年 4 月 27 日**に可決されました。新規則は、従前の 95/46/EC 指令を廃止して、*2018 年 5 月 25 日*から適用され、個人情報保護に関して、EU 加盟国における単一で共通の法制度が誕生することになります。

GDPR は、多くの法的義務を予定しているだけでなく、違反者に対し *2 千万ユーロ又は全世界レベルの年間総売上高の 4%のいずれか高い方*を上限とする**重い制裁金**を予定しています。また、**GDPR** は EU 域内事業者だけでなく、ヨーロッパの消費者を対象とする**日本**の事業者にも適用されます。

北浜法律事務所のヨーロッパ・プラクティス・グループ（EPG）は、本稿で、全世界的に影響するこの重要な新法に関するよくあるご質問をとり挙げ、実務的なアドバイスをご提供いたします。読者の皆さまのご理解に少しでも資すれば幸いです。

1. 適用時期は？

GDPR は、2016 年 5 月 24 日発効、**2018 年 5 月 25 日**から適用となります。GDPR は国内法化を経ることなく全 EU 加盟国に直接適用されます。

【監修者】ヨーロピアンプラクティスグループ
＜メンバー＞
外国法事務弁護士　Jiri M Mestecky（代表パートナー）
弁護士　生田　美弥子　（代表パートナー）
弁護士　桶田　俊彦（スペシャルカウンセル）
弁護士　中　亮介／弁護士　松下　外／弁護士　酒井　裕

【執筆者】Alix D'ARJUZON, Avocat à la Cour　（France）

〖大　阪〗北浜法律事務所・外国法共同事業
〒541-0041 大阪市中央区北浜 1-8-16 大阪証券取引所ビル
TEL 06-6202-1088（代）／FAX 06-6202-1080･9550

〖東　京〗弁護士法人北浜法律事務所東京事務所
〒100-0005 東京都千代田区丸の内 1-7-12 サピアタワー14Ｆ
TEL 03-5219-5151（代）／FAX 03-5219-5155

〖福　岡〗弁護士法人北浜法律事務所福岡事務所
〒812-0018 福岡市博多区住吉 1-2-25
キャナルシティ・ビジネスセンタービル４Ｆ
TEL 092-263-9990／FAX 092-263-9991

http://www.kitahama.or.jp/

2. What is "Personal Data" under the GDPR?

Under the GDPR, the definition of personal data is very broad and includes any information relating to a natural person (data subject) who is identified or identifiable, directly or indirectly.

For instance, a name, an address, a fingerprint or an online identifier are personal data (Article 4(1)). A photograph of a person is also generally considered a personal data. Any combination of information which makes a natural person identifiable, such as physical or psychological characteristics, identification numbers, or factors specific to the economic, cultural or social identity of that person is also considered personal data.

2. GDPR に基づく「個人情報」とは？

GDPR の「個人情報」の定義は非常に広く、自然人（個人情報の主体）を直接間接に特定する又は特定し得るあらゆる情報を含みます。

例を挙げると、氏名や住所、指紋、オンライン識別子などは個人情報です（第 4 条第(1)項）。人物の写真も一般に個人情報に当たると解されます。自然人の身体的又は心理的特性や識別番号、経済的、文化的又は社会的背景等の自然人を識別可能とする情報の組み合わせもまた、個人情報に該当します。

3. Which companies have to comply with the GDPR?

The GDPR applies to controllers [ii] and processors [iii] established in the EU which process personal data (wholly or partly by automated means or by using part of a filing system) in the context of their activities, regardless of whether the processing takes place in the EU or not (Article 3.1).

A significant change for companies in Japan is that the GDPR extends the scope of applicability under Article 3.2 to controllers and processors established outside the EU, such as Japan, where their processing activities are related to:

- *the offering of goods or services to data subjects who are in the EU, irrespective of whether payment by the data subject is required; or*
- *the monitoring of the behaviour of European data subjects, to the extent their activities take place within the EU.*

Therefore, in such cases, Japanese companies must comply with the provisions of the GDPR.

