規則(EU) 2018/1725

［参考訳］

2019 年 1 月 23 日
明治大学法学部教授
夏 井 高 人

＊＊＊

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC（OJ L 295, 21.11.2018, p.39-98）のテキスト（英語版）に基づき、和訳を試みた。テキストは、下記の Eur-lex の Web サイトから入手した。

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN
[2018 年 12 月 27 日確認]

規則(EU) 2018/1725 は、規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1-22）の全面改正法令である。規則(EC) No 45/2001 は、規則(EU) 2018/1725 の第 99 条により、2018 年 12 月 10 日をもって廃止された。規則(EC) No 45/2001 への参照は、規則(EU) 2018/1725 への参照として読み替えられる。

規則(EU) 2018/1725 は、前文及び条文の 2 つの部分で構成されている。この参考訳においては、規則(EU) 2018/1725 の前文及び条文の全文を訳出した。

この参考訳においては、原則として直訳とした。直訳のままでは日本語として意味の通らない部分や非常にわかりにくい部分に関しては、やむを得ず意訳とした。

この参考訳は、あくまでも規則(EU) 2018/1725 の私的な和訳であり、関連分野の研究者のための参考として提供するものである。確定訳ではなく、現時点における検討結果の一部を示すものであるので、今後、必要に応じて改訂・修正が加えられる可能性がある。誤記等があるときは、随時、法と情報雑誌上においてその正誤を公表する。

この参考訳に訳注はない。脚注は、全て原注である。

規則(EU) 2018/1725 は、規則(EC) No 45/2001 を一般データ保護規則(EU) 2016/679（GDPR）（OJ L 119, 4.5.2016, p.1-88）と均等なものとするための改正法としての位置づけをもつ（GDPR の前文(17)参照）。しかし、その改正内容の中で最も注目すべきことは、構成国間における捜査共助に伴い EU の機関及び組織が処理する個人データ（運用個人データ）の取扱いの明確化という点である。規則(EC) No 45/2001 の当初の改正案の文案中では必ずしも明確であるとは言えなかった部分が、採択された改正法である規則(EU) 2018/1725 の中においては、特に「TFEU の第 III 部第 V 款の第 4 章及び第 5 章の

適用範囲内にある活動を実施する場合の欧州連合の組織、事務局及び部局による運用個人データの処理」に関する第 IX 章の条項（第 70 条ないし第 95 条）によって明らかにされた。これにより、刑事司法共助に関し、EU レベルの業務における処理に適用される法令と構成国レベルの処理に適用される指令(EU) 2016/680（OJ L 119, 4.5.2016, p.89-131）とがパラレルになるように揃えられた。今後、Europol や欧州検事局（EPPO）を含め、警察活動と関連する EU の機関及び組織に適用される特別法令に関しても一部改正等が実施される見込みである（前文(12)、第 2 条第 2 項、第 98 条参照）。

当初の改正案に加えられ、規則(EU) 2018/1725 の第 IX 章の各条項の内容を EPPO 理事会規則(EU) 2017/1939（OJ L 283, 31.10.2017, p.1-71）及び指令(EU) 2016/680 と比較して整理すると、以下のとおりとなる。

個人データ保護と関連する事項	規則(EU) 2018/1725	規則(EU) 2017/1939	指令(EU) 2016/680
個人データ保護の基本原則	第 71 条	第 47 条	第 4 条
行政個人データの処理	第 72 条	第 48 条	（第 8 条）
運用個人データの処理	第 72 条	第 49 条	（第 8 条）
データ主体の類型区分	第 73 条	第 51 条	第 6 条
個人データの類型区分	第 74 条	第 52 条	第 7 条
特別の処理条件	第 75 条	第 53 条	第 9 条
EU の機関または組織に対する移転	第 70 条	第 54 条	－
特別類型の個人データの処理	第 76 条	第 55 条	第 10 条
自動的な判定、プロファイリング	第 77 条	第 56 条	第 11 条
データ主体の権利行使の方法	第 78 条	第 57 条	第 12 条
データ主体に対する情報提供	第 79 条	第 58 条	第 13 条
データ主体のアクセスの権利	第 80 条	第 59 条	第 14 条
アクセスの権利の制限	第 81 条	第 60 条	第 15 条
訂正・削除の権利、処理の制限	第 82 条	第 61 条	第 16 条
監督機関を介する権利の行使	第 83 条、第 84 条	第 62 条	第 17 条
共同管理者	第 86 条	第 64 条	第 21 条
処理者	第 87 条	第 65 条	第 22 条
バイデザイン・バイデフォルトの保護	第 85 条	第 67 条	第 20 条
履歴（ログ）	第 88 条	第 69 条	第 25 条
データ保護影響評価	第 89 条	第 71 条	第 27 条
監督機関との事前協議	第 90 条	第 72 条	第 28 条
個人データ処理の安全性	第 91 条	第 73 条	第 29 条
監督機関への個人データ侵害連絡	第 92 条	第 74 条	第 30 条
データ主体への個人データ侵害連絡	第 93 条	第 75 条	第 31 条
個人データの第三国移転の基本原則	第 94 条	第 80 条	第 35 条
守秘義務	第 95 条	第 86 条	－

規則(EU) 2018/1725 は、一般データ保護規則(EU) 2016/679（GDPR）の第 2 条第 3 項に基づき、規則(EC) No 45/2001 を一般データ保護規則(EU) 2016/679（GDPR）と均等なものとするために調整するための改正法である。しかし、規則(EU) 2018/1725 の第 IX 章は、一般データ保護規則(EU) 2016/679（GDPR）の第 2 条第 2 項(d)によって GDPR の適用除外となる警察（犯罪捜査）関連の職務遂行と関係する個人データ保護を対象とする指令(EU) 2016/680 と均等なものとするために調整するための改正部分である。

それゆえ、一般データ保護規則(EU) 2016/679（GDPR）の第 2 条第 3 項の形式的な立法根拠だけにとらわれることなく、規則(EU) 2018/1725 の審議経過及び採択後の条文の実質的な内容を丁寧に検討した上で、規則(EU) 2018/1725 が一般データ保護規則(EU) 2016/679（GDPR）及び指令(EU) 2016/680 の両者と均等な条項の体系を EU の機関及び組織に適用するための法令であることを正確に認識するための努力を重ねなければならない。

EU 及び構成国の行政機関に対する EU の基本的な個人データ保護法令の適用関係をまとめると、以下のようになる（ただし、電子通信部門に適用される e プライバシー指令 2002/58/EC（OJ L 201, 31.7.2002, p.37-47）を除く）。このような基本構造を念頭に置いた上で、e プライバシー指令 2002/58/EC、EPPO 理事会規則及び PNR 指令(EU) 2016/681（OJ L 119, 4.5.2016, p.132-149）を含め、個人データ保護と関連する特別法令及び関連法令の（法理論上及び法適用上の）位置づけを理解しなければならない。

	EU の機関及び組織	構成国の行政機関
一般行政機関	規則(EU) 2018/1725	GDPR
警察関係の行政機関		指令(EU) 2016/680

規則(EU) 2018/1725 の第 22 条第 2 項は、非常に重要である。データ主体は、自らが提供した個人データのセットを管理する行政機関から行政機関ではない管理者（プロバイダ等）に対してその個人データのセットを直接に送信させて当該個人データのセットを移転する権利（データ可搬性の権利）をもつ。この場合、個人データのセットの移転であるので、原則として、移転元の行政機関にはその個人データのセットが残されない。

ところが、日本国の個人情報保護法（平成 15 年法律第 57 号）、行政機関個人情報保護法（平成 15 年法律第 58 号）及び独立行政法人等個人情報保護法（平成 15 年法律第 59 号）には、このような場合を想定した条項が存在しない。このことは、自治体の個人情報保護条例でも基本的には同じである。これらの点を含め、これらの日本国の個人情報保護法令の大規模な法改正が必至である。

ただし、日本国において仮に必要な法改正または条例改正が実施されたとしても、行政機関による個人情報の処理業務の目的及び特質に鑑み、現実には、個人データの本人からの公共の利益（公共の福祉）を理由とするデータ可搬性（データポータビリティ）の権利の行使に対する拒否が正当なものとして認められる場合が圧倒的に多いであろうということは、想定しておく必要がある（規則(EU) 2018/1725 の第 22 条第 3 項参照）。それと同時に、公共の利益（公共の福祉）を全く度外視した「自由放任」という意味で完全に無制約な個人データの「自由な移転」または「自由な移動」を認めるような法令は、EU の個人データ保護法令と抵触するものであることは無論のこと、日本国の法令それ自体としても日本国憲法に定める関連人権保障条項に違反する無効な

法令である。

一般に、個人データの「可搬性（ポータビリティ）」は、日本国において喧伝されているいわゆる「情報銀行」等と称するものを介在させる情報流通とはその法的性質を全く異にするものである。それは、データ主体以外の者の経済的利益が関係をもつ余地を一切もたないし、データ主体以外の者のデータアクセスを認めるものでもない。つまり、個人データのいわゆる「利活用」（特に何らかの経済的利益を生み出す利用形態）とは一切関係のない制度である。無論、データの移転を補助するサービスが存在することは許容され、データ主体の依頼により、それらのサービス提供者が関連する作業を提供することは認められる。しかし、原則として、データ主体からの要求のみに基づき、ある管理者から別の管理者へと直接に個人データのセットをまるごと移転する権利が認められる必要があることから、基本形としては、中間介在者が一切存在しない状態で自由に移転できる法制度を定める必要がある。つまり、この制度は、それ自体としては、何らビジネスチャンスを産むものではあり得ない。ところが、現実には、これら混同した解説等が存在するので、注意を要する。

正しくは、日本国の法制中には、EU の法令におけるのと全く均等な意味における個人データの「可搬性（ポータビリティ）」の制度を定める条項は、何も存在しない。この制度は、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）とも無関係の制度である。

一般に、本人の意思を無視し、単純に事業者の私的な経済的利益のみを目的として行われる個人データの取引行為に対しては、関連する消費者保護法の適用を含め、厳正な対処が検討されなければならない。それが本人の意思に基づく場合であっても、同意の撤回が行われた場合及び本人から削除の請求が行われた場合、当該データの全部削除及び当該事業者から（ビッグデータ事業者及び関連分析の事業者を含め）第三者に移転した当該本人の個人データの全面的な削除（忘れられる権利）の実装と徹底が必要である。日本国の関連法令中で既に定められている部分に関しては当然のこととして、それが日本国の法令中で定められていないものであるとしても、例えば、個人情報保護委員会の運用指針や JIS 規格等を通じて、そのような削除の権利の実質的な実装と執行が強力に推進されるべきである。以上のことは、独立行政法人等の場合であっても、その業務内容が一般の事業者と基本的に変わらない性質をもつ場合には、原則として同じである。ただし、その場合においても、一般的な事業者とは法的性質の異なる要素をもつには、その独立行政法人等における個人データ処理の特殊性を適正に考慮に入れなければならない。

なお、「portability」を「可搬性」と訳すべきか否かは当該の者の趣味の範囲に属する部分もあるが、その概念内容の理解のためには、EU の個人データ保護と関連する法令だけではなく、様々な分野において既にこの概念が使用されているという事実を明確に認識し、かつ、この概念が用いられている主要な法令を全部精読・理解し、その概念内容を正確に把握するための努力を重ねる必要がある。そのような関連法令としては、古典的には、通信関連の法制をあげるのが妥当である。通信関係の法制における電話番号の移転に関して「portability」の概念が用いられている。EU における最新の法令である欧州電子通信法指令(EU) 2018/1972（OJ L 321, 17.12.2018, p.36-214）の中では、電子メールアドレスの「portability」が定められている。通信法制以外の分野においても、例えば、オンラインコンテント可搬性規則(EU) 2017/1128（OJ L 168, 30.6.2017, p.1-11）がある。同規則における「可搬性」の概念は、構成国の国境を越えるアクセスと関連するものであり、個人データ保護法令における「可搬性」とは異なる概念内容をもつものである。この場合における権

