JEITA 一般社団法人 電子情報技術産業協会
Japan Electronics and Information Technology Industries Association

平成 24 年 12 月

一般社団法人 電子情報技術産業協会
法務・知的財産権委員会
個人情報保護専門委員会
ＥＵデータ保護対応検討会

EU データ保護規則案に対する JEITA 意見書について

今般、当検討会では、情報政策委員会／国際活動ＷＧと連携し、EU データ保護対応 訪欧ミッションを 2012 年 11 月 8 日(木)から 11 月 14 日(水)にかけて派遣し、欧州関係先を訪問の上、JEITA の意見を説明するとともに、意見交換を行いました。

【資料】

・日本語_JEITA 意見書最終版 120927
・JEITA 意見書抜粋版（日本語）120927
・English_JEITA 意見書最終版 120927
・JEITA 意見書抜粋版（英語）120927

EU データ保護規則案に対する JEITA 意見書

2012 年 9 月 27 日
一般社団法人 電子情報技術産業協会

※**青字太字**は EU への要望に当たる箇所。

1．はじめに

1．1　JEITA の概要

- JEITA は、素材から電子部品や半導体、また、民生電子製品から産業システム機器、さらには、IT 製品からソリューションサービス等を含む日本の代表的な電子情報産業の業界団体である。
- 約 400 社の会員企業の事業は広くグローバルに展開されており、事業規模は日本国内約 14 兆円、海外約 26 兆円である。その中で、欧州は、研究開発、生産、販売、サービス提供等の事業拠点として、重要な位置を占めており、多くの拠点が設置されている。
- 欧州とそのような緊密な関係にある日本の電子情報産業界の企業にとって、今年 1 月に公表された EU データ保護規則案（the Proposed EU Data Protection Regulation）は、在欧の日本の現地法人も含め、我々日本企業にも直接影響のある規則であり、当該規則案に対して JEITA としての意見を述べさせて頂ければ幸いである。

1．2　データ保護に関する JEITA の基本的スタンス

- インターネットの普及や ICT 技術の進歩を背景に、多くの企業がそれらを活用し生産性の向上を図るとともに、イノベーションを創出し、人々に新たな価値を提供している。また公共部門においても同様に、国民に新たなサービスを提供したり、業務の効率化を図るなど、利便性の向上という価値を生み出している。さらには近年急速に普及している SNS は、新しい人と人の繋がりを生み出し、様々な形のコミュニティを形成している。
- しかし他方、大量のデータが国境を越えて流通する時代を迎えたことで、データの漏洩、とりわけ個人に関わるデータの漏洩やプライバシーの侵害というリスクが増大していることも事実である。このような個人データを取り巻く環境変化を受けて、今般欧州委員会において、1995 年に採択されたデータ保護指令の見直しがなされ、新たにデータ保護規則案が提示されたことは時宜を得たものと考える。
- 個人データの保護と活用の問題は各国の歴史・文化の違いや国民の受け止め方の差異などから、長年にわたり、それぞれの国、地域、また OECD 等の国際機関の場で様々な議論が行われてきているが、近年ではデータ保護の諸原則は全世界的に収斂（converge）しつつあると考えられる。このような国際的な潮流を踏まえれば、個人データ保護のためには(1)個人の権利の保障、(2)企業・組織の責任（responsibility/accountability）、(3)監督機関（supervisory authorities）による執行（enforcement）という 3 つの要素が重要であり、日本においてもこのような観点から個人データ保護フレームワークを見直していくことが必要だと認識している。
- 今般公表されたデータ保護規則案を見ると、個人データ保護の権利を強化するとともに、EU 加盟国ごとに法律が異なるために生ずる弊害の除去や、個人データ処理に係る監督機関への通知義務（general notification requirements）の廃止など、欧州域内で広く事業を展開する企業にとっても高く評価できる内容となっている。しかしながら、EU 居住者のデータ保護の観点から、企業に新たな責務が課されることとなり、運用方法によっては規則案を遵守するために産業界に新たなコスト負担が発生し、結果として欧州委員会が言及するような全体のコスト削減につながらない恐れがある。また、規則案では商品やサービスを提供する EU 居住者（data subjects residing in the Union）のデータを EU 域外で処理する場合にも管理者（controller）に EU 規則を適用するというルールも追加された。
- **人、物、金、情報といった経営資源が国境を越えて流通する時代における企業活動において、グロー**

バルなデータ保護のルールは、第一に解りやすく透明であること、第二に国内外を問わず公平であり調和が取れていること、第三に実行可能であり実効性があること、第四に企業活動を過度に抑制したり企業に過剰な負担を強いるものではないことが求められる。今般、欧州委員会からデータ保護規則案が提案されたことを機会に、以上のような観点から各国間または国際機関の場で関係者による議論が活発に行われ、現代の社会環境に適合した個人データの保護と活用に関する国際的なフレームワークが形成されていくことを期待したい。

２．EU データ保護規則案に対する JEITA の意見

２．１　個人データの第三国移転（transfer of personal data to third countries）について（第５章）

①第三国移転と十分性決定（第 39 条、第 41 条、第 42 条関連）

- 規則案第 41 条では、第三国（third country）内の特定の処理分野（processing sector）に対する十分性決定（adequacy decision）も可能とされており、これは望ましいことである。日本の民間企業は、個人情報保護法による規制に加え、各所管省庁の個人情報保護ガイドラインに基づき、個人データの安全管理措置を講じている。日本の業界団体としても、日本の民間分野が「十分なレベルの保護」を保証していることを欧州委員会に理解してもらうべく、ぜひ日本国、または民間分野や特定産業分野としての十分性決定に向けた取組みを行っていきたい。
- ただし、仮に日本政府から欧州委員会に十分性評価の申請を行うとした場合でも、最終的に十分性決定を得るためには相応の時間を要すると考えられるので、日本企業は当面、標準契約条項（standard data protection clauses）や BCR（拘束的企業準則：binding corporate rules）に基づいて、EU 域内の管理者（日本企業の現地法人を含む）から個人データ移転を受ける必要がある。標準契約条項は、欧州委員会または監督機関によって採択されたものについては、第 42 条第 3 項で「更なるオーソライズを必要としない」と規定されているため、日本企業が標準契約条項を利用する際に監督機関による更なる承認等の手続きは必要ないと解釈でき、従来よりも手続きが簡素化されると考えられる。このように EU 規則案において標準契約条項や BCR の手続きが簡素化されたのは、望ましいことである。
- しかし、EU 域外企業が EU 域内管理者からのデータ移転にあたって、個別に当該管理者と標準契約条項を締結することは、EU 域内管理者にとって負担と受け取られる可能性があり、これは域外企業のビジネス機会の損失を助長する可能性がある。日本企業にとっても、とりわけクラウドサービス事業者等にとってマイナスとなる。
- 日本には「プライバシーマーク」というデータ保護シール（data protection seal）制度が存在し、既に 12,000 社以上が認証（certification）を受けている。プライバシーマークの準拠基準である JISQ15001「個人情報保護マネジメントシステム-要求事項」は、通商産業省（現経済産業省）が 1997 年にEUデータ保護指令に基づき改訂した「民間部門における個人情報保護のためのガイドライン」を母体とするものである。そのため、プライバシーマークの認証を受けた日本の事業者は、「十分なレベルの保護（an adequate level of protection）」に準じるような適切な安全管理措置（appropriate safeguards）を講じていると、我々は考えている。このような日本のプライバシーマークと、第 39 条にいう欧州レベルのデータ保護シールとの相互承認（mutual recognition）が行われた場合には、プライバシーマークの認証を受けているということが、第 42 条第１項にいう「適切な安全管理措置」に該当するようにしてほしい。
- または、プライバシーマーク等のデータ保護シールの認証を受けることは、第 41 条第１項にいう第三国内の特定の処理分野に対する十分性決定の条件の１つとなると考えられるが、もしそうなのであれば、第 41 条第２項の中にデータ保護シールに関する記述を追加するなど、条文の中でその旨を明示してほしい。
- グローバルで活動する企業は、国境を越えて消費者の個人データを処理する機会がますます増えているため、このようなデータ移転に関して、二国間のみならず、マルチリージョン間で調和され、統一