3. GDPR の適用対象となる事業者とは？

GDPR は、EU 域内に拠点を持ち、個人情報（の全部又は一部）を、（自動化された手段で、又はファイリングシステムの一部を使用して）その業務の中で処理する管理者 [ii] 及び処理者 [iii] に適用され、その処理が EU 域内で行われているか否かは問われません（第 3 条第 1 項）。

日本の事業者にとって、以前との大きな違いは、GDPR 第 3 条第 2 項が、適用範囲を日本のような EU 域外で設立された管理者及び処理者にまで拡張した点です。但し、その処理業務が以下のどちらかに関連する場合に限られます。

- *有償無償を問わず、EU 域内に所在する個人情報の主体に対する物品又はサービスの提供*
- *EU 域内で活動するヨーロッパの個人情報の主体の行動のモニタリング*

従って、上記に該当する日本の事業者は、GDPR を遵守しなければなりません。

4. What are the concrete legal changes?

Unlike Directive 95/46/EC, the GDPR will be directly applicable to all EU member states and replaces the Directive which was adopted into the national legislation of each member state in order to protect the fundamental rights and freedoms of natural persons.

4. 具体的な法改正の内容は？

95/46/EC 指令と異なり、GDPR は、全 EU 加盟国に直接適用されます。GDPR は、自然人の基本的権利及び自由を保護するため、95/46/EC 指令に基づいて各加盟国が採択した国内法に取って代わるものとなります。

The common legal framework provided by the GDPR will ensure more transparency and legal foreseeability and encourages the free flow of personal data throughout the EU.

GDPR は、共通の法的枠組みを提供します。このことにより透明性と法的予見可能性が確保され、EU 全域において個人情報の自由な流通が促進されることになります。

More specifically, as explained below, the GDPR mainly: (1) reinforces data subjects' rights; (2) increases the responsibilities and the accountability of companies processing personal data; and (3) establishes a simplified and centralized system of control.

GDPR は、より具体的に以下に説明いたしますが、(1)個人情報の主体の権利の強化、(2)個人情報処理事業者の責任の加重と説明責任の加重、(3)簡易でかつ一元的な管理システムの構築、といったものを実現することになります。

4.1 Reinforcement of data subjects' rights

4.1 個人情報の主体の権利の強化

Some of the main rights of data subjects under the GDPR are the following:

GDPR に基づく、個人情報の主体に認められる主な権利としては、以下が挙げられます。

- **Right to give informed consent and withdraw same at any time**. Where personal data processing is based on a data subject's consent, a request for consent must be presented in an intelligible and easily accessible form, and it must be equally simple for the data subject to **withdraw** such consent as it is to give it. Furthermore, the processing of special categories of data[iv] requires a consent given by a **clear affirmative action** from the data subject; and the processing of a **child**'s personal data requires a parental authorization when the child is less than 16 years of age (default age limit);

- **同意権、撤回請求権** 個人情報の処理が個人情報の主体の同意に根拠づけられる場合、かかる同意は、明瞭かつ容易に入手可能な様式で求められなければなりません。また、かかる同意の**撤回**も、同意と同レベルに容易でなければなりません。さらに、特種な個人情報 [iv] の処理には、個人情報の主体の**積極的かつ明示的な**同意が必要です。**子ども**の個人情報の処理には、子どもが 16 歳未満(基本的年齢制限)であれば、親の許可が必要です。

- **Right to access**. The data subject must have the right to access his/her personal data and the right to obtain other information, such as the purposes of the processing and an explanation about his/her rights;

- **アクセス権** 個人情報の主体は、自己の個人情報にアクセスする権利を有し、当該情報の処理目的や自己の権利について説明等を受ける権利を有します。

- **Right to rectification**. The data subject has the right to request that the controller rectify any inaccuracy in his/her personal data without undue delay;

- **訂正請求権** 個人情報の主体は、自己の個人情報に不正確な点がある場合、管理者に対して遅滞なく訂正することを求める権利を有します。

- **Right to erasure**. In certain circumstances, the data subject may request the controller erase his/her data without undue delay, for example, when the data subject wants to withdraw his/her consent, when the data is no longer necessary, or when that data has been unlawfully processed. In