利は、基本的には、（著作物であるコンテントの利用と関連する）契約に基づく権利である。データローカライゼーション規則(EU) 2018/1807（OJ L 303, 28.11.2018, p. 59-68）における「porting」の概念も類似の機能をもっている。EU の複数の構成国を移動する場合における社会保険（特に強制保険）関係の任意既払額相当額の還付請求の権利行使においても、また、付加価値税（VAT）の関係においても、その社会的目的または機能の本質は同じである。これら個人データ保護法令、通信関連法令及びオンラインコンテント可搬性法令等における「可搬性」のミニマムの共通点としては、異なる場所（地理的場所及び論理的な場所）に権利者が（地理的または論理的に）移動した場合でも、EU 法が適用される域内にある限り、その権利者が既に保有している権利を同一の条件下で行使し、その権利行使による利益を享受できることを制度的に保証するということに尽きる。

加えて、規則(EU) 2018/1725、GDPR 及び EU の関連ガイドライン等を読むと、個人データ保護の法令における「可搬性」の権利は、データ主体の個人データの管理（control）と関連する権利であることが明らかにされていることを理解できる。しかし、その権利が他者の権利や正当な利益を害することのできないものであり、かつ、公共の利益による制限に服するものであることも明確にされている。契約の締結及び履行のためにデータ主体から提供された個人データに関しては、可搬性の権利が行使された場合であっても、その個人データの管理者は、削除義務を負わない。つまり、可搬性の対象となるデータのセットは、もともと当該データ主体のみが専有するものであり、他に権利者や管理者には権利が存在しないようなものであることを要する。具体的には、貸金庫を借りている者がその貸金庫の中に収納している財のようなものだけが可搬性の対象となる。電子的なものとしては、クラウド上のストレージサーバの中でクラウド利用者が保管しているデータがそれに該当する（この場合、クラウドベンダは、当該ストレージサーバ内の利用者のデータに対して権利を取得することがないし、利用者の同意なく、そのデータにアクセスすることもできない。その意味で、可搬性の権利の行使は、クラウドベンダに対し、データの移動処理のために限定されたアクセス権を与える行為であると理解することも可能である）。自己が専有する情報財の管理を全て決定できることは当然のことであるので、「可搬性」は、いわゆる「自己情報コントロール権」のような考え方とは無縁のものであり、単に、財産権としての情報財の管理のための権利の一種として理解するのが正しい。当該の者がもともといかなる意味においても権利者でない場合、個人データの「可搬性」が問題とされるべき余地が全くない。このことはまた、そのような情報財の管理のためのサービスを提供する第三者が、当該情報財である個人データに関する権利を取得することがあり得ないということも意味する。そのような第三者が契約によって当該個人データの管理に関与する場合、民法を含め、一般的な契約法上の基本原則が適用され、かつ、当該データ主体が消費者である場合、消費者契約法を含め、消費者保護と関連する法令が適用されることは当然のことである。

規則(EU) 2018/1725 は、EU のオープンデータ政策とも非常に大きな関連性をもつ法令である。特に、G to G だけではなく、B to G のデータ移動に関して重要である。この関連の政策を明示する文書として、欧州データ空間通知 COM(2018) 232 final がある。

規則(EU) 2018/1725 の前文(5)にある欧州司法裁判所の判例法とは、*European Commission* v *Federal Republic of Germany*, Case C-518/07, 9 March 2010, ECLI:EU:C:2010:125 のことを指す。

（この参考訳を作成するに際し考慮した事項）

規則(EU) 2018/1725、一般データ保護規則(EU) 2016/679（GDPR）及び指令(EU) 2016/680 の「controller」は「管理者」と、「processor」は「処理者」と、「processing」は「処理」と訳さなければならない。

仮に「controller」を「事業者」または「取扱事業者」と訳した場合、「undertakings」や「operators」等と識別できず、同様に、「processing」を「取扱い」と訳した場合、「handle（handling）」、「treat（treatment）」及び「deal（dealing）」と識別できない。また、一般に、「事業者」とは、（公的組織ではない）民間の組織または個人のことを意味するが、規則(EU) 2018/172 及び指令(EU) 2016/680 において「controller」が使用される場合、他に形容詞または形容句が存在しない限り、その「controller」とは、（民間の組織または個人ではない）公的組織のことを意味すると解する以外にないので（規則(EU) 2018/172 の第 3 条(8)参照）、規則(EU) 2018/172 及び指令(EU) 2016/680 の文脈において、「controller」を「事業者」と訳すことは常に不可である。同様に、一般データ保護規則(EU) 2016/679（GDPR）は、構成国の行政機関にも適用され、当該行政機関が個人データを処理する場合、その個人データを処理する行機関は「controller」に該当することになるのであるが、これを（行政機関であるにも拘らず）「事業者」または「取扱事業者」と訳すことは常に明白な誤訳となる。

そして、それらの語の目的語または形容詞等が明示されていない限り、仮に「controller」を「事業者」と訳し、あるいは、「processing」を「取扱い」と訳すとすれば、それらの訳文全体が致命的に混乱し、少なくとも、一貫性のないものとなる危険性がある。例えば、規則(EU) 2018/1725、一般データ保護規則(EU) 2016/679（GDPR）及び指令(EU) 2016/680 の「controller」をそれぞれ別異に訳すとすれば、真実では全く同一の概念であるのに、表見的に異なる概念であるかのように見えてしまうことになる。そのことは、EU との関係において、日本国の国益を深刻に害する原因ともなり得る。法令用語の訳語の選択は、単なる趣味・嗜好では済まされないような局面があり得ることを正しく理解しなければならない。

そのような致命的な混乱が生ずることを認識できないこと、及び、そのような混乱を承知で（日本語としての）識別力のない訳文を使用することは、（EU の個人データ保護法制に関して無知またはそれをほとんど知らない場合を除き）法律専門家として、絶対に認められることではない。

以上のような私見に疑問をもつ者は、法と情報雑誌第 1 巻から第 3 巻までに収録した全法律文書（法令、条約、協定等）、全政策文書、全判例及びそれら以外の全文献資料について、全て自らの手で直接に全文翻訳してみれば良い。そのような全文翻訳の際に必要な熟慮を尽くせば、標準以上の知力をもつ者である限り、私見以外の見解が成立する余地など全くあり得ないことであるということを容易に納得できるであろう。その逆もまた真である。

それゆえ、この参考訳においても、「controller」は「管理者」と、「processor」は「処理者」と、「processing」は「処理」と訳すべきであるとの方針を堅持し、そのような前提で、この参考訳を作成することにした。

なお、「Member State」を「構成国」と訳すべきであり、「加盟国」と訳してはならない理由については、これまで何度も述べてきたとおりである。疑問に思う者は、上記同様に自ら訳出を試みると良い。

これらの点に関し、一般に、合理性及び論理性の全くない生の自尊心にこだわり続けることは、単なる我欲の一種に過ぎない。自戒の念をこめて、一般に、法学研究者は、常に謙虚であり続け、自らの無知を少しでも克服するための最善の努力を重ね続けるべきである。

「operational personal data」は、EU の機関及び組織が取扱う個々の刑事事件の共助業務において処理される被疑者等の個人データ（特に事件ファイル中にある個人データ）のことを指す。これに対し、「administrative personal data」は、「operational personal data」以外の個人データであり、行政機関としての

EU の機関及び組織の業務遂行上で処理される一般的な個人データ（例：EU の機関及び組織の職員の人事管理データ、EU の機関及び組織と外部者との間の契約と関連する個人データ、事件処理と直接関係のない通信における個人データ等）のことを指す。

この参考訳においては、便宜、「operational personal data」を「運用個人データ」と訳し、「administrative personal data」を「行政個人データ」と訳すことにした。

「erasure」と「delete」は、一般に、「削除」または「消去」として訳し得る。EU の関連法令中において、この 2 つの語が意識的かつ厳格に使い分けられているか否かに関し、非常に多数の関連法令を調べてきたが、結論としては、常に明確な一貫性をもって使い分けられているとは認め難い。同じ事柄を示すための単なる言い換えに過ぎないような用例も多々見られる。それゆえ、「erasure」と「delete」を「削除」または「消去」のいずれに訳すかは、あくまでも一般論としては、多分に、当該翻訳を行う者が認識・理解する法体系及び個人的な趣味の問題に属するものとして扱うことができないわけではない。

しかし、規則(EU) 2018/1725 に関する限り、「erasure」と「delete」が意識的に使い分けられていると考えるのが妥当であり、しかも、前文(51)、第 29 条第 3 項(g)及び第 87 条第 3 項(d)の論理構造からすれば、「erasure」を「削除」と訳し、「delete」を「消去」と訳す以外の選択肢が存在しないと考えられる。

そこで、この参考訳においては、従前の参考訳における訳語の選択とは多少異なる部分もあるが、「erasure」を「削除」と訳し、「delete」を「消去」と訳すこととし、そのように訳語を統一することにした。

「legal act」に関し、従前の参考訳においては、原則として「法的行為」と訳し、契約と対比して述べられている場合には「法律行為」と訳した。しかしながら、例えば、EU の機関の内部規則や特別法令のような標準約款と同じような法的性質をもつ EU の行為によって処理者が法的に拘束される場合があり得ると考えるに至った。その結果、「legal act」を「法律行為」と訳すことは、それが公法人の私法行為のみに限定される趣旨と誤解されるという意味で、不適切であると判断するに至った。

一般に、EU の機関の内部規則や特別法令は、通説に基づいて理解するとすれば、公法人の私法行為とは異なり、公法行為の一種である。ただし、従来の通説とは異なるが、私法と公法を分けて考えない見解に立脚する場合、「法律行為」が従来の通説の意味における私法行為に限定されることはないという解釈論を導出することになるであろう（私見としては、公法と私法の区分には特に実益のあるものではなく、行政機関等の行為の特殊性は、それ自体の本質的な属性であると説明するよりも、行政機関等の行為の執行方法や不服申立方法に関して特殊な特別法令が定められている結果に過ぎないと考えるほうが明快である。現実に、国や地方自治体の業務の非常に多くが民間企業に事務委託されている現状に鑑みると、公法と私法とを明確に区分し、相互に性質を異にするものであると解する行政法学及び憲法学上の通説は、全て廃止されるべきであり、それに代えて、公法と私法を区別せず、公法人と私法人（更には混合的な法人）の共通点と相違点とをより合理的に説明可能な理論体系が再構築されるべきである。それによって、憲法学に限定する場合においても、独裁者である個人が国家として一定の地理的範囲を実力支配する政治的情報というものが、公法とは無関係な単なる私有関係の一種に過ぎないということを明確にすることができるのである。このような独裁の状態であっても公法が存在するという前提で法解釈論を構築せざるを得ない現在の通説は、単に無意味であるというだけではなく、有害であることさえあり得る）。

以上を踏まえた上で、この参考訳においては、現時点ではまだ強力に維持されている憲法学及び行政法学上の通説における公法と私法の区分と矛盾しないようにするため、とりあえず、「legal act」を

一律に「法的行為」と訳すという方針に改めた。しかし、将来、現在の憲法学及び行政法学上の通説が消滅または崩壊した後には、その後の時点において優勢な法理論を基礎として、「legal act」の訳語の再検討が行われるべきである。