された移転方法を必要としている。このような観点から、中長期的にはデータ保護に関する国際基準が整備され、EUにおける十分性決定（第 41 条）や適切な安全管理措置（第 42 条）との調和が図られることが望ましい。

②従業員データの第三国移転（第 44 条関連）

- 日本企業では、従業員データのみに限って、雇用契約の履行等の正当な目的でEU域内の現地法人から日本の本社に移転するケースが多い。このようなデータ移転においては、個人の権利が侵害されるリスクは低いと考えられるため、標準契約条項やBCRよりも簡易な移転方法として、例えば本人（data subject）がデータ移転について同意（consent）した場合も可能であることを明示してほしい。
- 本人が同意した場合にデータ移転が可能であること自体は第 44 条第 1 項(a)号で規定されているが、我々が危惧するのは、第 7 条第 4 項で「データ主体と管理者の地位の間の従属関係に重大な不均衡が存在する場合には、同意は処理のための法的根拠を与えないものとする」と規定されており、前文（whereas clauses）の（34）項では「同意は、データ主体と管理者の間に明確な不均衡が存在する場合には、個人データ処理のための有効な法的根拠を与えない。このことは、とりわけデータ主体が管理者に依存する状況にあるとき、特に雇用の関係において被用者の個人データを雇用者が処理する場合に該当する」とされているため、従業員からの同意を得ることが雇用者が従業員データを第三国に移転することの法的根拠とならない恐れがある点である。

２．２　EU 規則の域外適用について（第３条第２項）

①域外適用の除外条件

- インターネット上で提供されるサービスの発展によって、現行の EU データ保護指令の第 4 条第 1 項(c)号にいうように EU 域内の設備（equipment）でデータ処理（processing）を行う場合のみ EU 域外の管理者を EU 法の対象とすることが、EU 居住者のデータ保護にとって不十分となったことは十分に理解できる。
- しかし、例えば、日本企業が開設する日本語のショッピングサイトで、たまたまEU居住者（EU在住の日本人を含む）が商品を購入した場合、あるいは日本企業が開設する日本語のソーシャルネットワーキングサイトでたまたまEU居住者が会員となった場合、これらの日本企業が第 3 条第 2 項の適用対象となってしまうのは合理的ではない。もちろん、このような場合には適用対象とならないと考えられるが、どのような場合に第 3 条第 2 項が適用され、どのような場合に適用されないかが明確でないとEU域外企業にとって法的な不確実性が高い。したがって、例えば商品やサービスの提供範囲にEU加盟国が含まれない旨をサイト上で明示している場合は適用対象とならないなど、EU域外企業が第３条第２項の適用対象とみなされないための条件を明確化してほしい。

２．３　個人データの定義について（第４条(1)(2)）

- EU 規則案における「個人データ（personal data）」の定義では、現行の EU 指令と比較し、個人識別手段の例として「位置データ（location data）」と「オンライン識別子（online identifier）」が追加されている。また、EU 規則案の前文（whereas clauses）の(24)項では「識別番号、位置データ、オンライン識別子（IP アドレスやクッキー等）、その他の特定の要素は、それ自体として、全ての環境において必ずしも個人データとみなされる必要はない」と説明されており、場合によっては、これらのデータが単独で個人データとみなされる可能性があることが示唆されている。
- 民間企業が IP アドレス、クッキー等のオンライン識別子を個人に関連付けて管理している場合、たとえ当該企業が当該個人の氏名を収集・保存していなかったとしても、オンラインで個人を追跡したりプロファイリングすることが可能であるため、このようなデータが保護対象となりうることは良く理解できる。
- しかし EU 規則案では、こうした位置データ、IP アドレス、クッキー、もしくはその他のオンライン

識別子（PC やスマートフォンの端末 ID 等）が、どのような場合に個人データとみなされるかについて、明確に定義されていない。

- 「個人データ」の定義は、EU 規則案で規定する管理者（や処理者）の義務全体に関わる事柄であり、例えばあるデータが「個人データ」とみなされるか否かによって、それらのデータに対する安全管理措置（第 30 条）や、忘れられる権利（第 17 条）への対応、個人データ違反時の報告・連絡（第 31 条、第 32 条）、監督機関による課徴金（第 79 条）等は大きく異なってくる。そのため、個人データの範囲が明確でないことは、民間企業の事業活動の上で大きな法的不確実性をもたらす。
- 民間企業の立場からは、識別番号、位置データ、オンライン識別子等の「グレー」なデータがどのような場合には個人データとみなされないか、すなわち管理者や処理者があるデータに対してどのような措置を行っていれば当該データの処理にあたって個人データとして保護することの義務を免除されるかを明確化してほしい。
- 例えば、米国の連邦取引委員会が本年 3 月に公表した報告書「Protecting Consumer Privacy in an Era of Rapid Change」では、保護対象となるデータを「特定の消費者、コンピュータ、又はその他の端末に無理なくリンク可能なデータ（data that is reasonably linkable to a specific consumer, computer, or other device）」 とし、企業が「(1)データが脱識別化（匿名化や仮名化）されたことを保証する合理的な措置を取っている、(2)当該データを再識別化しようとしないことに公的にコミットメントしている、(3)データ受領者が当該データを再識別化しようとすることを契約上で禁止している」という 3 つの条件を満たせば当該データは「無理なくリンク可能なデータ」ではない（data is not “reasonably linkable” to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to reidentify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data）と定義している。このような定義は、民間企業にとって大変に分かりやすいものである。

２．４　処理の合法性とポリシーの透明性について（第 6 条、第 7 条、第 11 条）

①ポリシーの透明性と本人同意（第 4 条(8)、第 6 条第 1 項、第 7 条、第 11 条）

- EU 規則案において、民間企業等のプライバシーポリシーが煩雑で分かりにくい現状を踏まえ、第 11 条で管理者に対して新たに「透明性（transparency）」の義務を追加したこと、また、プライバシーポリシーが分かりにくいため本人の同意が形式的なものに陥っている現状を踏まえ、第 4 条(8)と第 7 条第 1 項・第 2 項で管理者に対して明示的な同意（explicit consent）を取得することの義務、また第 7 条第 3 項で同意を撤回できる権利を保障する義務を追加したことは十分に理解できる。
- しかし、民間企業のデータ・プラクティスはますます複雑化し、消費者に取って見えにくく分かりにくいものになっているため、プライバシーポリシーを詳しく書けば書くほど、消費者にとっては読みにくく、面倒なものになり、逆に、ほとんど内容を読まずに機械的に「同意」してしまうことになりかねない。また、そのような機械的な同意を避けるためには、個人に対してあらゆるケースでプライバシーポリシーをよく理解した上での明示的な同意を求めることが必要となるが、このことはかえってサービス利用時に個人に多大な負担をかけ、利便性を妨げることになる。本人（data subject）の同意を尊重し、個人の権利を守ろうとすればするほど、個人にとっての負担が大きくなるというジレンマを解決する手段を見出さなければならない。
- プライバシーポリシーの透明性を高めるためには、本人が同意を与える「データ処理の目的」について、内容を分類して標準化し、プライバシーポリシー内では目立つ形で表示するようにするべきである。また、第 6 条第 1 項(b)～(f)に挙げられたような同意を必要としない処理目的については、プライバシーポリシーのトップページではなくリンク先での表示も可能とするなど、むしろ目立たない形での表示を可能とするべきである。ただし、第 6 条第 1 項(b)～(f)に挙げられたような同意を必要としない処理目的であっても、一般的に受容されていない処理目的、すなわち個人に対して不意打ちとなるような処理目的については、目立つ形で表示するようにするべきである。
- また、第 39 条にいうデータ保護シールを表示することは、個人が民間企業等によるデータ処理の合法性（lawfulness）を評価するための優れた手段となりうる。このようなデータ保護シールを表示す