- **消去請求権** 一定の場合には、個人情報の主体は、自己の個人情報を、管理者が遅滞なく消去するよう求めることができます。例えば、個人情報の主体が同意の撤回を希望するとき、当該個人情報がもはや必要でなくなったとき、個人情報が違法に処理されたときなどが挙げられます。該当する場合には、個人

such cases, when the data subject requests erasure of his/her personal data, the controller must send the request for erasure to all of the companies that are processing or have processed the relevant personal data;

情報の主体から消去を求められた管理者は、当該個人情報を処理中の事業者のみならず、過去の全事業者に対しても消去要求を送付しなければなりません。

- **Right to data portability**. When the personal data processing is carried out by automated means and based on consent, the data subject may ask the controller to provide his/her personal data in a structured and commonly used format in order to easily transfer such data from one controller to another;

- **データ移行請求権** 個人情報の処理が同意に基づいて自動処理されているとき、個人情報の主体は、管理者に対し、自己の個人情報を、管理者から管理者へ容易に移転提供できるような一般的な使用形式に加工して提供するよう求めることができます。

- **Right to be informed of data breach**. When a data breach is likely to cause a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach to data subjects without undue delay; and

- **データ侵害の通知の受領権** 個人情報の侵害により自然人の権利及び自由に甚大な侵害が発生する可能性があるとき、管理者は、個人情報の侵害を、遅滞なく個人情報の主体に伝えなければなりません。

- **Right to object to profiling**[v]. Where personal data is processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data, which includes profiling related to such direct marketing.

- **プロファイリングに対する異議申立権** 個人情報がダイレクトマーケティングの目的で処理される場合に、個人情報の主体は、かかるダイレクトマーケティングに関連するプロファイリングを含む自己の個人情報の処理に対し、いつでも異議を申し立てることができます。

While such rights substantially increase the obligations of the companies processing personal data, it is important to bear in mind that a data subject **cannot invoke a majority of these rights** once the data has been anonymized by the controllers. Indeed, if the controller is able to demonstrate that it can no longer identify the data subjects, the rights to access, rectification, erasure and data portability mentioned above do not necessarily have to be respected.

なお、これらの権利は、個人情報を処理する事業者の義務を大幅に加重するものですが、いったん個人情報が管理者によって匿名化されると、個人情報の主体は**これらの権利の大半を行使できなくなる**ことに留意が必要です。実際、管理者が、個人情報の主体が特定できないことを示した場合には、上記のアクセス権、訂正請求権、消去請求権、データ移行請求権を尊重する必要はなくなります。

4.2 Increasing controllers and processors' responsibilities

4.2 増大する管理者及び処理者の責任

Under the GDPR, controllers no longer have the obligation to notify or seek approval from national supervisory authorities [vi] in many circumstances, but instead bear heavy accountability and obligations to demonstrate compliance with the GDPR. Furthermore, for the first time, processors also have direct obligations. The main obligations of the controllers and processors are the following:

GDPR が導入されると、大半の管理者の国の監督当局[vi]に対する通知義務や承認請求義務がなくなりますが、その代わりに GDPR に基づく重い説明責任や遵守義務が課されます。さらに、GDPR によって今回初めて、処理者に対しても直接義務が課されることになりました。管理者及び処理者の主な義務は、以下のとおりです。

- **Data protection impact assessments.** When a type of personal data processing may result in a high risk to the rights and freedoms of data subjects, controllers must carry out a data protection impact assessment to evaluate the likelihood and severity of the risk. In case of high risk, controllers must consult with supervisory authorities prior to the processing of personal data;

- **個人情報保護の影響評価** ある種類の個人情報処理が個人情報の主体の権利と自由に大きなリスクをもたらす結果となる可能性があるときには、管理者は、そのリスクが顕在化する可能性とその重大性を評価すべく個人情報保護の影響評価を行わなければなりません。また、そのリスクが大きい場合には、管理者は、個人情報を処理するに先立って監督当局に相談しなければなりません。

- **Data protection by design and by default.** Controllers must implement technical and organizational measures, such as using pseudonyms, designed to comply with data protection principles and they must integrate such safeguards into the processing of personal data. They also have to ensure that, by default, only specific personal data which is necessary for the purposes of the processing is actually processed;