「type」は、全て「種類」と訳すことにした。「categories」は、全て「類型」と訳すことにした。

なお、「type」に関して、「種類」では語感が異なると考えるときは、「タイプ」とカタカナ表記するのにとどめるべきである。

「impact」及び「affect」は、いずれも「影響を及ぼすこと」または「影響」を意味するが、「impact」は、良い影響の場合と悪い影響の場合の両者を含む場合または中性的な場合が多いのに対し、「affect」は、主として悪い影響または負の影響のことを意味することが多い。

この参考訳においては、そのようなニュアンスの相違を意識した上で、適宜、訳し分けることにした。

「demonstrate」は、民事訴訟においては、証拠による「証明」のことを指すことが多い。しかし、規則(EU) 2018/1725 及び一般データ保護規則(EU) 2016/679（GDPR）においては、主として、「説明責任」の文脈において「demonstrate」が用いられている。この場合における「demonstrate」は、証拠によって裁判官を納得させる程度の優位性のある証明の程度を要求するものではなく、例えば、欧州データ保護監督官（EDPS）または構成国の監督機関から説明を求められた場合に、それらの機関を納得させる程度のものであることで足り、（関連法令によって書面によることが定められていない限り）当該管理者等による口頭の行為によっても実施可能であることから、そのような場合における「demonstrate」は、明らかに、「証明」ではない。

一般に、法律家ではない世俗の世界においては、「証明」との語を厳格に使用することが滅多になく、また、実際にはその必要性もなく、加えて、（職業翻訳家を含め）法律家ではない一般人または素人に対してそのような法律用語としての厳格性を求めることそれ自体がそもそも無理なことではある。しかしながら、こと法律文書の翻訳に関し、特に当該分野を所管する行政機関や職業法律家によって訳出される場合においては、その文書の中で用いられている語の法律用語としての厳格性を意識した訳語の選択が求められることは言うまでもないことである。このことは、専門分野に属する技術文書の翻訳においても同じである。一般論としては、可能な限り平易かつ明解な文の作成を心掛けるべきことは当然のこととして、（そもそも一般的な用語・用例等それ自体が誤っており、破棄、修正または無視されるべき場合を除き）当該専門分野における定義、用語、用例等を尊重すべきであり、義務教育レベルの「国語」を基準とすることは、間違いである。それゆえ、一般に、ある専門分野に属する文書の「翻訳」とは、基本的な一定水準以上の語学能力の存在を必須の前提とした上で、当該専門分野全体をどれだけ広く、かつ、深く理解し、どれだけ多くの関連知識をもっているかによって決定される作業である。そのような意味での専門知識を欠く限り、特定の語学能力検定試験の結果が良いか悪いかという事実は、それ自体としては、全く何の意味ももたない無意味な事柄に属する。一般に、若い学生は、可能な限り広い教養を修めつつ、各自の専門分野に関して徹底的に精通する努力を尽くすべきであり、その勉学の過程において、その専門分野における専門文献を読み解くために必要な語学を修得し、応用できるようになれば良いのである。その場合において、能力検定試験は、全く必要がない。日常会話だけなら小さな子どもでも容易に覚えられる。仕事上の会話能力は、自分の表現内容または思考内容が論理的に整合性のあるものとして確実に存在しており、かつ、当該言語の語彙が非常に豊富であり、用例

の理解が正確であれば、仕事の現場における日々の努力を重ねることにより、オンジョブで習得可能である。仮に会話能力が十分ではない場合であっても、当該の者の思想内容が真に優れたものである場合には、その分野に属する諸外国の専門家が競ってその翻訳に勤しむことになるであろう。特に記号論理学上の整合性の高い表現物（例：技術仕様書、技術説明書等）は、AI を応用した自動翻訳または自動通訳の対象に適しているので、いずれ、当該表現物の表現者自身が外国語会話能力を修得する必要性が存在しなくなることであろう。

ちなみに、一般に、各自の専門分野における勉学の過程において、個々の専門分野の研究遂行のために要求される水準の語学力を自力（独学）で獲得できない者は、少なくとも、その者の人生設計において、専門的な研究者としての道を進むことを諦めるべきである。一般に、専門的な学術研究の分野は、常に独学だけで構成されている。誰か他の先生から教えられることを待ち望み、教えられた内容を複製または模倣して成果物を作成することばかりというのでは、学術研究における精神とは明らかに相反する堕落した心理である。学術の分野においては、（優れた職業裁判官がそうであるのと同様に）孤立や孤独を怖れない強靭かつ孤高の精神構造が求められる。

以上を踏まえた上で、この参考訳においては、従前と同様、「demonstrate」を「説明」と訳すことにした。

ただし、その「説明」が十分なものであるか否かが民事訴訟または行政訴訟において争われる場合、当該国において一般的に採用されている証明責任の基本原則に則り、その「説明」の合理性が証拠によって「証明」されなければならない。

法令の「application」は、その適用開始のことまたはその適用開始の時点を指すときは「施行」と訳すことが可能である。しかし、EU の法令においては、適用開始時点以降、適用終了までの全期間を通じて「application」が用いられるので、（EU の法令における制度が日本国の法令における制度と全く同一であるとの初歩的な）誤解を避けるため、「application」を「施行」ではなく「適用」と訳すのが妥当である。

他方、行政手続等の申請または申立ての場合においては、「application」は、「申請書」、「申立書」またはそれらの文書の提出行為のことを意味する。

これらの諸点を踏まえ、この参考訳においては、「application」に関し、法令との関係においては「適用」と訳し、それ以外の場合には適宜訳し分けるという従来の方針を維持することにした。

「decision」は、文脈により、「判断」、「決定」または「判定」である。「認定」とは訳さない。EU の法令においては、原則として、「accreditation」の場合に「認定」との訳語を用いる。

規則(EU) 2018/1725 及び一般データ保護規則(EU) 2016/679（GDPR）においては、「vital」は、「生存」である。「生命」を示すためには「life」が用いられる。例えば、規則(EU) 2018/1725 の前文(6)の「vital interests, including physical integrity or life」がその典型的な用例である。

規則(EU) 2018/1725 の前文及び条文の中には、一般データ保護規則(EU) 2016/679（GDPR）の前文及び条文と同一のものが含まれている。GDPR に関しては、その時点において利用可能な資料等を全て駆使し、その時点において最善と判断する参考訳を提供し、その改訂を重ねてきたが、この規則(EU) 2018/1725 の参考訳中においては、GDPR の対応する原文の文言と同一の文言に関し、従前の GDPR の参考訳中の訳文と若干異なる部分がある。そのような部分は、従前の参考訳及びその改定版の作成のための検討後に行われた更なる検討を踏まえたものである。それゆえ、そのような部分は、

GDPR の参考訳の最新版としての機能も果たしている。GDPR に関しては、比較的近い将来、更に改訂を加えた参考訳（確定版）を作成できる見込みである。

規則(EU) 2018/1725 の前文(43)の中において、「subject. and prevent」とある部分は、誤記の一種と推定されるが、合理的に解釈した上で翻訳することにした。

以上のほかは、後掲一般データ保護規則(EU) 2016/679（GDPR）の参考訳・再訂版、後掲 EPPO 理事会規則(EU) 2017/1939 の参考訳、後掲規則(EC) No 45/2001 の改正案の参考訳の各冒頭部分で述べたとおりである。

（訳出済みの関連法令等及び参考文献）

一般データ保護規則(EU) 2016/679（GDPR）の参考訳・再訂版は、法と情報雑誌 3 巻 5 号 1～114 頁にある。規則(EC) No 45/2001 の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 111～146 頁にある。規則(EC) No 45/2001 の改正案の参考訳は、法と情報雑誌 2 巻 4 号 249～354 頁にある。e プライバシー指令 2002/58/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 158～187 頁にある。EPPO 理事会規則(EU) 2017/1939 の参考訳は、法と情報雑誌 3 巻 1 号 1～91 頁にある。指令 (EU) 2016/680 の参考訳は、法と情報雑誌 2 巻 1 号 41～140 頁にある。PNR 指令(EU) 2016/681 の参考訳は、法と情報雑誌 2 巻 3 号 119～155 頁にある。

EPPO 理事会規則(EU) 2017/1939 の参考訳は、法と情報雑誌 3 巻 1 号 1～91 頁にある。Europol 規則(EU) 2016/794 の参考訳は、法と情報雑誌 2 巻 3 号 1～101 頁にある。

決定 No 1247/2002/EC の参考訳は、法と情報雑誌 2 巻 4 号 355～360 頁にある。規則(EU) No 182/2011 の参考訳は、法と情報雑誌 3 巻 5 号 168～179 頁にある。規則(EC) No 1049/2001 の参考訳は、法と情報雑誌 2 巻 3 号 102～118 頁にある。理事会指令 93/13/EEC の参考訳は、法と情報雑誌 3 巻 11 号 143～152 頁にある。理事会決定 2009/917/JHA の参考訳は、法と情報雑誌 2 巻 2 号 1～30 頁にある。

データローカライゼーション規則(EU) 2018/1807 の参考訳は、法と情報雑誌 4 巻 1 号 82～100 頁にある。指令(EU) 2015/1535 の参考訳は、法と情報雑誌 3 巻 7 号 1～20 頁にある。オンラインコンテント可搬性規則(EU) 2017/1128 の参考訳は、法と情報雑誌 3 巻 6 号 114～132 頁にある。欧州データ空間通知 COM(2018) 232 final の参考訳は、法と情報雑誌 3 巻 10 号 107～127 頁にある。

この参考訳を作成するに際しては、上記各参考訳の冒頭部分に掲記した参考文献等のほか、個人情報保護委員会訳「データポータビリティの権利に関するガイドライン」（個人情報保護委員会 Web サイト・2019 年 1 月 1 日確認）を参考にした。

＊＊＊

欧州連合の機関、組織、事務局及び部局による個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725

欧州議会及び欧州連合の理事会は、
欧州連合の機能に関する条約、とりわけ、その第 16 条第 2 項に鑑み、
欧州委員会からの提案に鑑み、
構成国の議会に対して立法提案を送付した後、
欧州経済社会委員会の意見書に鑑み[1]、
通常の立法手続に従って審議し[2]、
以下のとおりであるので、この規則を採択する。

(1) 個人データの処理と関連する自然人の保護は、基本的な権利の 1 つである。欧州連合基本権憲章（「憲章」）の第 8 条第 1 項及び欧州連合の機能に関する条約（TFEU）の第 16 条第 1 項は、全ての者が彼または彼女に関する個人データの保護の権利をもつと定めている。この権利は、人権及び基本的自由の保護に関する欧州条約の第 8 条の下においても保障されている。

(2) 欧州議会及び理事会の規則(EC) No 45/2001[3]は、自然人に対して法的に執行可能な権利を提供し、欧州共同体の機関及び組織内の管理者のデータ処理上の義務を定め、そして、欧州連合の機関及び組織による個人データの処理の監視について職責を負う独立の監督機関、すなわち、欧州データ保護監督官を創設している。しかしながら、この規則は、欧州連合法の適用範囲の外にある欧州連合の機関及び組織の活動の過程における個人データの処理に対しては、適用されない。

(3) 欧州議会及び理事会の規則(EU) 2016/679[4]及び欧州議会及び理事会の指令(EU) 2016/680[5]は、2016 年 4 月 27 日に採択された。規則が、個人データの処理と関連する自然人を保護し、かつ、欧州連合内における個人データの支障のない移動を確保するための一般的な規則を定める一方、指令は、刑事に関する司法共助及び捜査共助の分野において、個人データの処理と関連する自然人を保護し、かつ、欧州連合内における個人データの支障のない移動を確保するための特別規定を定めている。

(4) 規則(EU) 2016/679 は、欧州連合内における強力かつ一貫性のあるデータ保護の枠組みを提供し、かつ、規則(EU) 2016/679 と同時に適用できるようにするため、規則(EC) No 45/2001 を調整す

---

[1] OJ C 288, 31.8.2017, p.107.