る管理者に対しては、第 11 条にいうプライバシーポリシーの透明性の詳細基準を定める際に、一定の透明性の要件を満たしているものとして、特別の配慮をお願いしたい。

②従業員データの合法的処理（第 7 条第 4 項）

・ また、第 7 条第 4 項では「データ主体と管理者の地位の間の従属関係に重大な不均衡が存在する場合には、同意は処理のための法的根拠を与えないものとする」と規定されており、前文の（34）項では「同意は、データ主体と管理者の間に明確な不均衡が存在する場合には、個人データ処理のための有効な法的根拠を与えない。このことは、とりわけデータ主体が管理者に依存する状況にあるとき、特に雇用の関係において被用者の個人データを雇用者が処理する場合に該当する」とされている。このことは、被用者よりも強い立場にある雇用者が、被用者に同意を強いることによって、正当でない目的で従業者データ（とりわけ人種、民族、政治的見解、宗教、遺伝データ、健康医療データ等の特定機微データ）が処理されることを禁じるための説明として、理解できる。
このような意味において、従業員からの同意は雇用者が従業員データを処理することの法的根拠を与えないということは理解できるが、逆に、雇用者が雇用契約の履行等の正当な目的で従業員データを処理する場合に、どのような方法で合法性を担保すればよいかについての言及がないため、雇用者に対してミスリーディングな説明となっている。雇用者が正当な目的で従業員データの処理を行う際の処理の合法性は、第 6 条第 1 項(b)の「データ主体が当事者であるような契約の履行のために、又は契約締結に先立ちデータ主体の請求に対処するために処理が必要なとき」または第 6 条第 1 項(f)の「管理者が追求する正当な利益の目的のために処理が必要なとき」のいずれかの適用によって担保されると考えられるが、もしそうであるならば、その旨を明示してほしい。また、もし、いずれの条項も合法性を担保するものではないということであれば、合法性を担保するための方策を明確化するようにお願いしたい。

③大規模災害時のデータ処理（第 6 条第 1 項）

・ 地震・津波等の大規模災害が発生した際、被災者個人の権利利益を損なわない限りで、被災者の生活再建などの被災者支援を効率的に行うことを目的として、関係機関の間で本人同意を得ずにデータの提供や利用が必要になる場合があると考えられる。このような大規模災害発生時におけるデータ処理の合法性は、第 6 条第 1 項(d)の「データ主体の重大な利益を保護するために処理が必要なとき」または(e)の「公共の利益又は管理者に付与された職権の行使において実行されるタスクの遂行のために処理が必要なとき」が適用されると考えられるが、管理者側での疑義が発生しないように、その旨を明確化してほしい。

2．5　忘れられる権利とデータ・ポータビリティの権利について（第 17 条、第 18 条）

①忘れられる権利と消去する権利（第 17 条）

・ 現行の EU 指令の第 12 条にも自分の個人データを消去する権利が規定されているが、現行指令の規定ではデータが不正確だったり不法に収集された等の理由がないと必ずしも消去する権利が保障されない。それに対し、ソーシャルネットワーキングサイト等での個人データの公開の拡大を受けて、規則案第 17 条では本人が同意を撤回したり、同意した保有期間の期限が来たりした場合には個人データを消去する権利が保障されることとなり、個人データ保護の立場からは大きな前進であると理解している。
・ しかし、消去対象となる個人データの範囲については第 17 条では「データ主体に関する個人データ」という記述があるが、規則案に定める「個人データ」の範囲は上記 2.3 節で述べたように、明確ではない。
・ また、管理者側で付加した、当該個人に対する評価情報（信用情報など）や診療情報（カルテ、検査結果等）も、本人が消去請求を行った場合に消去対象となるのか、それとも、これらは第 17 条第 3 項(d)にいう例外事由（「管理者が従うべき EU 又は加盟国の法律によりデータを保持する法的義務を

遵守する場合」）に該当しうるのかについても明確ではない。

- なお、前文の(23)項では「データ保護の諸原則はデータ主体がもはや識別可能でない仕方で匿名化されたデータには適用されるべきでない」と言われており、匿名化されたデータは「個人データ」に該当しないと考えられるので、匿名化されたデータ（data rendered anonymous）については消去対象とはならないと我々は解釈している。
- 消去対象となる個人データの範囲は、民間企業が個人データの処理を伴う製品やサービスを開発する上で、とりわけ個人データの管理方法を設計する上で、データ主体（data subject）の消去請求に対して適切な措置を取れるようにするために極めて重要である。したがって、これについては委任法令（delegated acts）や実施法令（implementing acts）等の中で明確化してほしい。

②データ・ポータビリティの権利（第 18 条）

- 第 18 条において、あるサービスから他のサービスに自分の個人データを移転する個人の権利を認めていることは望ましいことである。
- しかし、個人の権利を保護するために一定の形式で入手できるデータは、本人のプロフィール情報（氏名、性別、年齢、住所、写真、趣味等）や書き込み内容に限定するべきであり、本人のサイト閲覧履歴や購買履歴といったログデータまで対象とするべきではない。これらの当該企業のビジネスモデルに大きく関わるデータまで、利用者の請求に応じて他のサービスに移転できる一定形式で渡さなければならないとなると、民間企業が革新的サービスを生み出すインセンティブを損ねるおそれがあるので、過大な要件とならないように配慮してほしい。このようなログデータに対して個人のデータ保護の権利を保障するためには、当該データを匿名化する、もしくは第 17 条に基づき当該データを消去することで十分であると考える。

２．６　管理者と処理者の義務（obligations）について（第４章）

①個人データ違反の監督機関への通知、データ主体への連絡（第 31 条、第 32 条）

- 第 31 条と第 32 条において、管理者や処理者に対し、個人データ違反（personal data breaches）を監督機関に通知し、データ主体に連絡することが義務付けられた。こうした通知義務自体は事業者として当然の責務であり、我が国の「個人情報の保護に関する基本方針」でも「事業者において、個人情報の漏えい等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表することが重要」と言われている。
- しかし、当該企業が個人データ違反に気づいてから、「可能な限り 24 時間以内に」、事実関係（漏洩等したデータの種類、件数、影響（consequences）等）や悪影響の軽減策（measures to mitigate the possible adverse effects）、管理者による対処策（measures proposed or taken by the controller）を含めて監督機関に通知することは、今日の個人データ漏洩事件がしばしば複数のデータベースに渡る何百万件という単位でのデータを巻き込むものであることに鑑みれば、漏洩範囲の特定や対処策の決定等に或る程度の時間を要する（例えば悪質なハッキングの場合は技術的調査に時間を要する場合がある）と考えられるため、可能な限り 24 時間以内という義務は果たすことが非常に難しい。個人データ違反の発見の第一報（データ違反の種類、分かる範囲での概要、およびデータ保護オフィサーの連絡先）は 24 時間以内に行うとしても、第 31 条第 3 項で規定された詳細内容については内部でのオーソライズが取れ次第、不当な遅滞なく監督機関に通知するといった、より実行可能な要件に変更してほしい。
- また、必ずしも全てのデータ違反が、データ主体の権利に対して重大なリスクを提示する訳ではない。我が国の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」では、「書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合」は主務大臣（監督機関に相当）に対する報告は免除されている。このように、データ主体への影響が軽微であるために監督機関への通知や本人への連絡の義務が免除されるケースについて、明確化してほしい。

②データ保護影響評価（第 33 条）

- 第 33 条においてデータ主体の権利に明示的なリスクを与えるような個人データ処理に関し、管理者等にデータ保護影響評価の実施を義務付けることは、個人データ保護の観点からも、民間企業が事後の対策を行うことによるコスト増加を防ぐ観点からも、望ましいものである。
- 第 34 条第 2 項では、データ保護影響評価において監督機関のコンサルテーションが必要とされるケースが挙げられているが、この事前コンサルテーションに長い期間を要してしまうと、民間企業における当該個人データ処理を伴うサービス開始時期がそれだけ後ろ倒しとなり、事業活動に影響を与えるおそれがある。このような場合に迅速な事前コンサルテーションが可能となるように、監督機関における実施メカニズムや体制を十分に整備してほしい。
- 多くの日本企業においては、従業員の福利厚生を図る目的で、健康診断情報など健康に関するデータを収集している。このような場合は、第 33 条第 2 項(b)にいう特定の個人（従業員）に対する何らかの措置や決定を行う目的で健康に関するデータの処理を行っている訳ではないので、データ保護影響評価の実施対象とならないことを委任法令において明示してほしい。