- **個人情報保護バイ・デザイン及びバイ・デフォルト** 管理者は、個人情報保護の原則を遵守するため、仮名匿名を使用する等、技術的かつ組織的措置を施すなど、個人情報の処理に際して保護措置を取る必要があります。また、原則として、情報処理の目的に必要な特定の個人情報だけを処理するようにしなければなりません。

- **Adoption of codes of conduct.** Controllers will have to demonstrate that their processing systems are in compliance with the new GDPR, notably by adopting codes of conduct or certification mechanisms;

- **行動規範の採択** 管理者は、行動規範規則や認証メカニズムの採択等により、その情報処理システムが新 GDPR を遵守していることを示す必要があります。

- **Fair processing notice.** Controllers must provide data subjects with much more detailed information at the time their personal data is acquired, such as information regarding data subjects' rights and the period for which data will be stored;

- **公正な処理の通知** 管理者は、個人情報の主体の個人情報を入手した時点で、個人情報の主体の権利に関する情報や、個人情報の保持期間といったより詳細な情報を、個人情報の主体に対し、提供しなければなりません。

- **Records of processing activities.** Controllers and processors must compile and maintain a written record, containing specific information, of their personal data processing activities;

- **処理活動の記録** 管理者及び処理者は、具体的な個人情報処理活動記録を書面でまとめ、これを保管しなければなりません。

- **Data breach notification.** Controllers must notify supervisory authorities, where feasible, within 72 hours of becoming aware of any personal data breach which can result in a risk to the rights or freedoms of natural persons. Processors must also notify controllers after becoming aware of any data breaches; and

- **個人情報侵害の報告** 管理者は、自然人の権利と自由が脅かされる結果となり得る個人情報の侵害を認識した場合、可能な限り、72 時間以内に監督当局にその旨を報告しなければなりません。処理者もまた、個人情報の侵害を認識した場合、管理者に報告しなければなりません。

- **Joint responsibility.** For the first time, when several companies jointly determine the purposes and means for the processing of personal data, they

- **共同責任** 事業者が複数で個人情報の処理の目的と手段を定めたときは、複数事業者がその処理に共同で責任を負うことが初めて定められました。

will all be jointly responsible for such processing.

4.3 Establishment of a more efficient control system

Under the GDPR, the system for the control of personal data has been simplified and centralized by the following measures:

- **Designation of a Data Protection Officer (DPO).** Data controllers and processors must designate a DPO in certain cases[vii]. The DPO may be an employee of the controller or processor but must act with full independence to inform and advise the controller or processor and its employees of their obligations and to monitor compliance with the GDPR. The DPO must also cooperate with supervisory authorities and inform data subjects with regard to all issues relating to the processing of their personal data.

- **Designation of a representative in the EU**. Companies not established in the EU which often process personal data or which process special categories of data on a large scale must designate a representative in the EU that will constitute a direct contact for supervisory authorities and data subjects.

- **Competence of a leading supervisory authority**. The national supervisory authority of the primary entity associated with the controller or the processor will act as the lead supervisory authority for cross-border processing of personal data.

- **Establishment of a European Data Protection Board (EDPB).** The EDPB will primarily be in charge of issuing opinions, resolving disputes, reporting to the Commission of the EU, and promoting cooperation among national supervisory authorities.

5. What are the sanctions in case of non-compliance?

One critical new aspect of the GDPR is the significant increase in administrative fines from the supervisory authorities, which can be up to:

4.3 効率的な管理体制の構築

GDPR の下では、個人情報の管理体制は、以下の措置によって簡易でかつ一元的なものとなりました。

- **個人情報保護責任者の指名** 個人情報の管理者及び処理者は、一定の場合[vii]には、個人情報保護責任者を指名しなければなりません。個人情報保護責任者は、管理者や処理者の従業員でも構いませんが、完全に独立の立場から、管理者や処理者及びその従業員に対し、その義務について通知し、GDPR の遵守状況を監視しなければなりません。また、個人情報保護責任者は、監督当局に協力し、個人情報の主体に、その個人情報の処理に関するあらゆる問題について報告しなければなりません。