[2] 欧州議会の 2018 年 9 月 13 日付け意見書（官報未登載）及び理事会の 2018 年 10 月 11 日付け決定。

[3] 欧州共同体の機関、組織、事務局及び部局による個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する規則(EC) No 45/2001 (OJ L 8, 12.1.2001, p.1).

[4] 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）（OJ L 119, 4.5.2016, p.1）

[5] 犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行に関する職務権限を有する機関による個人データの処理と関連する自然人の保護及びそのデータの支障のない移動、並びに、理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/680（OJ L 119, 4.5.2016, p.89）

ることを定めている。

(5) 欧州連合の機関、組織、事務局及び部局のためのデータ保護法令と構成国の公的部門のために採択されたデータ保護法令とを可能な限り揃えることは、欧州連合を通じて一貫性のある個人データ保護の取り組みにとって利益となることである。この規則の条項が規則(EU)2016/679 の条項と同じ基本原則に従う場合、これら 2 つのセットの条項は、欧州連合の司法裁判所（「司法裁判所」）の判例法の下において、とりわけ、この規則の制度が規則(EU)2016/679 の制度と均等なものとして理解されなければならないという理由により、均質のものとして解釈されなければならない。

(6) 例えば、欧州連合の機関及び組織によって彼らが雇用されているという理由により、欧州連合の機関及び組織によってその個人データが処理される者は、いかなる過程においてそうであるにせよ、保護されなければならない。この規則は、死亡した者の個人データの処理には適用されない。この規則は、法人の名称及び形態並びにその法人の連絡先を含め、法人と関係する個人データの処理、とりわけ、法人として設立された事業者と関係する個人データの処理をその適用対象としていない。

(7) 回避という重大なリスクを生むことを防止するため、自然人の保護は、技術的に中立なものであるべきであり、用いられる技術に依存するものであってはならない。

(8) この規則は、欧州連合の全ての機関、組織、事務局及び部局による個人データの処理に適用されなければならない。この指令は、その全部または一部が自動的な手段による個人データの処理に対して、並びに、個人データがファイリングシステムの一部を構成している場合またはファイリングの一部を構成する予定である場合、自動的な手段による処理以外の処理に対して適用されなければならない。特定の基準に従って構成されてないファイルまたはファイルのセット並びにその表紙は、この規則の適用の範囲内にあるものとしてはならない。

(9) リスボン条約を採択した政府間会議の最終合意書に添付された刑事に関する司法共助及び捜査共助の分野における個人データの保護に関する第 21 号宣言の中において、同会議は、その分野の特殊な性質のゆえに、TFEU の第 16 条に基づく刑事に関する司法共助及び捜査共助の分野における個人データの保護及び個人データの支障のない移動に関する特別の規定が明らかに必要となり得るということを認めた。それゆえ、刑事に関する司法共助及び捜査共助の分野において活動を実施する場合、欧州連合の組織、事務局または部局による刑事上の捜査の目的のために処置される個人データのような運用個人データの処理に対しては、一般的な規定を含むこの規則の異なる章が適用されなければならない。

(10) 指令(EU) 2016/680 は、公共の安全への脅威に対する防護及びその防止を含め、犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行の目的のために処理される個人データの保護及びその支障のない移動のための整合化された規定を定めている。欧州連合の全域において適法に執行可能な権利を介して自然人の同じレベルの保護を確保するため、そして、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する欧州連合の組織、事務局または部局と職務権限を有する機関との間の個人データの交換を妨げる格差を避けるため、そのような欧州連合の組織、事務局または部局によって処理される運用個人データの保護及びその支障のない移動のための規定は、指令(EU) 2016/680 と一貫性のあるものでなければならない。

(11) 運用個人データの処理に関するこの規則の章の一般規定は、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合に欧州連合の組織、事務局及び部局による

運用個人データの処理に適用される特別規定を妨げることなく、適用される。そのような特別規定は、運用個人データの処理に関するこの規則の章の中にある条項に対する特別法とみなされなければならない（特別法は一般法を破る）。法令の断片化を避けるため、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合に欧州連合の組織、事務局及び部局による運用個人データの処理に適用される特別の個人データ保護の規定は、運用個人データの処理に関するこの規則の章を支える基本原則、並びに、独立の監督、救済、法的責任及び制裁と関連するこの規則の条項と一貫性のあるものでなければならない。

(12) 運用個人データの処理に関するこの規則の章は、犯罪行為の防止、検知、捜査または訴追の目的のために、それらの機関がそれらの機関の主たる職務としてその活動を実施するのか、または、付随的な職務として実施するのかを問わず、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合の欧州連合の組織、事務局及び部局に対して適用されなければならない。ただし、それらの機関に対して運用個人データの処理に関するこの規則の章を修正されたとおりに適用できるようにするため、Europol 及び欧州検事局を設置する法的行為が改正されるまで、その章を Europol または欧州検事局に対して適用してはならない。

(13) 欧州委員会は、この規則の見直し、とりわけ、運用個人データの処理に関するこの規則の章の見直しを実施しなければならない。欧州委員会は、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合の欧州連合の組織、事務局及び部局による運用個人データの処理を規律する諸条約に基づいて採択された他の法的行為の見直しも実施しなければならない。そのような見直しの後、個人データの処理と関連する自然人の統一的かつ一貫性のある保護を確保するため、欧州委員会は、それを Europol 及び欧州検事局に対して適用するため、運用個人データの処理に関するこの規則の章の必要な修正を含め、適切な立法提案をすることもできるものとすべきである。その修正は、独立の監督、救済、法的責任及び制裁と関連する条項を考慮に入れなければならない。

(14) TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する欧州連合の組織、事務局及び部局による、職員のデータのような、行政個人データの処理は、この規則の適用範囲内にあるものとしなければならない。

(15) この規則は、欧州連合条約（TEU）の第 V 款の第 2 章の適用範囲内にある活動を実施する欧州連合の機関、組織、事務局または部局による個人データの処理に適用されなければならない。この規則は、共通の安全保障及び防衛政策を実装する TEU の第 42 条第 1 項及び第 44 条に示す任務による個人データの処理には適用してはならない。それが適切なときは、共通の安全保障及び防衛政策の分野における個人データの処理を別個に規律するため、関連提案が提出されなければならない。

(16) データ保護の基本原則は、識別された自然人または識別可能な自然人に関する全ての情報に対して適用されなければならない。追加情報の使用によって、ある自然人に割当てられ得る仮名化された個人データは、識別可能な自然人に関する情報として理解されなければならない。ある自然人が識別可能であるかどうかを判断するためには、選別のように、その自然人を直接または間接に識別するために管理者またはそれ以外の者によって用いられる合理的な可能性のある全ての手段を考慮に入れなければならない。自然人を識別するために手段が用いられる合理的な可能性があるか否かを判定するためには、処理の時点において利用可能な技術及び技術発展を考慮に入れた上で、識別のために求められる費用額及び時間量のような全ての客観的な要素

を考慮に入れなければならない。それゆえ、データ保護の基本原則は、匿名の情報、すなわち、識別された自然人または識別可能な自然人と関係のない情報、または、データ主体を識別できないようにする方法で匿名化された個人データに対しては、適用してはならない。それゆえ、この規則は、統計の目的または調査研究の目的を含め、そのような匿名情報の処理と関係するものではない。

(17) 個人データに対して仮名化を適用することは、関係するデータ主体に対するリスクを削減し得るものであり、また、管理者及び処理者が彼らのデータ保護上の義務に適合することを助けるものである。この規則における「仮名化」の明示の導入は、それ以外のデータ保護手段を排除することを意図するものではない。

(18) 自然人は、インターネットプロトコルアドレス、cookie 識別子、または、無線識別タグのようなその他の識別子のように、彼らの装置、アプリケーション、ツール及びプロトコルによって提供されるオンライン識別子と関連付けられ得る。これは、とりわけ、サーバによって受信されるユニークな識別子その他の情報と組み合わされるときは、自然人のプロファイルをつくり出し、そして、自然人を識別するために用いられる追跡の余地を残し得るものである。

(19) 同意は、電子的な手段による場合を含め、書面による陳述または口頭による陳述のように、彼または彼女と関連する個人データの処理に対するデータ主体の合意の、任意に与えられ、特定され、事前に説明を受け、不明瞭ではない表示を構成する明らかに肯定的な行為によって与えられる。この同意は、インターネット上の Web サイトを訪問する際にボックスをチェックすること、情報社会サービスのための技術的な設定を選択すること、または、この文脈において、彼または彼女の個人データの予定された処理についてのデータ主体の承諾を明確に示す上記以外の陳述または行為を含み得る。それゆえ、沈黙、予めチェック済みのボックスまたは不作為は、同意を構成するものとしてはならない。同意は、同一の目的のために行われる全ての処理活動に対して与えられるべきである。処理が複数の目的をもっている場合、同意は、それら全ての目的に対して与えられなければならない。データ主体の同意が電子的な手段による要求の後に与えられる場合、その要求は、明確であり、理解しやすく、かつ、提供されるサービスの利用を不必要に損なわないものでなければならない。それと同時に、データ主体は、その撤回前の同意に基づく処理の適法性を害することなく、いつでも、その同意を撤回する権利をもつものとしなければならない。同意が任意で与えられることを確保するため、データ主体と管理者との間において明らかな不均衡が存在しているため、当該個々の状況の全ての場合において当該同意が任意に与えられたものではない可能性が存在する個々の場合において、同意は、個人データの処理のための有効な法的根拠を与えるものとしてはならない。データ収集の時点において、科学調査の目的のための個人データ処理の目的を全て特定することが不可能であることがしばしばある。それゆえ、データ主体は、科学調査に関する承認された倫理基準を維持している場合、科学調査研究の一定の分野に対する彼らの同意を与えることが許容されなければならない。データ主体は、予定された目的によって許容される範囲内で、一定の調査研究の分野に対してのみ、または、調査研究プロジェクトの一部に対してのみ、彼らの同意を与える機会をもつものとしなければならない。

(20) いかなる個人データの処理も、適法かつ公正でなければならない。彼らに関する個人データが収集され、利用され、調査され、または、その他の処理をされていること、及び、どの範囲の個人データが処理されており、または、処理されることになるのかが、自然人に対して明らかにされなければならない。透明性の原則は、それらの個人データの処理と関連する情報及び連絡に容易

にアクセスできること及び容易に理解できること、そして、明確でわかりやすい文言が用いられることを要求する。この基本原則は、とりわけ、管理者の識別名及び処理の目的、並びに、関係する自然人を尊重する公正かつ透明性のある処理及び処理されている彼らに関する個人データの確認及び連絡を得る彼らの権利を確保するための別の情報に関する、データ主体に対する情報提供と関係している。自然人は、個人データの処理と関連するリスク、法令、安全性確保措置及び権利、並びに、その処理と関連する彼らの権利をどのように行使するかについて、知らされなければならない。とりわけ、個人データを処理するための個々の目的は、その個人データの収集の時点において、明示のものであり、正当なものであり、かつ、確定されたものでなければならない。個人データは、それが処理される目的のために十分であり、関連性があり、それに必要な範囲に限定されるものでなければならない。このことは、とりわけ、その個人データが記録保存される期間が厳格にミニマムな範囲に制限されることを確保することを要求する。個人データは、その処理の目的が他の手段によっては合理的に満たされない場合においてのみ、処理されるものとしなければならない。個人データが必要な範囲を超えて保存されないことを確保するため、削除または定期的な見直しのための期限が管理者によって定められなければならない。不正確な個人データが訂正または消去されることを確保するための全ての合理的な手立てが講じられなければならない。個人データは、個人データ及びその処理に用いられる装置への無権限のアクセスまたはその使用を防止するための場合、並びに、その個人データが送受信される際の無権限の開示を防止するための場合を含め、個人データの適切な安全性及び機密性を確保する態様で、処理されなければならない。