③データ保護・バイ・デザインと処理のセキュリティ（第 23 条、第 30 条）

- 第 23 条（データ保護・バイ・デザインとデータ保護・バイ・デフォルト）や第 30 条（処理のセキュリティ）では、欧州委員会が委任法令や実施法令において、詳細な技術的標準や技術的措置のための基準を策定することが規定されている。このような委任法令・実施法令においては、民間企業の事業内容や事業規模に応じて（cf. 第 79 条第 3 項（b））、過度の経済的負担とならないように、実行可能な技術の適用に配慮した合理的な標準や基準を策定してほしい。また、民間の標準化団体を含む国際的な場での議論やコンセンサスとも調和の取れたものとしてほしい。
- また、不正アクセス等の悪意ある攻撃に対しては、セキュリティ対策によって完全に防御することは困難である。仮に企業が外部攻撃によってデータ漏洩等の個人データ違反を起こしたとしても、当該企業が上述の合理的な技術的措置を講じている場合には、管理者または処理者としての義務を果たしているとみなされるように配慮してほしい。

２．７　監督機関による課徴金について（第 79 条）

- 監督機関による課徴金（fine）は、第 79 条第 4 項～第 6 項において、民間企業の場合は最大で年間世界売上（its annual worldwide turnover）の 0.5%、1%、2%という 3 パターンに分類されている。企業の個人データ違反（個人データ漏洩等）そのものに対する課徴金は設定されていないが、第 30 条（セキュリティ）に基づき適切な措置を実施していなかったり、第 31 条及び第 32 条に基づき監督機関やデータ主体に対して個人データ違反に関する通知や連絡をしなかったりした場合には、最大で年間世界売上の 2%の課徴金が科されうる。この課徴金の上限額は、非常に高額なものであり、当該企業の存続を危うくしかねない。
- 民間企業が合理的なデータセキュリティの措置を講じていたとしても、悪意のあるハッカーに不正アクセスされてしまう可能性があり、知名度のある大企業ほどそのようなハッカーの標的にされやすいと言える。このような状況にも鑑み、年間世界売上の 2%という課徴金の上限額は過大であるため、絶対額としての上限額を設けてほしい。
- また、課徴金の額の決定については、第 79 条第 2 項において「行政的課徴金の額は、違反の性質、重大性及び持続性、違反の故意的又は過失的性質、当該自然人又は法人の責任の度合い及び当人による以前の違反の度合い、第 23 条に従い実施された技術的及び組織的措置及び手続き、並びに違反を救済するための監督機関への協力の度合いに応じて決めるものとする」とされているが、その具体的な算定基準は示されていない。第 79 条において欧州委員会による詳細規定（委任法令や実施法令）の策定は特に予定されていないようだが、このような詳細規定等において課徴金の具体的な算定基準をぜひ明確にしてほしい。

２．８　認証メカニズム、データ保護シールについて（第 39 条）

・ 第 39 条において、加盟国と欧州委員会は、とりわけEUのレベルにおいて、データ保護認証メカニズムの設立とデータ保護シールの設立を促進し、欧州委員会は詳細基準を委任法令や実施法令で策定することとなっているが、認証メカニズムやデータ保護シールは日本（プライバシーマーク等）を含め、様々な国において既に設立、運用され、成果を上げている。**今後、EUのレベルで当該制度を具体化していくにあたっては、これらの国々の既存制度を参考にして頂き、とりわけこれらの制度との相互承認に向けた検討を行って頂きたい。**

以　上

EU データ保護規則案に対する JEITA 意見書（主要な意見抜粋）

2012 年 9 月 27 日
一般社団法人 電子情報技術産業協会（JEITA）

欧州と緊密な関係にある日本の電子情報産業界の企業にとって、今年 1 月に公表された EU データ保護規則案は、在欧の日本の現地法人も含め、我々日本企業にも直接影響のある規則であり、当該規則案に対して JEITA としての意見を述べさせて頂ければ幸いである。（JEITA 意見書の全文は別添参照のこと。）

1．個人データの第三国移転と適切な安全管理措置（第 42 条、第 39 条関連）

- **第42条第2項に「適切な安全管理措置」として下記項目を追加してほしい。**
  "(e) データの受領者が第 39 条にいうデータ保護認証メカニズムまたはデータ保護シールの認証を受けていること。"

- **第39条第2項に下記の文章を追加してほしい。（和訳では「第三国内での認証の要件」の後に）**
  "及び第三国のものを含む既存のデータ保護シール制度との相互承認の要件"

- 日本には「プライバシーマーク」というデータ保護シール制度が存在し、既に12,000社以上が認証を受けている。プライバシーマークの準拠基準であるJISQ15001「個人情報保護マネジメントシステム-要求事項」は、通商産業省（現経済産業省）が1997年にEUデータ保護指令に基づき改訂した「民間部門における個人情報保護のためのガイドライン」を母体とするものである。そのため、プライバシーマークの認証を受けた日本の事業者は、「十分なレベルの保護」に準じるような適切な安全管理措置を講じていると、我々は考えている。

- このような日本のプライバシーマークと、第39条にいう欧州レベルのデータ保護シールとの相互承認が行われた場合、もしくはプライバシーマーク自体が第39条にいうデータ保護シールとして承認を受けた場合には、プライバシーマークの認証を受けているということが、第42条第１項にいう「適切な安全管理措置」に該当するようにしてほしい。

- 第39条第2項において、欧州委員会はデータ保護認証メカニズムやデータ保護シールの詳細基準を委任法令で策定することとなっているが、このような認証メカニズムやデータ保護シールは日本のプライバシーマークを含め、様々な国において既に設立、運用され、成果を上げている。今後、EU のレベルで当該制度を具体化していくにあたっては、これらの国々の既存制度を参考にして頂き、とりわけこれらの制度との相互承認に向けた検討を行って頂きたい。

２．域外適用の除外条件（第３条第２項関連）

・ 例えば商品やサービスの提供範囲に EU 加盟国が含まれない旨をサイト上で明示している場合は適用対象とならないなど、EU 域外企業が第 3 条第 2 項の適用対象とみなされないための条件を明確化してほしい。

・ 日本企業が開設する日本語のショッピングサイトで、たまたま EU 居住者（EU 在住の日本人を含む）が商品を購入した場合、あるいは日本企業が開設する日本語のソーシャルネットワーキングサイトでたまたま EU 居住者が会員となった場合、これらの日本企業が第３条第２項の適用対象となってしまうのは合理的ではない。もちろん、このような場合には適用対象とならないと考えられるが、どのような場合に第３条第２項が適用され、どのような場合に適用されないかが明確でないと EU 域外企業にとって法的な不確実性が高い。

３．従業員データの第三国移転（第 44 条関連）

・ 日本企業では、従業員データのみに限って、雇用契約の履行等の正当な目的で EU 域内の現地法人から日本の本社に移転するケースが多い。このようなデータ移転においては、個人の権利が侵害されるリスクは低いと考えられるため、標準契約条項や BCR よりも簡易な移転方法として、例えば、第 44 条第 1 項(a)に基づき本人がデータ移転について同意した場合も可能であること、もしくは第 44 条第 1 項(b)にいう「移転が、データ主体と管理者の間の契約の履行のために必要な場合」に該当することを明示してほしい。