- **EU 域内における代理人の指名** EU 域内に拠点を持たない事業者が、個人情報を頻繁に処理するか、特別な種類の個人情報を大量に処理する場合には、監督当局及び個人情報の主体との間の直接の連絡窓口となる EU 域内代理人を指定しなければなりません。

- **主たる監督当局の管轄権** 個人情報の越境処理については、管理者又は処理者が関係する主要主体を管轄する加盟国の監督当局が、主たる監督当局となります。

- **欧州個人情報保護委員会の設立** 欧州個人情報保護委員会は、主に意見の公表、紛争解決、欧州委員会への報告、国家監督当局間の協力の促進を担当します。

5. 違反の場合の制裁は？

GDPR の重要な新たな特徴のひとつに、監督当局が課す制裁金の大幅な増額があります。その制裁金の上限は、以下のとおりです。

- **10,000,000 Euros or 2% of the total worldwide annual turnover,** whichever is higher, for the preceding financial year of the company, for a majority of violations; or

- **20,000,000 Euros or 4% of the total worldwide annual turnover,** whichever is higher, for the preceding financial year of the company, for the most serious violations.

- 大半の違反について、**1000 万ユーロ又は事業者**の前会計年度の**全世界年間総売上高の 2%のいずれか高い方**、又は

- 最も重大な違反について、**2000 万ユーロ又は事業者**の前会計年度の**全世界年間総売上高の 4%**のいずれか高い方

To compare, prior to the GDPR, the French supervisory authority could only give fines up to 3,000,000 euros.

比較すると、GDPR 制定前は、フランスの監督当局の制裁金の上限は 300 万ユーロでした。

In addition to these onerous fines, under the GDPR, data subjects may institute **civil litigation** against controllers and processors in the event they believe that their rights have been infringed.

このような重い制裁金の他に、GDPR の下では、個人情報の主体は、自己の権利が侵害されたと判断した場合に、管理者及び処理者を相手取って**民事訴訟**を提起することができます。

Therefore, given the severity of the sanctions, controllers and processors must pay particular attention to, and strictly comply with, the GDPR and its provisions.

以上のことから、制裁の厳格化を考慮して、管理者及び処理者は、GDPR の規定に特に注意し、これを遵守しなければなりません。

6. Our recommendations in anticipation of these legal changes

6. 法改正への対応策

As a majority of the above legal changes take time to be integrated into a company's personal data processing system, we strongly advise that companies begin planning as quickly as possible.

上記に述べた法改正の大半は、各事業者の個人情報の処理システムの中に組み込むには時間を要するものばかりですので、対策にはできる限り速やかに着手されるべきかと存じます。

Our specific recommendations are as follows:

お勧めする具体的な対応策は、次のとおりです。

- Confirm whether your company meets the conditions to be subject to the GDPR.

- 貴社が GDPR の適用対象か否かを確認する。

- Analyze the legal basis upon which your company processes personal data (data subject's consent, legitimate interest, etc.) and the type of personal data collected (special categories of data or not) in order to determine the legal obligations with which your company will have to comply;

- 遵守すべき法的義務を明確化すべく、貴社が個人情報を処理する際の法的根拠（個人情報の主体の同意、その他の法的根拠）や収集した個人情報の種類（特別な種類の個人情報か否か）を分析する。

- Verify that the purposes for which your company processes personal data necessitates the identification of data subjects and try to limit as much as possible this identification in order to reduce the possibility that data subjects will object;

- 貴社が個人情報を処理する上で個人情報の主体の特定が必要かどうか確認し、個人情報の主体からの異議の機会を減らすべく、その特定の程度をできるだけ制限するようにする。

- Review your personal data processing notices and codes of conduct;
- 個人情報の処理通知手続や行動規範規則を見直す。

- Train your employees so that they can comply with their new obligations under the GDPR;
- 従業員が GDPR 上の新たな義務を遵守するよう教育・訓練する。

- Check whether your company has to designate a DPO and/or a representative in the EU;
- 個人情報保護責任者又は EU 域内の代理人を指名しなければならないかを確認する。

- Prepare the implementation of personal data privacy by design and by default, in order to streamline personal data processing and build safeguards;
- 個人情報の処理を効率化し、保護措置を構築するため、個人情報のプライバシー・バイ・デザイン原則及び個人情報のプライバシー・バイ・デフォルト原則の実施の準備をする。