(21) 説明責任の原則に従い、欧州連合の機関及び組織が、欧州連合の同じ機関または組織の内部において個人データを送信し、その取得者が管理者の立場にない場合、または、欧州連合の別の機関または組織に対して送信する場合、その機関または組織は、その取得者の職務権限内にある職務の正当な遂行のためにその個人データが求められているのか否かを確認しなければならない。とりわけ、取得者から個人データ送信の要請を受けた後、管理者は、取得者による個人データの適法な処理のための関連する根拠が存在することを確認しなければならない。管理者は、そのデータの送信の必要性について、暫定的な評価も行わなければならない。その必要性について疑問が生ずるときは、管理者は、取得者から更に情報の提供を求めなければならない。取得者は、データの送信の必要性が事後的に検証可能なものであることを確保しなければならない。

(22) 処理が適法であるために、個人データは、公共の利益において、もしくは、欧州連合の機関及び組織の公的権限の存在において実施されるそれらの機関及び組織による職務の遂行のための必要性を基礎として、管理者が服すべき法律上の義務の遵守のための必要性を基礎として、または、関係するデータ主体の同意、もしくは、データ主体が当事者となっている契約の履行のための必要性、もしくは、契約の締結に入る前にデータ主体の申込みの際の手立てを講ずるための必要性を含め、この規則の下における上記以外の幾つかの正当な根拠を基礎として、処理されなければならない。欧州連合の機関及び組織による公共の利益において行われる職務の遂行のための個人データの処理は、それらの機関及び組織の運営及び稼働のために必要となる個人データの処理を含む。データ主体の生活または他の自然人の生活にとって本質的な利益を保護する必要性がある場合においても、個人データの処理は、適法とみなされなければならない。他の自然人の生存の利益を根拠とする個人データの処理は、原則として、その処理が別の法的

根拠に基づくことができないことが明らかである場合においてのみ、実施されるものとしなければならない。例えば、感染症及びその拡大の監視、または、とりわけ、自然災害及び人為的な災害の状況下における人道上の緊急事態を含め、人道上の目的のために処理が必要となる場合のように、幾つかの種類の処理は、公共の利益及びデータ主体の生存の利益という重要な法的根拠を同時にもつことがあり得る。

(23) この規則の中に示す欧州連合の法律は、明確かつ正確なものでなければならず、また、その適用は、憲章並びに人権及び基本的自由に関する欧州条約の中に定める諸要件に従い、データ主体にとってそれが予見可能なものでなければならない。

(24) この規則の中に示す内部規則は、データ主体それぞれとの関係において法的効果を発生させることを意図する一般的な適用のある明確かつ詳細な法的行為でなければならない。それらの内部規則は、欧州連合の機関及び組織の管理運営の最も高いレベルにおいて、その権限の範囲内で、かつ、その業務遂行と関連する事項について、採択されるものでなければならない。それらの規則の適用は、憲章並びに人権及び基本的自由に関する欧州条約の中に定める諸要件に従い、その規則に服する者にとってそれが予見可能なものでなければならない。内部規則は、とりわけ、欧州連合の機関によって採択される場合、決定の方式を採ることができる。

(25) その個人データが最初に収集された目的以外の目的のための個人データの処理は、その処理が、その個人データが最初に収集された目的と適合する場合においてのみ許容されるものとしなければならない。そのような場合、その個人データの収集を許容した法的根拠とは別の法的根拠は、要求されない。公共の利益において、もしくは、管理者に与えられた公的権限の行使において実施される職務の遂行のために処理が必要となる場合、欧州連合法は、別の目的による処理が適合し、かつ、適法とみなされるための職務及び目的を決定及び指定できる。公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のための別の目的による処理は、適合性のある適法な処理業務であると判断されなければならない。個人データの処理のために欧州連合法が定める法的根拠は、別の目的による処理のための法的根拠を提供するものでもあり得る。別の目的による処理の目的が、その個人データが最初に収集された目的と適合するものであるか否かを確認するため、管理者は、最初の処理の適法性のための全ての要件を検討した後、就中、以下の事柄を考慮に入れなければならない：すなわち、当初の目的と予定されている別の処理の目的との関連性；個人データが収集された過程、とりわけ、その別の目的に関して、管理者とデータ主体との関係に基づくデータ主体の合理的な期待；個人データの性質；予定されている別の目的による処理によってデータ主体に生ずる結果；並びに、当初の処理業務及び予定されている別の目的による処理の両者における適切な安全性確保措置の存在である。

(26) 処理がデータ主体の同意を基礎とするものである場合、管理者は、データ主体がその処理業務に対して同意を与えたことを説明できなければならない。とりわけ、別の事柄に関する書面による宣言の過程においては、その安全性確保措置は、同意が与えられることになるという事実及びその同意の範囲についてデータ主体が気づくことを確保しなければならない。理事会指令 93/13/EEC[1]に従い、管理者によって予め作成された同意の宣言は、理解しやすく、容易にアクセスできる方式により、明瞭かつ平易な文言を用いて提供されなければならず、かつ、不公正な条

[1] 消費者契約における不公正な条件に関する 1993 年 4 月 5 日の理事会指令 93/13/EEC（OJ J 95, 21.4.1993, p.29）

件を含むものであってはならない。同意が通知されるために、データ主体は、少なくとも、管理者の識別名、及び、その個人データについて予定されている処理の目的を認識していなければならない。データ主体が真正または任意の選択肢をもたない場合、または、データ主体が不利益を受けることなくその同意を拒否または撤回できない場合、その同意は、任意に与えられたものとみなされてはならない。

(27) 子どもは、リスク、結果及び関係する安全性確保措置、並びに、個人データの処理と関連する彼らの権利を十分に認識できないため、彼らの個人データに関して特別の保護を受ける。とりわけ、個人間通信サービスまたはオンラインでのチケット販売のように、欧州連合の機関及び組織の Web サイト上で子供に対してサービスが直接に提示され、個人データの処理が同意に基づくものである場合、子どもと関連する個人プロファイルの作成及び個人データの収集に対し、そのような特別の保護が適用されなければならない。

(28) 欧州連合の機関及び組織以外の欧州連合内で設立された取得者が、欧州連合の機関及び組織から取得者に対して個人データを送付させようとする場合、それらの取得者は、公共の利益において、または、それらの取得者の与えられた公的な権限の行使において実施される彼らの職務の遂行のために、それらの取得者に対してデータが送信される必要性があることを説明しなければならない。代替的に、それらの取得者は、公共の利益における個別の目的のためにその送信が必要であることを説明しなければならず、かつ、管理者は、データ主体の正当な利益が損なわれるおそれがあると推定すべき理由が存在するか否かを判断しなければならない。そのような場合、その管理者は、要求された個人データの送信の比例性を評価するため、様々な競合する利益を説明可能なように評定しなければならない。公共の利益における個別の目的は、欧州連合の機関及び組織の透明性と関係するものであり得る。更に、欧州連合の機関及び組織は、それらの機関及び組織自身が、透明性の原則及び良い行政の原則を遵守し、送信を開始する場合、そのような必要性を説明しなければならない。欧州連合の機関及び組織以外の欧州連合内で設立された取得者に対する送信に関してこの規則に定める要件は、適法な処理の条件を補完するものとして理解されなければならない。

(29) その性質上、基本的な権利及び自由との関係において特に機微な個人データは、そのデータの処理の過程が基本的な権利及び自由に対する深刻なリスクをつくり出し得るものであるので、特別の保護を受ける。そのような個人データは、この規則に定める特定の条件に適合するものでない限り、処理されてはならない。それらの個人データは、人種的または民族的な出自を明らかにする個人データを含める。この規則の中における「人種的な出自」という用語の使用は、それによって、異なる人種が存在することを決定しようとする思想を欧州連合が認めているということを意味するものではない。自然人のユニークな識別または本人確認のできる特別な技術的手段を用いて写真が処理される場合においてのみ生体データの定義の適用があるので、写真の処理は、特別類型の個人データの処理であると自動的に判断してはならない。機微のデータの処理のための個々の要件に加え、とりわけ、適法な処理のための条件と関連するこの規則の一般原則及び上記以外の規定が適用されなければならない。そのような特別類型の個人データの処理に関する一般的禁止からの特例は、就中、データ主体がどこで彼または彼女の明示の同意を与えた場合、または、その特別の必要性に関し、とりわけ、その目的が基本的な権利の行使を許容するためのものである一定の団体もしくは協会による正当な活動の過程において処理が実施される場合を明示で定めなければならない。

(30) より高度な保護を受ける特別類型の個人データは、とりわけ、医療及び社会福祉のサービス及び制度の運営の過程において、自然人及び社会全体の利益のための目的を達成するために必要な場合に限り、健康と関連する目的のために処理されるものとしなければならない。それゆえ、この規則は、個別の必要性との関係において、とりわけ、そのデータの処理が、職業上の法的な守秘義務に服する者によって健康と関連する一定の目的のために実施される場合において、健康と関係する特別類型の個人データの処理に関する整合化された条件を定めなければならない。欧州連合法は、基本的な権利及び自然人の個人データが保護されるようにするため、個別的かつ適切な措置を定めなければならない。

(31) 特別類型の個人データの処理は、公衆衛生の分野において、データ主体の同意なしに、公共の利益を理由として、必要となることがある。そのような処理は、自然人の権利及び自由を保護するための適切な個別の措置によらなければならない。この場合、「公衆衛生」とは、欧州議会及び理事会の規則 No 1338/2008[1]に定義されているように、すなわち、疾病率及び障害、健康状態に影響を与える素因、医療の必要性、医療に割り当てられる資源、医療の提供及び医療へのユニバーサルアクセス、並びに、医療並びに医療の支出及び資金手当、そして、死亡原因を含め、健康に関する全ての要素、換言すると、健康状態のこととして解釈されなければならない。そのような公共の利益を理由とする健康と関係する個人データの処理は、個人データが第三者によって別の目的のために処理されるという結果をもたらしてはならない。

(32) 管理者によって処理される個人データが、管理者に対して自然人の識別を認めていない場合、そのデータ管理者は、この規則の条項を遵守するという目的だけのために、データ主体を識別するための追加情報を入手することを義務付けられてはならない。ただし、その管理者は、彼または彼女の権利の行使を支持するためにデータ主体から提供される追加情報の取得を拒んではならない。識別子は、例えば、クレデンティアルと同じような、認証の仕組みを介してオンラインサービスにログインするためにデータ管理者から提供され、データ主体によって使用されるデータ主体のデジタル識別子を含めるものとしなければならない。

(33) 公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のための個人データの処理は、この規則によるデータ主体の権利及び自由のための適切な安全性確保措置に服さなければならない。それらの安全性確保措置は、とりわけ、データのミニマム化の原則を確保するため、技術上及び組織上の措置が設けられることを確保しなければならない。公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のための個人データの別の目的による処理は、（例えば、データの仮名化のような）適切な安全性確保措置が存在することを条件として、データ主体の識別を許容しないデータ処理、または、許容されなくなったデータ処理によってそれらの目的を満たすことの実現可能性を管理者が評価したときは、実施される。欧州連合の機関及び組織は、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のために行われる個人データの処理のための安全性確保措置を定めなければならない。その安全性確保措置は、欧州連合の機関及び組織の業務遂行と関連する事項に関して欧州連合の機関及び組織によって採択される内部規則を含めることができる。