・ 本人が同意した場合にデータ移転が可能であること自体は第 44 条第 1 項(a)号で規定されているが、我々が危惧するのは、第７条第４項で「データ主体と管理者の地位の間の従属関係に重大な不均衡が存在する場合には、同意は処理のための法的根拠を与えないものとする」と規定されており、前文の（34）項では「同意は、データ主体と管理者の間に明確な不均衡が存在する場合には、個人データ処理のための有効な法的根拠を与えない。このことは、とりわけデータ主体が管理者に依存する状況にあるとき、特に雇用の関係において被用者の個人データを雇用者が処理する場合に該当する」とされているため、従業員からの同意を得ることが雇用者が従業員データを第三国に移転することの法的根拠とならない恐れがある点である。

●JEITA の概要

JEITA は、素材から電子部品や半導体、また、民生電子製品から産業システム機器、さらには、IT 製品からソリューションサービス等を含む日本の代表的な電子情報産業の業界団体である。約 400 社の会員企業の事業は広くグローバルに展開されており、事業規模は日本国内約 14 兆円、海外約 26 兆円である。その中で、欧州は、研究開発、生産、販売、サービス提供等の事業拠点として、重要な位置を占めており、多くの拠点が設置されている。

付録：関連する条項

第 3 条　地域的なスコープ
1.本規則は、EU 域内に事業所を持つ管理者又は処理者の活動に関係する個人データの処理に適用される。
2.本規則は、EU 域内に事業所を持たない管理者による、EU 域内に居住するデータ主体の個人データの処理に、処理活動が以下に関連している場合に適用される。
(a)そのようなデータ主体に商品又はサービスを提供すること。又は
(b)そのようなデータ主体の行動をモニターすること。

第 7 条　同意の条件
4.データ主体と管理者の地位の間の従属関係に重大な不均衡が存在する場合には、同意は処理のための法的根拠を与えないものとする。

第 39 条　認証
1.加盟国と欧州委員会は、とりわけ EU のレベルにおいて、データ保護認証メカニズムの設立並びにデータ保護シール及びマークの設立を促進するものとする。これらは、データ主体が管理者及び処理者によって提供されるデータ保護のレベルを迅速に評価することを可能とする。データ保護認証メカニズムは、様々な部門及び様々な処理活動の具体的特徴を考慮に入れながら、本規則の適正な適用に貢献するものとする。
2.欧州委員会は、第 1 項で規定されたデータ保護認証メカニズムに関して、付与及び剥奪の条件、並びに EU 域内及び第三国内での認証の要件を含めて、より詳細な基準と要件を規定するために、第 86 条に則り委任された法令（委任法令）を採択する権限を与えられるものとする。

第 42 条　適切な安全管理措置による移転
1.欧州委員会が第 41 条に従った決定を行っていない場合、管理者や処理者は、法的拘束力のある文書において個人データ保護に関する適切な安全管理措置が提示した場合にのみ、第三国又は国際組織に個人データを移転することができる。
2.第 1 項で言及された適切な安全管理措置は、とりわけ、以下のいずれかによって提供されるものとする。
(a)第 43 条に則った拘束的企業準則。又は、
(b)欧州委員会によって採択されたデータ保護の標準契約条項。この実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。又は、
(c)第 57 条で規定された整合性メカニズムに則り監督機関によって採択されたデータ保護の標準契約条項であって、第 62 条(1)の(b)に従い欧州委員会によって全般的に妥当であると宣言がなされた場合。又は、
(d)本条第 4 項に則り監督機関にオーソライズされた、管理者又は処理者とデータの受領者の間の契約条項。

第 44 条　例外
1.第 41 条に従った十分性の決定がなされていない場合、又は第 42 条に従った適切な安全管理措置が取られていない場合、第三国又は国際組織への個人データの移転又は一連の移転は以下のいずれかの条件でのみ行うことができる。
(a)データ主体が提案された移転に対して、十分性の決定や適切な安全管理措置がないことによる移転のリスクについて十分に情報を与えられた後に、同意を与えた場合。又は、
(b)移転が、データ主体と管理者の間の契約の履行のために必要な場合、又はデータ主体の要求により契約締結間の措置の実施に必要な場合。又は、

(c)移転が、データ主体の利益のために管理者と他の自然人又は法人の間で締結された契約の締結又は履行のために必要な場合。又は、
(d)移転が、公共の利益の理由から必要な場合。又は、
(e)移転が、法的要求の立証、実行又は抗弁に必要な場合。又は、
(f)移転が、データ主体が物理的又は法的に同意を与えることが不可能な場合であって、データ主体又はその他の人間の重大な利益を保護するために必要な場合。又は、
(g)移転が、EU 又は加盟国の法律に従って公衆に情報を提供することが意図され、かつ公衆一般又は正当な利益を示せる人によるコンサルテーションに門戸を開いている官報（register）によってなされ場合。ただし、EU 又は加盟国の法律でコンサルテーションのために規定された条件が当該ケースに当てはまる範囲に限る。又は、
(h)移転が、管理者又は処理者が求める正当な利益の目的にとって必要であり、それが頻繁、又は大量とはみなされず、かつ管理者又は処理者がデータ移転又は一連のデータ移転の運用に関わる全ての環境を評価し、必要あればこの評価に基づき個人データ保護に係る適切な安全管理措置を提示している場合。

前文(34)
同意は、データ主体と管理者の間に明確な不均衡が存在する場合には、個人データ処理のための有効な法的根拠を与えない。このことは、とりわけデータ主体が管理者に依存する状況にあるとき、特に雇用の関係において被用者の個人データを雇用者が処理する場合に該当する。管理者が公的機関の場合、公的機関がその公的権限によって義務を課すことができ、かつ、データ主体の利益に鑑み、同意が束縛を受けずに与えられたとみなすことができない場合、特定のデータ処理活動においてのみ不均衡が存在することがありうる。

JEITA's Opinion on the Proposed EU Data Protection Regulation
September 27, 2012
Japan Electronics and Information Technology Industries Association(JEITA)

1. Introduction

1.1 Overview of JEITA

- The Japan Electronics and Information Technology Industries Association, or JEITA, is an industrial association of Japan's typical electronics and information technology manufacturers, ranging from materials to electronic components and semiconductors, from consumer electronics to industrial system devices, from IT products to solution services.
- Its approximately 400 member companies are operating globally and their aggregate domestic and overseas turnovers amount to nearly 14 trillion yen and 26 trillion yen, respectively. Europe is one of the important centers for research and development, production, marketing, service, etc., and many member companies have established business sites there.
- Given the close relationship between Japan's electronics and information technology industries and Europe, the Proposed EU Data Protection Regulation released in January this year directly affects Japanese companies and their European affiliates as well, and JEITA would be pleased to be given the opportunity to give feedback on the proposed regulation.

1.2 JEITA's basic stance on data protection

- With the widespread use of the Internet and the advancement of ICT technologies, many companies are taking advantage of them to enhance their productivity, create innovations, and deliver new added value to people. In the public sector, these technologies are also used to create increased convenience, including the provision of new services to citizens and the enhancement of work efficiency. Furthermore, rapidly spreading SNSs are creating new personal links and various forms of communities.
- On the other hand, the distribution of large amounts of data across borders has increased the risk of data leakage, especially personal data, and the violation of privacy. We believe that the European Commission took timely action in response to these changes in the environment surrounding personal data as it reviewed the 1995 directive on data protection and presented a proposal for new data protection regulation.
- The protection and use of personal data have long been discussed from various angles on the regional, national and international levels, including at the OECD, due to the difference in history, culture, and the people's attitude toward personal data. However, in recent years, we have witnessed a global convergence of ideas about the principles of data protection. Given this international trend, we believe that there are three critical factors to personal data protection: (i) the protection of individual rights, (ii) the responsibility/accountability of companies and organizations, and (iii) enforcement by supervisory authorities. Japan's personal data protection framework should also be reviewed from this viewpoint.
- The proposed Data Protection Regulation recently released would be very welcome even by companies operating across Europe in that it reinforces the right of personal data protection, removes the detrimental consequences of national legislation variances among the European Union member states, and abolishes the obligation to notify supervisory authorities about the processing of personal data (general notification requirements). However, the new obligation that the proposed regulation impose on companies in order to safeguard data concerning EU residents could be enforced in a way that would cause relevant industries to bear new costs to ensure compliance with the regulation, with the result that the overall cost reduction claimed by the Commission would not be realized. The

proposal also contains a new rule whereby the EU regulation should also be applied to controllers in the case where data related to data subjects residing in the European Union and to whom products and services are provided is processed outside the EU.