- Assess the privacy impact of your personal data processing activities;
- 貴社の個人情報処理活動のプライバシーへの影響を評価する。

- Be aware of data subjects' rights and take appropriate measures to eventually request proper consent from data subjects and enable data subjects to withdraw their consent or request the erasure of their data;
- 個人情報の主体の権利を認識し、将来的に個人情報の主体に適切な同意を求め、また個人情報の主体が同意を撤回したり、個人情報の消去を求めたりできるような適切な措置を講じる。

- Implement procedures enabling your company to react quickly in the event of data security breaches;
- 情報セキュリティの侵害があった場合に、迅速に対応できる手順を準備する。

- Identify the organizational and technical measures that will enable your company to demonstrate compliance with the GDPR to authorities; and
- GDPR を遵守していることを当局に示せるように組織的かつ技術的措置を特定しておく。

- Clarify the obligations of each company that could be jointly involved with your company in the processing of personal information in order to avoid the risk of unforeseen joint responsibility.
- 想定外の共同責任のリスクを避けるため、貴社が共同で個人情報の処理に関与する可能性のある各社の義務を明確にする。

The above steps are some examples of measures that can be taken **now** within your company in order to anticipate and ensure compliance with the GDPR.

上記の対応策は、GDPR 適用を見越してこれを確実に遵守するために、貴社が**現在**社内で講じ得る施策の一例です。

Experts in our firm's European Practice Group remain at your disposal to provide you with further information regarding the GDPR and to give you further advice regarding the implementation of measures in accordance with the GDPR.

弊所のヨーロッパ・プラクティス・グループの弁護士が、必要に応じて、さらなる GDPR 関連情報や、GDPR に従った対応策に関してさらにアドバイスさせて頂きますので、どうぞご相談ください。

[i] Regulation (UE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

[i] 個人情報の処理に係る自然人の保護及び当該個人情報の自由な流通並びに欧州共同体 1995 年 46 号指令の廃止に関する 2016 年 4 月 27

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

[ii] "Controller" means a natural or legal person who determines the purposes and means of the processing of personal data.

[iii] "Processor" means a natural or legal person which processes personal data on behalf of the controller.

[iv] Special categories of personal data are specified in Article 9 of the GDPR and concern personal data revealing racial or ethnic origin, political opinions, and religious or philosophical beliefs…

[v] Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person.

[vi] The supervisory authorities are the independent public authorities established in each Member State to monitor the application of the GDPR. Please find hereafter the link to access to the list of all data protection authorities:
http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[vii] The DPO shall be designated in any case where: (i) the processing is carried out by a public authority; (ii) the core activity consists of processing operations which require regular and systematic monitoring of data subjects on a large scale; or (iii) the core activity consists of large scale processing of special categories of data (racial origin, political opinion, etc.), or of data relating to criminal convictions and offences.

日付欧州議会及び理事会の 2016 年 679 号個人情報保護規則
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

ii「管理者」とは、個人情報の処理の目的及び手段を決定する自然人又は法人をいいます。

iii「処理者」とは、管理者のために個人情報を処理する自然人又は法人をいいます。

iv 特別な種類の個人情報は、個人情報保護規則の第 9 条に特定されており、民族的素性、政治的思想及び宗教的又は哲学的信条等を明らかにする個人情報に関するものです。

v プロファイリングとは、自然人の一定の個人的な側面の評価を目的とした、個人情報の使用から成るあらゆる形態の個人情報の自動処理をいいます。

vi 監督当局は、個人情報保護規則の適用を監視するために各加盟国で設立された独立した公共機関です。全ての個人情報保護機関の一覧表は、こちらのリンクでご覧ください。
http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

vii 個人情報保護責任者は、(i)個人情報の処理が公共機関により行われる場合、(ii)個人情報処理の中心的な活動が、大量な個人情報の主体の定期的かつ系統立った監視を要する処理業務から成る場合、又は(iii)個人情報処理の中心的な活動が、特別な種類の情報（民族的素性、政治的思想等）や犯歴に関する情報の大量の処理から成る場合に指名するものとされています。