[1] 公衆衛生及び職場における健康と安全の欧州共同体統計に関する欧州議会及び理事会の 2008 年 12 月 16 日の規則 (EC) No 1338/2008（OJ L 354, 31.12.2008, p.70）

(34) 要求するための仕組み、並びに、該当するときは、とりわけ、個人データに対するアクセス及び訂正または削除を無料で得るための仕組み、並びに、異議を述べる権利の行使を含め、この規則に基づくデータ主体の権利の行使を容易にするため、書式が提供されなければならない。特に電子的な方法によって個人データが処理される場合、管理者は、電子的に要求を行うための手段も提供しなければならない。管理者は、遅滞なく、遅くとも 1 か月以内に、データ主体の要求に対して応答することを義務付けられ、かつ、管理者がその要求に応ずるつもりがない場合、その理由を与えなければならない。

(35) 公正かつ透明性のある処理の原則は、データ主体がその処理業務の存在及びその目的の情報提供を受けることを要求する。管理者は、データ主体に対し、その個人データが処理される個別状況及び過程を考慮に入れた公正かつ透明性のある処理を確保するために必要となる情報を更に提供しなければならない。更に、データ主体は、プロファイリングの存在及びそのようなプロファイリングから生ずる結果についても情報提供を受けるものとしなければならない。個人データがデータ主体から収集される際、そのデータ主体は、彼または彼女がその個人データの提供を義務付けられているのか否か、及び、彼または彼女がそのデータを提供しない場合に生ずる結果についても情報提供を受けるものとしなければならない。その情報は、容易に視認でき、分かりやすく、明確に理解できる態様によって、予定されている処理の意味のある概要を提供するための標準的なアイコンと組み合わせて提供され得る。アイコンが電子的に表示される場合、それらのアイコンは、機械読取可能なものでなければならない。

(36) データ主体と関連する個人データの処理と関係する情報は、データ主体からの収集の時点において、または、個人データが他の情報源から取得される場合、案件の状況の相違に応じて合理的な期間内に、彼または彼女に対して与えられなければならない。個人データが別の取得者に対して正当に開示される場合、そのデータ主体は、その個人データがその取得者に対して最初に開示される時に情報提供を受けるものとしなければならない。個人データが取得された目的とは別の目的のために管理者がその個人データを処理しようとする場合、その管理者は、別の目的による処理を開始する前に、そのデータ主体に対し、当該別の目的に関する情報及びその他の必要な情報を提供しなければならない。様々な情報源が用いられたために、データ主体に対してその個人データの情報源の情報を提供できない場合、一般的な情報が提供されなければならない。

(37) データ主体は、彼または彼女に関して収集された個人データにアクセスする権利をもち、かつ、その処理の適法性に注意を払い、それを検証するために、容易に、かつ、合理的な間隔で、その権利を行使するものとしなければならない。この権利は、データ主体の健康に関するデータ、例えば、診断、検査結果、治療担当医師による評価並びに提供された治療行為もしくは治療介入行為のような情報を含む彼らの医療記録中にあるデータにアクセスをもつためのデータ主体の権利を含む。それゆえ、全てのデータ主体は、とりわけ、その個人データが処理される目的、可能な場合、その個人データが処理される期間、その個人データの取得者、自動的な個人データ処理の中に含まれている論理、並びに、少なくともプロファイリングに基づく処理である場合、そのような処理の結果に関し、知る権利及び連絡を受ける権利をもつものとしなければならない。その権利は、営業秘密または知的財産及び特にソフトウェアの著作権保護を含め、他の者の権利または自由に対して負の影響を与えてはならない。ただし、そのような検討の結果は、データ主体に対する全ての情報の提供拒絶となるものであってはならない。管理者がデータ主体に関

する情報を大規模に処理する場合、その管理者は、その情報が提供される前に、その提供の要求と関連する情報または処理活動をデータ主体が特定するように要求できるものとすべきである。

(38) データ主体は、彼または彼女に関する個人データが訂正される権利、及び、そのようなデータを保持することがこの規則または管理者が服すべき欧州連合法に違反する場合、「忘れられる権利」をもつものとしなければならない。当該個人データが収集され、もしくは、それ以外の処理をされる目的との関連においてその個人データが必要なくなった場合、または、データ主体が彼もしくは彼女の同意を撤回し、もしくは、彼もしくは彼女に関する個人データの処理に対して異議を述べた場合、または、彼または彼女の個人データの処理がこの規則を何ら遵守するものではない場合、データ主体は、彼または彼女の個人データが削除され、処理されなくなる権利をもつものとしなければならない。この権利は、とりわけ、データ主体が、子どもの時に、その処理に含まれるリスクについて全て認識しないまま彼または彼女の同意を与えたけれども、後になって、そのような個人データの削除、特にインターネット上のデータの削除を望むようになった場合と関連するものである。データ主体は、彼または彼女が既に子どもではないという事実とは無関係に、その権利を行使できるものとすべきである。ただし、表現及び情報伝達の自由の権利の行使のために必要な場合、法律上の義務を遵守するために必要な場合、公衆衛生の分野における公共の利益を法的根拠として、公共の利益において、または、管理者に与えられた公的な権限の行使において行われる職務の遂行のために必要な場合、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のために必要な場合、または、訴訟の提起もしくは攻撃防御のために必要がある場合、別の目的のためにその個人データを保持することは、適法としなければならない。

(39) オンライン環境における忘れられる権利を強化するため、削除の権利は、その個人データを公開のものとした管理者が、当該個人データを処理している管理者に対し、当該個人データへのリンク、そのコピーまたは複製物を削除するように通知することを義務付けられるという方法によっても、拡張されるべきである。そのようにする場合、当該管理者は、利用可能な技術及びその管理者にとって利用可能な手段を考慮に入れた上で、技術的な措置を含め、そのデータ主体の要求対象である個人データを処理している管理者に対して通知をするための合理的な手立てを講じなければならない。

(40) 個人データの処理を制限するための手法は、就中、選別されたデータを一時的に他の処理システムに移転すること、選別された個人データを利用者が利用できないようにすること、または、公開されたデータを一時的に Web サイト上から除去することを含め得る。自動的なファイリングシステムにおいては、処理の制限は、原則として、その個人データが別の目的による処理業務の対象とされないようにし、かつ、修正されないようにする態様で、技術的な手段によって確保されなければならない。個人データの処理が制限されているという事実は、そのシステムの中で明確に表示されなければならない。

(41) 彼または彼女自身のデータに対する監視をより強化するため、個人データの処理が自動的な手段によって行われる場合、データ主体は、彼または彼女が管理者に対して提供した彼または彼女と関係する個人データを、構成され、一般に用いられ、かつ、機械読取可能かつ相互運用可能なフォーマットによって受信し、そして、その個人データを別の管理者に対して送信することが認められ得なければならない。データ管理者は、データの可搬性を可能とする相互運用可能なフォーマットを開発することを奨励されるべきである。この権利は、データ主体が彼もしくは彼女

の同意に基づいてその個人データを提供した場合に適用されなければならない。それゆえ、その権利は、管理者が服する法律上の義務を遵守するため、または、公共の利益において、もしくは、管理者に与えられた公的な権限の行使において行われる職務の遂行のために個人データの処理が必要となる場合においては、適用されない。彼または彼女と関係する個人データの送信または受信のためのデータ主体の権利は、管理者に対して、技術的に互換性のある処理システムの導入または維持すべき義務をつくり出してはならない。ある個人データのセットに複数のデータ主体が関係している場合、個人データを受信する権利は、この規則による他のデータ主体の権利及び自由を妨げてはならない。更に、この権利は、データ主体の個人データの削除を得る権利及びこの規則に定めるようなその権利の制限を妨げてはならず、また、とりわけ、当該契約の履行のために必要となる範囲内にある範囲内で、かつ、その限りで、契約の履行のために彼または彼女から提供されたそのデータ主体と関係する個人データの削除を意味するものとしはならない。技術的に実現可能な場合、データ主体は、ある管理者から別の管理者へと直接に個人データを送信させる権利をもつ。

(42) 公共の利益において、または、管理者に与えられた公的な権限の行使において行われる職務の遂行のために処理が必要であるという理由により、個人データが適法に処理され得る場合、それにも拘らず、データ主体は、彼または彼女の特別の状況と関連する個人データの処理に異議を述べる資格が与えられなければならない。管理者は、データ主体の基本的な権利及び自由よりも管理者の強制的な正当な利益のほうが優越することを説明しなければならない。

(43) データ主体は、人間が介在しない e リクルートのような、自動的な処理のみを基礎とし、かつ、彼もしくは彼女に関する法的効果を発生させ、または、彼もしくは彼女に対して類似の重大な影響を及ぼす、彼または彼女に関する人格的側面を評価する判定の対象とされない権利をもつものとしなければならない。その判定は、措置を含み得る。そのような処理は、その判定が、彼もしくは彼女に関する法的効果を発生させ、または、彼もしくは彼女に対して類似の重大な影響を及ぼす場合、とりわけ、データ主体の就労能力、経済状態、健康、個人的な嗜好または興味、信頼性または行動、位置または移動に関する側面を分析または予測するための、自然人に関する人格的側面を評価する何らかの形態の個人データの自動的な処理で構成される「プロファイリング」を含む。

ただし、プロファイリングを含め、そのような処理を基礎とする判定は、欧州連合法によって明示で認められる場合においては、許容されるものとしなければならない。いかなる場合においても、そのような処理は、適切な安全性確保措置に服さなければならず、その措置は、データ主体に対する個別の情報提供、人間の介在を得る権利、彼または彼女の見解を表明する権利、そのような評価の後に到達した判定の説明を受ける権利、そして、その判定に対して異議を述べる権利を含めなければならない。そのような措置は、子どもと関係するものであってはならない。データ主体に関する公正かつ透明性のある処理を確保するため、その個人データが処理される個別の状況及び過程を考慮に入れた上で、管理者は、プロファイリングのための適切な数学上または統計上の手順を使用し、かつ、とりわけ、個人データに内在する不正確さをもたらす諸要素が修正されること、及び、エラーのリスクがミニマム化されることを確保し、データ主体の利益及び権利と関連している潜在的なリスクを考慮に入れた態様により、そして、就中、自然人に対し、人種的もしくは民族的な出自、政治的な意見、信教もしくは信条、労働組合への加入、遺伝子もしくは健康状態、または、性的な指向に基づく差別的効果が生ずることを避ける方法により、または、その

ような効果をもつ措置を生じさせる処理を避ける態様により、個人データを防護するための適切な技術上及び組織上の手段を実装しなければならない。特別類型の個人データを基礎とする自動的な判定及びプロファイリングは、個別の条件の下においてのみ、許容されるものとしなければならない。

(44) 公共の安全の防護のため、並びに、犯罪行為の防止、捜査及び訴追または刑罰の執行を防護するため、民主主義社会において必要であり、かつ、比例的である限りにおいて、諸条約に基づいて採択された法的行為、または、その業務遂行と関連する事項について欧州連合の機関及び組織によって採択された内部規則は、個々の基本原則、情報提供の権利、個人データへのアクセスの権利及びその訂正もしくは削除の権利、データ可搬性の権利、電子通信データの秘密、並びに、データ主体に対する個人データ侵害の連絡、及び、管理者の一定の関連する義務に関し、制限を加えることができる。