- **Global data protection rules for companies operating in an environment where persons, goods, money, information, and other management resources are distributed across the borders (i) must be transparent and easy to understand, (ii) must be fair and harmonized both internally and externally, (iii) must be practical and effective, and (iv) must not impose excessive control on company activities or excessive burdens on companies. We hope that the release of the proposed Data Protection Regulation by the European Commission will trigger active discussion at the national or international agency level from the perspective described above and lead to the formation of an international framework concerning the protection and use of personal data that fits the modern social environment.**

2. JEITA's Opinion on the Proposed EU Data Protection Regulation

2.1 Transfer of personal data to third countries (Chapter V)

(i) On transfer to third countries and adequacy decision (related to Articles 39, 41, and 42)

- Article 41 of the proposed regulation allows for a decision on the adequacy concerning a processing sector within a third country, which we believe is preferable. Private companies in Japan safeguard personal data in accordance with the Act on the Protection of Personal Information as well as personal information protection guidelines issued by competent ministries and agencies. Japanese industrial associations will take action to convince the European Commission that Japan's private sector ensures an "adequate level of protection", in order to obtain a decision on adequacy for Japan as a whole or its private sector or certain industries.
- However, if an adequacy assessment application is filed by the Japanese government with the Commission, it will take some time to obtain a final decision. For the time being, Japanese companies have to receive personal data from controllers located within the EU (including Japanese companies' affiliates) in accordance with standard data protection clauses or BCRs (binding corporate rules). Article 42, paragraph 3 stipulates that standard data protection clauses adopted by the Commission or supervisory authorities "shall not require any further authorization". This can be interpreted to mean that Japanese companies do not have to obtain any further authorization from supervisory authorities when taking advantage of standard data protection clauses, implying a simpler procedure. We welcome such simplification of procedures concerning standard data protection clauses and BCRs in the proposal.
- However, controllers located within the EU may feel it burdensome to conclude standard data protection clauses with each non-EU company with respect to data transfer from the controllers, and this may lead to a loss of business opportunities for external companies. It would be detrimental to Japanese companies, especially those engaged in cloud services.
- Japan has the "Privacy Mark System" (a data protection seal), and more than 12,000 companies have already been certified under this system. JISQ15001 "Personal information protection management systems: Requirements", which governs the Privacy Mark, is based on the "Guidelines for the protection of personal information in the private sector", which were revised by the Ministry of International Trade and Industry (now the Ministry of Economy, Trade and Industry" in 1997 pursuant to the EU data protection directive. Thus, we believe that Japanese companies certified under the Privacy Mark system take appropriate safeguards equivalent to an "adequate level of protection". **We request that once Japan's Privacy Mark and European-level data protection seals as mentioned in Article 39 are mutually recognized, the Privacy Mark certification should be automatically**

taken as an adduction of "appropriate safeguards" as mentioned in Article 42, paragraph 1.

- Or the acquisition of the Privacy Mark or other data protection seals can be considered to be one of the criteria for making a decision on adequacy with respect to a processing sector within a third country. If this is the case, we request that it be clearly stated in the regulation, possibly a new sentence in Article 41, paragraph 2 about data protection seals.
- Globally operating enterprises are increasingly processing consumers' personal data across borders, and therefore need a data transfer method that is harmonized and standardized between countries and among regions. Thus, it is desirable that international standards concerning data protection be established in the medium-to-long term and harmonized with the EU Data Protection Regulation in terms of a decision on adequacy (Article 41) and appropriate safeguards (Article 42).

(ii) Transfer of employee data to third countries (related to Article 44)

- Many Japanese affiliates within the EU transfer only their employee data to head offices in Japan for legitimate purposes, such as the fulfillment of the employment contract. Because of the low possibility that individual rights are infringed in such data transfer, we request that the regulation expressly permit such data transfer, which is simpler than a transfer pursuant to standard data protection clauses or BCRs, on the condition that, for example, the data subject consents to such data transfer.
- It is, in fact, stipulated in Article 44, paragraph 1, point (a) that a data transfer is permitted if the data subject has consented to it. But what we are concerned about is that the employee's consent may not provide a legal basis for the employer to transfer the employee's personal data to a third country; this can be inferred from Article 7, paragraph 4, stating "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller", and from whereas clause (34), stating "Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer in an employment context."

2.2 Extraterritorial application of the EU regulation (Article 3, paragraph 2)

(i) Conditions for exclusion from extraterritorial application

- We agree that the development of services supplied via the Internet has rendered it insufficient for the protection of personal data concerning EU residents to apply the EU legislation to non-EU controllers only in the case where data processing is conducted with equipment located within the EU, as stipulated in Article 4, paragraph 1(c) of the current EU data protection directive.
- However, in the case where, for example, an EU resident (including a Japanese national residing in the EU) happens to buy a product at a Japanese shopping site established by a Japanese company or happens to become a member of a Japanese social networking site operated by a Japanese company, it would not be reasonable to apply Article 3, paragraph 2 to such Japanese company. Of course, we believe that these cases are not subject to extraterritorial application, but non-EU companies would face a high degree of legal uncertainty unless it is expressly stipulated in what cases Article 3, paragraph 2 will be applied or not applied. Therefore, we request that the regulation expressly enumerate the conditions for excluding non-EU enterprises from Article 3, paragraph 2, including, by way of example, a statement on the website that the products and services

are not intended for EU member states.

2.3 Definition of personal data (Article 4 (1) and (2))

- In connection with the definition of the term "personal data", the proposed regulation refer to "location data" and "online identifier" as means of identifying an individual, which are not included in the current EU directive. And whereas clause (24) of the proposed regulation states "It follows that identification numbers, location data, online identifiers (such as Internet Protocol addresses or cookie identifiers) or other specific factors as such need not necessarily be considered as personal data in all circumstances", implying that in some cases these data, as such, may be considered to be personal data.
- In the case where private companies control Internet Protocol addresses, cookies, and other online identifiers in relation to individuals, it is possible to trace or profile the individuals online even if their names are not collected or stored by the companies. We agree that these data can be the subject of protection.
- However, the proposed EU Regulation do not clearly define in what circumstances these location data, Internet Protocol addresses, cookies, or other online identifiers (such as PC and smart phone identifiers) are considered personal data.
- The definition of the term "personal data" affects all the obligations of controllers (and processors) under the proposed regulation. For example, whether particular data is considered "personal data" or not greatly affects security measures for such data (Article 30), responses to the right to be forgotten (Article 17), the notification and communication of a personal data breach (Articles 31 and 32), and the imposition of a fine by the supervisory authority (Article 79). Therefore, if the scope of personal data is not clearly defined, it would mean significant legal uncertainty for the business activities of private companies.
- **As a representative of private companies, we request that the regulation clearly stipulate under what circumstances identification numbers, location data, online identifiers, or other "gray-zone" data will not be considered personal data, in other words, what kinds of measures controllers or processors should implement for such data in order to be exempted from the obligation to protect it as personal data when processing it.**
- For example, the report "Protecting Consumer Privacy in an Era of Rapid Change" released by the U.S. Federal Trade Commission in March this year defines protected data as "data that is reasonably linkable to a specific consumer, computer, or other device" and stipulates that data is not "reasonably linkable" to the extent that a company (1) takes reasonable measures to ensure that the data is de-identified (rendered anonymous or given a pseudonym), (2) publicly commits not to try to re-identify the data, and (3) contractually prohibits downstream recipients from trying to re-identify the data. This definition is very clear to private companies.

2.4 Lawfulness of processing and transparent policy (Articles 6, 7, and 11)

(i) Transparent policy and data subject's consent (Articles 4(8), 6.1, 7, and 11)

- We understand that because of the complexity and unintelligibility of the prevailing privacy policies of private companies, Article 11 of the proposed regulation imposes a new obligation of "transparency" on controllers, and because of the unintelligibility thereof that often renders data subjects' consents a mere formality, Articles 4(8) and 7.1 and 7.2 of the proposal require controllers to obtain explicit consents and Article 7.3 prescribes a new obligation to guarantee the right of data subjects to withdraw their consent.
- However, as private enterprises' data practices are becoming increasingly complicated and harder to

notice or understand for consumers, the more in detail privacy policies are written, the harder to understand and the more annoying they will be for consumers, possibly leading to the opposite result: consumers may mechanically "consent" without reading them carefully. In order to avoid such mechanical consents, it would be necessary to request individuals to carefully read the privacy policies and then give their explicit consent in all cases, but this would mean a significant burden and inconvenience to service users. **We need to identify a means for resolving this dilemma: if we try more to respect data subjects' consent and protect their individual rights, then their burden increases.**

- **In order to increase the transparency of privacy policies, it is preferable to classify the "purposes of data processing" for which the consent of the data subject is required into standard categories and ensure that these categories will be conspicuously indicated in privacy policies. The purposes of processing for which the data subject's consent is not required, such as those described in Articles 6.1.(b) to (f), should be allowed to be indicated in an inconspicuous way, e.g., on a page linked to the top page of a privacy policy rather than on the top page itself. However, if the purposes of processing for which the data subject's consent is not required, such as those described in Articles 6.1.(b) to (f), are not generally accepted ones or can be a surprise to individuals, then they should be indicated conspicuously.**
- **Further, the indication of data protection seals under Article 39 can be a good means to allow individuals to assess the lawfulness of data processing by private enterprises etc. We request that controllers who indicate such data protection seals be specially treated as meeting certain of the detailed transparency requirements that will be established under Article 11.**

(ii) Lawful processing of employee data (Article 7, paragraph 4)

- Article 7, paragraph 4 states "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller", and whereas clause (34) states "Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer in an employment context." This can be understood as explaining that the employer, who is in a stronger position than employees, is prohibited to coerce employees into consent and process employee data (especially their race, ethnic origin, political view, region, genetic data, health and medical data, and certain other pieces of sensitive data) for illegitimate purposes.
- We can understand that employees' consent, in this sense, does not provide a legal basis for the processing of employee data by the employer. However, this explanation would mislead employers because it does not mention what they should do to ensure the lawfulness of employee data processing when it is done for the fulfillment of the employment contract or other legitimate purposes. **It seems that the lawfulness of employee data processing by employers when it is done for legitimate purposes is ensured by either Article 6.1.(b) "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract", or Article 6.1.(f) "processing is necessary for the purposes of the legitimate interests pursued by a controller". If this is the case, we request it to be clearly stated. Or if neither of the clauses can be interpreted to ensure the lawfulness of such processing, we request that the regulation specify what should be done to ensure lawfulness.**

(iii) Data processing upon the occurrence of a large-scale disaster (Article 6, paragraph 1)

If an earthquake, tsunami, or other large-scale disaster occurs, it would be necessary to provide or use personal data without the consent of the data subjects for the purpose of assisting disaster victims to rebuild their lives and promoting other reliefs in an efficient manner, but to the extent not detrimental to their individual rights and interests. **It seems that the lawfulness of data processing upon the occurrence of such large-scale disasters is ensured by Article 6.1.(d) "processing is necessary in order to protect the vital interests of the data subject" or Article 6.1.(e) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". We request it to be clearly stated in the regulation so that controllers will have no doubt about it.**

2.5 Right to be forgotten and right to data portability (Articles 17 and 18)

(i) Right to be forgotten and to erasure (Article 17)

- The current EU directive also prescribes, in its Article 12, the right to have one's own personal data erased, but this right to erasure is not necessarily guaranteed unless there are good reasons, such as the inaccurate nature or illegal collection of the data. With the volume of personal data made public at social networking sites etc. increasing, the proposed regulation stipulates in its Article 17 that data subjects have the right to have their personal data erased if they withdraw their consent or upon the expiration of the storage period consented to. We understand this is great progress in the protection of personal data.
- However, while the scope of personal data required to be erased is mentioned in Article 17 ("personal data relating to them"), the scope of the term "personal data" itself is not clearly defined in the regulation as discussed in Section 2.3 above.
- It is also not clear if, when erasure requests are made by data subjects, information added by controllers, such as evaluations (credit status etc.) and medical information (charts, test results, etc.) concerning the individuals, must also be erased or may be excluded under Article 17.3.(d) ("for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject").
- **We interpret data rendered anonymous as not being required to be erased since whereas clause (23) states "The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable" and data rendered anonymous is not considered as "personal data".**
- **The scope of personal data required to be erased is very important for private companies to ensure their ability to respond properly to data subjects' erasure requests as they are received, when developing products and services involving personal data processing, in particular, designing personal data management methods. Therefore, we request it to be clearly defined in a delegated or implementing act.**

(ii) Right to data portability (Article 18)

- Article 18 appropriately prescribes an individual's right to transfer his/her own personal data from one service to another.

  However, the data that can be obtained in a certain format to protect an individual's right should be limited to his/her profile information (such as name, sex, age, address, photograph, hobby) and personal postings, and should not include log data, such as his/her site visit and purchase histories. These data are closely related to corporate

business models, and should private companies be required to give, at user requests, such data in a format which allows data portability to another service, they might be discouraged from creating innovative services. So, we hope that the portability requirement will not be an excessive one. We think the right of personal data protection with respect to such log data can be adequately secured by rendering such data anonymous or erasing them in accordance with Article 17.

2.6 Obligations of the controller and the processor (Chapter IV)

(i) Notification of a personal data breach to the supervisory authority and communication thereof to the data subject (Articles 31 and 32)

- Articles 31 and 32 require the controller/processor to notify personal data breaches to the supervisory authority and communicate them to the data subject. Such notification itself is a taken-for-granted duty of a company, and Japan's Basic Policy on the Protection of Personal Information also states "If the leakage of personal information etc. occurs, it is important for the company to disclose the fact etc. to the extent possible in order to prevent the occurrence of secondary damage, similar incidents, etc."
- However, it is very difficult for the company to fulfill the obligation of notifying the facts (the types and number of data leaked, the consequences of the leakage, measures to mitigate the possible adverse effects, and measures proposed or taken by the controller) to the supervisory authority, "where feasible, not later than 24 hours after having become aware of" the leakage. Given the fact that recent personal data leaks often involve millions of data stored in several databases, it would take some time to identify the scope of leakage and determine the future course of action (for example, in the case of malicious hacking, a technical investigation can be a time-consuming activity). **Although the controller should be required to give the first report on a personal data breach within 24 hours (specifying the type of the breach, a brief description of the then available information, and the data protection officer's contact details), we request that the detailed requirement prescribed in Article 31, paragraph 3 be replaced with a more practicable one: for example, the controller shall give a detailed notification to the supervisory authority without undue delay as soon as an internal authorization is obtained.**
- And not all data breaches necessarily pose a serious risk to the right of the data subject. Japan's Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information exempt companies from the obligation of notification to the competent minister (which corresponds to the supervisory authority) in the case of the "loss etc. of a commercial directory etc. that is easily available to anyone at a bookstore". Thus, **we request that the EU regulation expressly prescribe the cases in which companies are exempted from the obligation to notification to the supervisory authority and communication to the data subject because of the minor impact on the data subject.**

(ii) Data protection impact assessment (Article 33)

- Article 33 requires the controller etc. to assess the impact on personal data protection of the envisaged processing operations that can present specific risks to the rights of data subjects, which we think is appropriate for protecting personal data as well as for eliminating the need for companies to take "Bolt-on" measures, which mean additional costs to them.
- Article 34, paragraph 2 mentions a case in which the consultation of the supervisory authority is required in connection with a data protection impact assessment. If this prior consultation is a time-consuming process, private companies might have to postpone the commencement of the service involving the personal data processing operations at issue accordingly, and this might affect their

business activities. **We request that the supervisory authorities ensure, by establishing an appropriate mechanism or system, that such prior consultation will be completed promptly.**