　このことは、公共の安全、特に自然災害または人為的災害への対応における人間の生命の防護、欧州連合の機関及び組織の内部の安全、それら以外の、欧州連合もしくは構成国の一般的な公共の利益の重要な諸目標、とりわけ、欧州連合の共通対外安全保障政策上の諸目標、または、欧州連合もしくは構成国の重要な経済的利益もしくは金融上の利益、並びに、一般的な公共の利益を理由とし、または、データ主体または社会保護を含め他者の権利及び自由の保護の目的、公衆衛生及び人道上の目的によるする公共登録簿の維持管理を含める。

(45) 管理者または管理者の代わりの者によって実施される個人情報の処理に関し、管理者の職責及び法的責任が定められなければならない。とりわけ、管理者は、適切かつ効果的な措置を実装すること、そして、その措置の実効性を含め、処理活動がこの規則を遵守していることを説明できることを義務付けられなければならない。それらの措置は、処理の性質、範囲、過程及び目的、並びに、自然人の権利及び自由に対するリスクを考慮に入れるものとしなければならない。

(46) 自然人の権利及び自由に対する様々な発生確率と深刻度をもつリスクが個人データの処理から生じ得る。それは、物的な損失、財産的な損失もしくは非財産的な損失を発生させ得る：すなわち、その処理が、差別、ID 窃盗または ID 詐欺、財産的な損失、信用の毀損、職務上の守秘義務によって保護されている個人データの機密性の喪失、仮名の無権限の復元、または、それら以外の重大な経済的または社会的な不利益を生じさせ得る場合；データ主体がその権利または自由を奪われ、または、その個人データに対する管理の実行を妨げられる場合；人種的もしくは民族的な出自、政治的な意見、信教または思想上の信条、労働組合の加入を明らかにする個人データの処理、並びに、遺伝子データ、健康と関係するデータもしくは性生活と関係するデータ、または、有罪判決及び犯罪行為もしくは関連する保護措置と関係するデータの処理の場合；人格的側面が評価される場合、とりわけ、個人プロファイルを作成するために、または、それを用いるために、就労能力、経済状態、健康、個人的な嗜好もしくは興味、信頼性もしくは行動、位置もしくは移動に関する側面が解析または予測される場合；脆弱な性質をもつ個人、とりわけ、子どもの個人データが処理される場合；または、処理が莫大な量の個人データを含んでいる場合及び多数のデータ主体に対して影響を及ぼす場合がそうである。

(47) データ主体の権利及び自由に対するリスクの発生確率及びその深刻度は、その処理の性質、範囲、過程及び目的を参照して判断されなければならない。リスクは、データ処理業務がリスクまたは高度なリスクを含むか否かを決めることのできる客観的な評価を基礎として評定されなければならない。

(48) 個人データの処理と関連する自然人の権利及び自由の保護は、この規則の義務に適合することを確保するための適切な技術上及び組織上の措置が講じられることを要求する。この規則の遵守を説明できるようにするため、管理者は、内部的な基本方針を採択しなければならず、かつ、とりわけ、バイデザイン及びバイデフォルトのデータ保護の原則に適合する措置を実装しなければならない。そのような措置は、就中、個人データの処理のミニマム化、可能な限り速やかな個人データの加名化、権能及び個人データの処理に関する透明性、データ主体がデータ処理を監視できるようにすること、管理者が安全機能を開発し、向上させることができるようにすることによって、構成され得る。バイデザイン及びバイデフォルトのデータ保護の原則は、公共入札の過程においても考慮に入れられなければならない。

(49) 規則(EU) 2016/679 は、管理者が、承認された認証方法に依ることによって遵守を説明することを定めている。同様に、欧州連合の機関及び組織は、規則(EU) 2016/679 の第 42 条に従い、認証を得ることにより、この規則の遵守を説明できるものとすべきである。

(50) データ主体の権利及び自由の保護、並びに、管理者及び処理者の職責及び法的責任は、管理者が他の管理者と共同で処理の目的及び方法を定める場合、または、処理業務が管理者の代わりに実施される場合を含め、この規則に基づく職責の明確な割当てを要求する。

(51) 管理者の代わりに処理者によって行われる処理に関するこの規則の義務の遵守を確保するため、処理者に対して処理活動を委託する場合、管理者は、とりわけ、処理の安全性に関するものを含め、この規則の義務に適合する技術上及び組織上の措置を実装するための専門知識、信頼性及び資源の面に関し、十分な保証を提供する処理者のみを使用しなければならない。欧州連合の機関及び組織以外の処理者が承認された行動準則または承認された認証方法を遵守していることは、管理者の義務の遵守を説明するための要素として用いられ得る。欧州連合の機関及び組織以外の処理者による処理の実施は、実施される処理の過程における処理者の個別の職務及び職責並びにデータ主体の権利及び自由に対するリスクを考慮に入れた上で、処理者を管理者と結びつけ、処理の対象事項及び期間、処理の性質及び目的、個人データの種類及びデータ主体の類型を定める契約によって、または、処理者として活動する欧州連合の機関及び組織の場合においては、契約、もしくは、それ以外の欧州連合法に基づく法的行為によって、規律されなければならない。管理者及び処理者は、個別の契約、または、欧州委員会によって直接に採択された標準約款、もしくは、欧州データ保護監督官に採択され、欧州委員会によって承認された標準約款の利用を選択できるものとすべきである。管理者の代わりの処理を完了した後、その処理者が服する欧州連合法または構成国法に基づいて当該個人データを記録保存すべき義務が存在する場合を除き、処理者は、管理者の選択により、その個人データを返却し、または、消去しなければならない。

(52) この規則の遵守を説明するために、管理者は、その責任において、処理活動の記録を維持管理しなければならず、また、処理者は、その責任において、処理活動の類型の記録を維持管理しなければならない。欧州連合の機関及び組織は、欧州データ保護監督官と協力すること、及び、その機関及び組織の処理業務の監視の用に供し得るようにするため、要請に応じて、それらの記録を欧州データ保護監督官が利用できるようにすることを義務付けられる。欧州連合の機関及び組織の規模を考慮に入れた上で、それが適切ではない場合を除き、欧州連合の機関及び組織は、その機関及び組織の処理活動の記録の中央登録所を設けることができるものとすべきである。透明性の理由のゆえに、それらの機関及び組織は、そのような登録所を公開のものとすることも

できるものとすべきである。

(53) 安全性を維持するため、及び、この規則の違反となる処理を防止するため、管理者または処理者は、その処理に内在するリスクを評定しなければならず、また、暗号のような、それらのリスクを削減するための手段を実装しなければならない。その手段は、そのリスクとの関係において、最新技術及び実装費用並びに保護されるべき個人データの性質を考慮に入れた上で、機密性を含め、適切なレベルの安全性を確保しなければならない。データの安全性のリスクを評価する際、送受信され、記録保存され、または、その他の処理をされる個人データの偶発的または違法な破壊、喪失、改変、無権限の開示または無権限のアクセスのような、個人データ処理によって示され、とりわけ、物的な損失、財産的もしくは非財産的な損失を発生させるかもしれないリスクに対して検討が加えなければならない。

(54) 欧州連合の機関及び組織は、憲章の第 7 条に定める電子通信の秘密を確保しなければならない。とりわけ、欧州連合の機関及び組織は、それらの機関及び組織の電子通信ネットワークの安全性を確保しなければならない。それらの機関及び組織は、欧州議会及び理事会の指令 2002/58/EC[1]に従い、それらの機関及び組織の公衆が利用可能な Web サイトにアクセスする利用者の端末装置及びモバイルアプリケーションと関係する情報を防護しなければならない。それらの機関及び組織は、利用者名簿に記録保存されている個人データも保護しなければならない。

(55) 個人データ侵害は、適切かつ適時に対処されないと、自然人に対し、物的な損失、財産的な損失もしくは非財産的な損失をもたらし得る。それゆえ、管理者は、説明責任の原則に従い、その個人データ侵害が自然人の権利及び自由に対するリスクを発生させるおそれがないことを管理者が説明できる場合を除き、個人データ侵害が発生したことに管理者が気づいたならば可能な限り速やかに、及び、それが可能なときは、それに気づいてから遅くとも 72 時間以内に、不適切な遅滞なく、欧州データ保護監督官に対し、その個人データ侵害を通知しなければならない。72 時間以内に通知できない場合、その遅延の理由をその通知に付さなければならず、そして、更なる不適切な遅延なく、同時に、情報を提供することができる。そのような遅延が正当化される場合、通知をする前に問題のインシデントを全て解決するのではなく、可能な限り速やかに、その侵害に関し、より機微性が低く、より個別性の低い情報が公表されるべきである。

(56) 管理者は、当該個人データ侵害が自然人の権利及び自由に対する高度なリスクを発生させる可能性があるときは、彼または彼女が予め必要な警戒をできるようにするため、データ主体に対し、不適切な遅滞なく、個人データ侵害を連絡しなければならない。その連絡は、個人データ侵害の性質、及び、潜在的な負の影響を削減するための関係する自然人向けの勧告を記述しなければならない。そのようなデータ主体に対する連絡は、欧州データ保護監督官から提供された運用指針、または、それ以外の法執行機関のような関連機関から提供された運用指針を尊重しつつ、可能な限り速やかに、かつ、欧州データ保護監督官監督官と緊密に協力し、合理的に実施可能にされなければならない。

(57) 規則(EC) No 45/2001 は、データ保護責任者に対して個人データの処理を通知すべき管理者の一般的な義務を定めている。欧州連合の機関及び組織の規模を考慮に入れた上で、それが不適切である場合を除き、データ保護責任者は、通知された処理業務の登録簿を保管しなければ

[1] 電子通信部門における個人データの処理及びプライバシー保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC（プライバシー及び電子通信に関する指令）（OJ L 201, 31.7.2002, p. 37）

ならない。この一般的な義務と並んで、その処理の性質、範囲、過程及び目的のゆえに、自然人の権利及び自由を高度のリスクに晒すおそれのある処理業務を監視するため、効果的な手続及び仕組みが設けられなければならない。そのような手続は、とりわけ、そのような種類の処理業務が、新たな技術の利用を含んでいる場合、または、それに関して、管理者によるデータ保護影響評価がこれまで行われたことのないような新たな種類のものである場合、または、当初の処理の時から経過した時日に照らし、データ保護影響評価が必要となった場合においても設けられるべきである。そのような場合、その処理業務の性質、範囲、過程及び目的並びにリスクの発生源を考慮に入れた上で、高度のリスクの特別の蓋然性及び深刻度を評価するために、その処理を開始する前に、管理者によってデータ保護影響評価が実施されなければならない。その影響評価は、とりわけ、当該リスクの削減のため、個人データの保護の確保のため、及び、この規則の遵守を説明するために準備される措置、安全性確保措置及び仕組みを含めなければならない。

(58) データ保護影響評価が、そのリスクを削減するための安全性確保措置、防護措置及び仕組みがなければ、自然人の権利及び自由に対する高度のリスクをもたらすおそれがあることを示しており、かつ、管理者が、利用可能な技術及び実装費用の面において、合理的な手段によってはそのリスクを削減できないとの見解をもつ場合、その管理者は、その処理を開始する前に、欧州データ保護監督官と協議しなければならない。そのような高度のリスクは、ある種類の処理並びに処理の範囲及び頻度から生ずる可能性があり、それは、自然人の権利及び自由に対する加害または妨害を現実に発生させ得るものでもある。欧州データ保護監督官は、指定された期間内に、協議の要請に対処しなければならない。ただし、その期間内に欧州データ保護監督官から応答がないということは、処理業務を禁止する権限を含め、この規則に定める彼または彼女の職務及び権限に従った欧州データ保護監督官の介入を妨げてはならない。その協議の過程の一部として、欧州データ保護監督官に対し、問題となっている処理に関して実施されたデータ保護影響評価の結果、とりわけ、自然人の権利及び自由に対するリスクを削減するために準備された措置を提出できるものとすべきである。