- **Many Japanese companies collect employees' health data, including medical examinations, in order to promote their welfare. In this case, health data is not processed for taking measures or decisions regarding specific individuals (employees) as mentioned in point (b) of Article 33.2, and we request that a delegated act clearly stipulate that a data protection impact assessment need not be carried out in such case.**

(iii) Data protection by design and security of processing (Articles 23 and 30)

- Article 23 (Data protection by design and by default) and Article 30 (Security of processing) empower the Commission to adopt delegated or implementing acts for the purpose of specifying further technical standards and technical measure criteria. **We request that such standards and criteria established by delegated or implementing acts should be reasonable in light of the nature and size of private companies' business activities (cf. point (b) of Article 79.3), should take practicable technology application into consideration, and should not place an excessive economic burden on them. We also request that such standards and criteria be harmonized with international discussions and consensuses, including by private-sector standardization organizations.**
- **It is difficult to completely protect personal data from malicious attacks, including unauthorized access, with security measures. If a personal data breach, such as leakage, takes place as a result of an external attack, the company should still be regarded as having fulfilled its obligations as a controller or processor so long as it has taken reasonable technical measures as mentioned above.**

2.7 Fine by the supervisory authority (Article 79)

- Paragraphs 4 to 6 of Article 79 prescribe three fine rates to be imposed by the supervisory authority: up to 0.5%, 1%, and 2% of a private company's annual worldwide turnover. Although the regulation does not provide for a fine on a company's personal data breach itself (such as the leakage of personal data), a fine equal to up to 2% of its annual worldwide turnover will be imposed in the case of the failure to take appropriate measures in accordance with Article 30 (Security) or to notify a personal data breach to the supervisory authority in accordance with Article 31 or communicate it to the data subject in accordance with Article 32. This maximum amount is so large that it can endanger the existence of the company.
- Even if private companies have taken reasonable data security measures, it is still possible that their data is illegally accessed by malicious hackers. The more widely known a company is, the more attractive it may appear to such hackers. **Given these situations, the maximum fine of 2% of a company's annual worldwide turnover is too heavy, and we request that the maximum amount be stated as an absolute figure.**
- With respect to the determination of the amount of a fine, Article 79, paragraph 2 states "The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach", but no specific calculation basis is set out. **It seems that Article 79 does not expect the Commission to establish further rules (such as delegated or**

implementing acts), but we insist that a specific calculation basis be defined in such further regulations or otherwise.

2.8 Certification mechanism and data protection seal (Article 39)

- Article 39 requires the member states and the Commission to encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, and empowers the Commission to adopt delegated or implementing acts for the purpose of further specifying the criteria and requirements for this purpose. There are already several certification mechanisms and data protection seals in place around the world (e.g., Japan's Privacy Mark), and they are working effectively. We hope that in the examination of European-level data protection certification mechanisms and seals, these existing systems, in particular, mutual recognition therewith, will be taken into consideration.

--- END OF DOCUMENT ---

JEITA's Opinion on the Proposed EU Data Protection Regulation (excerpted version)

September 27, 2012

Japan Electronics and Information Technology Industries Association (JEITA)

Given the close relationship between Japan's electronics and information technology industries and Europe, the Proposed EU Data Protection Regulation released in January this year directly affects Japanese companies and their European affiliates as well, and JEITA would be pleased to be given the opportunity to give feedback on the proposed regulation. (See also the whole JEITA's Opinion we attached.)

1. Transfer to third countries and appropriate safeguards (related to Articles 42 and 39)

- We request that the following point should be added to Article 42 paragraph 2, as "appropriate safeguards."

  "(e) certification of data protection certification mechanisms or data protection seals referred to in Article 39, obtained by the data recipient."

- We request that the following sentence should be added to Article 39 paragraph 2, after "in third countries."

  "and mutual recognition with existing data protection seal systems including in third countries."

- Japan has the "Privacy Mark System" (a data protection seal), and more than 12,000 companies have already been certified under this system. JISQ15001 "Personal information protection management systems: Requirements", which governs the Privacy Mark, is based on the "Guidelines for the protection of personal information in the private sector", which were revised by the Ministry of International Trade and Industry (now the Ministry of Economy, Trade and Industry" in 1997 pursuant to the EU data protection directive. Thus, we believe that Japanese companies certified under the Privacy Mark system take appropriate safeguards equivalent to an "adequate level of protection".
- We request that once Japan's Privacy Mark and European-level data protection seals as mentioned in Article 39 are mutually recognized, or once Japan's Privacy Mark is accredited as a data protection seal referred to in Article 39, the Privacy Mark certification should be automatically taken as an adduction of "appropriate safeguards" as mentioned in Article 42, paragraph 1.
- Article 39, paragraph 2 empowers the Commission to adopt delegated acts for the purpose of further specifying the criteria and requirements of data protection certification mechanisms and of data protection seals. There are already several certification mechanisms and data protection seals in place around the world (e.g., Japan's Privacy Mark), and they are working effectively. We hope that in the examination of European-level data protection certification mechanisms and seals, these existing systems, in particular, mutual recognition therewith, will be taken into consideration.

2. Conditions for exclusion from extraterritorial application (related to Article 3, paragraph 2)

- We request that the regulation expressly enumerate the conditions for excluding non-EU enterprises from Article 3, paragraph 2, including, by way of example, a statement on the website that the products and services are not intended for EU member states.

- In the case where, for example, an EU resident (including a Japanese national residing in the EU) happens to buy a product at a Japanese shopping site established by a Japanese company or happens to become a member of a Japanese social networking site operated by a Japanese company, it would not be reasonable to apply Article 3, paragraph 2 to such Japanese company. Of course, we believe that these cases are not subject to extraterritorial application, but non-EU companies would face a high degree of legal uncertainty unless it is expressly stipulated in what cases Article 3, paragraph 2 will be applied or not applied.

3. Transfer of employee data to third countries (related to Article 44)

- Many Japanese affiliates within the EU transfer only their employee data to head offices in Japan for legitimate purposes, such as the fulfillment of the employment contract. Because of the low possibility that individual rights are infringed in such data transfer, we request that the regulation expressly permit such data transfer, which is simpler than a transfer pursuant to standard data protection clauses or BCRs, on the condition that, for example, the data subject consents to such data transfer in accordance with Article 44, paragraph 1, point (a). Or we request it be clearly stated that such data transfer can be deemed “the transfer is necessary for the performance of a contract between the data subject and the controller” referred to in Article 44, paragraph 1, point (b).

- It is, in fact, stipulated in Article 44, paragraph 1, point (a) that a data transfer is permitted if the data subject has consented to it. But what we are concerned about is that the employee's consent may not provide a legal basis for the employer to transfer the employee's personal data to a third country; this can be inferred from Article 7, paragraph 4, stating "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller", and from whereas clause (34), stating "Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer in an employment context."

●Overview of JEITA

The Japan Electronics and Information Technology Industries Association, or JEITA, is an industrial association of Japan's typical electronics and information technology manufacturers, ranging from materials to electronic components and semiconductors, from consumer electronics to industrial system devices, from IT products to solution services. Its approximately 400 member companies are operating globally and their aggregate domestic and overseas turnovers amount to nearly 14 trillion yen and 26 trillion yen, respectively. Europe is one of the important centers for research and development, production, marketing, service, etc., and many member companies have established business sites there.

Appendix: Related provisions

Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) the offering of goods or services to such data subjects in the Union; or
(b) the monitoring of their behaviour.

Article 7 Conditions for consent

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

Article 39 Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

Article 42 Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:
(a) binding corporate rules in accordance with Article 43; or
(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or
(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or
(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

Article 44 Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:
(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or
(d) the transfer is necessary for important grounds of public interest; or
(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or
(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or
(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

Whereas clause (34)
Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.