(59) とりわけ、含まれているリスクをデータ主体のために削減することに関し、予定されている処理がこの規則を遵守することを確保するため、個人データの処理に関して定め、データ主体の権利の制限のための条件を定め、または、データ主体の権利のための安全性確保措置を定めている場合、欧州データ保護監督官は、欧州連合の機関及び組織の業務遂行と関連する事項に関して欧州連合の機関及び組織によって採択された行政措置の通知を受け、かつ、内部規則に関して協議を受けるものとしなければならない。

(60) 規則(EU) 2016/679 は、法人格をもつ欧州連合の独立の組織として、欧州データ保護委員会を設置した。委員会は、欧州委員会に助言することによる場合を含め、欧州連合全域における規則(EU) 2016/679 及び指令 2016/680 の一貫性のある適用に貢献しなければならない。それと同時に、欧州データ保護監督官は、彼または彼女の発意による場合及びその要請に応ずる場合を含め、欧州連合の全ての機関及び組織との関係において、彼または彼女の監督権限及び助言権限を行使し続けなければならない。欧州連合全域を通じてデータ保護法令の一貫性を確保するため、勧告案を準備する際、欧州委員会は、欧州データ保護監督官と協議する努力を尽くさなければならない。欧州委員会による協議は、個人データの保護の権利に対する影響をもつ立法行為の後、または、TFEU の第 289 条、第 290 条及び第 291 条に定める委任される行為及び実装行為を準備する間、並びに、TFEU の第 218 条に定める第三国及び国際機関との協定に関する

勧告及び提案を採択した後においては、義務的なものとしなければならない。そのような場合、欧州委員会は、例えば、十分性の判定、または、標準化されたアイコン及び認証方法の要件に関する委任される行為のように、欧州データ保護委員会との必要的協議を規則(EU)2016/679 が定める場合を除き、欧州データ保護監督官との協議を義務付けられなければならない。当の行為が、個人データの処理と関連する個人の権利及び自由の保護にとって特別の重要性のあるものである場合、欧州委員会は、上記に加え、欧州データ保護委員会と協議できるものとすべきである。そのような場合、欧州データ保護監督官は、欧州データ保護委員会の構成員として、共同意見書を発するため、彼の仕事と欧州データ保護委員会の仕事とを調整しなければならない。欧州データ保護監督官、及び、該当するときは、欧州データ保護委員会は、8 週間以内に、それらの機関の書面による助言を提供しなければならない。その期限は、例えば、欧州委員会が委任される行為及び実装行為を準備する際のように、緊急性を要する場合またはその他の適切な場合、短縮されなければならない。

(61) 規則(EU) 2016/679 の第 75 条に従い、欧州データ保護監督官は、欧州データ保護委員会の事務局を提供しなければならない。

(62) 欧州連合の全ての機関及び組織内において、データ保護責任者は、この規則の条項が適用されることを確保しなければならず、また、管理者及び処理者に対し、彼らの義務を果たすことに関し、助言しなければならない。そのデータ保護責任者は、データ保護の法律及び実務の専門知識を持つ者でなければならず、それは、とりわけ、管理者または処理者によって実施されるデータ処理業務、並びに、関与する個人データに求められる保護に従って決定されなければならない。そのようなデータ保護責任者は、独立した態様で、その責務及び職務を遂行するための立場にあるものとしなければならない。

(63) 欧州連合の機関及び組織から第三国内の管理者、処理者もしくはその他の取得者または国際機関に対して個人データが移転される場合、この規則によって欧州連合内において確保されるレベルの自然人の保護が保証されなければならない。それと同じ保証は、その第三国または国際機関から、同じ第三国もしくは別の第三国または国際機関の管理者、処理者に対する個人データの転送の場合に適用される。いかなる場合においても、第三国または国際機関に対する移転は、この規則を全面的に遵守し、かつ、憲章に掲げられた基本的な権利及び自由を尊重してのみ、実施され得る。この規則の他の条項により、第三国または国際機関に対する個人データの移転と関連してこの規則の条項に定める条件が管理者または処理者によって遵守される場合においてのみ、移転を行うことができる。

(64) 欧州委員会は、規則(EU) 2016/679 の第 45 条または指令(EU) 2016/680 の第 36 条に基づき、第三国、第三国内の地域もしくは特定の部門、または、国際機関が、十分なレベルのデータ保護を提供していると判定できる。そのような場合、欧州連合の機関または組織から当該第三国または国際機関に対する個人データの移転は、更に別の承認を受ける必要なく、行うことができる。

(65) 十分性の判定がない場合、管理者または処理者は、データ主体のための適切な安全性確保措置によって、第三国内におけるデータ保護の欠落を補うための措置を講じなければならない。そのような安全性確保措置は、欧州委員会によって採択された標準データ保護約款、欧州データ保護監督官によって採択された標準データ保護約款、または、欧州データ保護監督官によって承認された契約条項を利用することによって構成できる。処理者が欧州連合の機関または組織ではない場合、それらの処理者の安全性確保措置は、規則(EU) 2016/679 に基づいて国際移転

のために用いられる拘束的企業準則、行動準則及び認証方法によっても構成できる。これらの安全性確保措置は、効果的な行政救済または司法救済を得るため、及び、損害賠償を請求するための場合を含め、欧州連合内または第三国内において、データ主体の権利の執行可能な権利及び効果的な司法救済の可用性を含め、欧州連合内の処理に適用されるデータ保護の義務及びデータ主体の権利の遵守を確保しなければならない。それらの安全性確保措置は、とりわけ、個人データの処理と関連する一般的な基本原則、バイデザイン及びバイデフォルトのデータ保護の原則の遵守に関するものでなければならない。了解覚書のような行政文書の中に挿入されるデータ主体のための執行可能かつ効果的な権利を定める条項を根拠とする場合を含め、欧州連合の機関または組織から、対応する責務または権能をもつ第三国内の行政機関もしくは行政組織または国際機関に対し、移転を行うことができる。法的拘束力のない行政文書の中で安全性確保措置が定められている場合、欧州データ保護監督官から承認を受けなければならない。

(66) 欧州委員会または欧州データ保護監督官によって採択された標準データ保護約款を管理者または処理者が利用可能であるということは、欧州委員会または欧州データ監督官によって採択された標準データ保護約款と直接または間接に矛盾せず、データ主体の基本的な権利及び自由を妨げないことを条件として、管理者または処理者が、処理者と別の処理者との間の契約のような、より広範囲の契約の中に標準データ保護約款の条項を含めることを妨げるものではなく、また、別の条項または安全性確保措置を付加することを妨げるものでもない。管理者及び処理者は、標準データ保護約款を補完する契約上の約定を介して、追加的な安全性確保措置を提供することが奨励されなければならない。

(67) 幾つかの第三国は、欧州連合の機関及び組織の処理活動を直接に規律することを旨とする法律、規則及びその他の法的行為を採択している。これは、管理者または処理者に対して個人データの移転または開示を要請する第三国内の裁判所もしくは法廷の判決または行政機関の決定であって、かつ、要請元の第三国と欧州連合との間で有効な国際協定を基礎とするものではないものを含み得る。これらの法律、規則及びそれ以外の法的行為の域外適用は、国際法違反となり得るものであり、また、この規則によって欧州連合内で確保されるべき自然人の保護の達成を阻害するものとなり得る。移転は、第三国への移転に関するこの規則の条件に適合する場合においてのみ、認められるべきである。このことは、就中、欧州連合法の中で認められている公共の利益上の重要な法的根拠のゆえに開示が必要となる場合がそうである。

(68) データ主体が彼または彼女の明示の同意を与えた場合、移転が一時的なものであり、かつ、規制当局における手続を含め、それが司法手続内のものであるか、行政手続もしくは裁判外手続によるものであるかを問わず、契約または訴訟との関係において必要となる場合という一定の事業の下において、移転の可能性に関する個別状況に関し、条項が設けられなければならない。欧州連合法によって定められる公共の利益上の重要な法的根拠がそのような移転を要求する場合、または、法律によって設置され、公衆もしくは正当な利益をもつ個人からの照会に応ずるための登録所から移転が行われる場合においても、移転の可能性に関し、条項が設けられなければならない。後者の場合、そのような移転は、欧州連合法によって認められる場合を除き、データ主体の利益及び基本的な権利を考慮に入れた上で、その登録所の中に収められている個人データ全体またはデータの類型全体を含めるものであってはならず、かつ、正当な利益をもつ者からの照会に対して登録所が応じようとする場合、それらの者の要請に応ずる場合、または、その要請者が取得者となる場合においてのみ、その移転が行われるものとすべきである。

(69) これらの特例は、とりわけ、公共の利益上の重要な理由により要求され、かつ、その必要があるデータ移転に適用され、例えば、欧州連合の機関及び組織と、競争当局、税務当局または税関当局、金融監視当局、並びに、例えば、感染症の追跡調査の場合、または、スポーツにおけるドーピングの抑制及びまたは抑止のために、社会保障に関する事項もしくは公衆衛生上の職務権限を有する当局の間において行われる国際的なデータ交換に適用されなければならない。個人データの移転は、データ主体がその同意を与えることができない場合において、身体的な完全性または生命を含め、データ主体またはそれ以外の者の生存の利益の保護のために必要となる場合においても、適法とみなされなければならない。十分性の判定がない場合、欧州連合法は、公共の利益上の重要な理由のために、個別の類型のデータの第三国または国際機関に対する移転の制限を明確に定めることができる。ジュネーブ諸条約に基づいて負った職務の遂行のため、または、武力衝突に適用可能な国際人道法を遵守するため、身体的または法的な原因により同意を与えることができないデータ主体の個人データの国際的な人道組織に対する移転は、公共の利益上の重要な理由のために、または、データ主体の生存の利益に係わるという理由により、必要なものと判断することができる。

(70) 第三国内における十分なレベルのデータ保護に関して欧州委員会が何らの判定もしなかった場合、いかなる場合においても、管理者または処理者は、欧州連合内において彼らのデータの処理に関して執行可能かつ効果的な権利をもつデータ主体が、そのデータが移転されたときは、基本的な権利及び安全性確保措置からの利益を享受し続ける解決策を利用できるようにしなければならない。

(71) 個人データが欧州連合の対外国境を越えて移動する場合、データ保護の権利を行使するため、とりわけ、その情報の違法な利用または開示から自らを防護するための自然人の能力は、リスクの増大に晒されることとなり得る。それと同時に、国内監督機関及び欧州データ保護監督官は、その管轄地の外にある活動に関し、異議に対処できず、または、調査を実施できない状態となり得る。国境を越えるという文脈の中で共に仕事をするという彼らの努力は、不十分な防止権限または是正権限、一貫性のない法制度、及び、資源の制約のような実務的な障碍によっても妨げられ得る。それゆえ、彼らの国際的に対応する相手との情報交換を助けるため、欧州データ保護監督官と国内監督機関との間の緊密な協力を向上させなければならない。

(72) 規則(EC) No 45/2001 において完全に独立して彼または彼女の職務を遂行し、かつ、彼または彼女の権限を行使する資格を与えられた欧州データ保護監督官が設置されたことは、自然人の個人データの処理と関連する自然人の保護の重要な構成要素の 1 つである。この規則は、彼または彼女の役割及び独立性を更に強化し、かつ、明確にしなければならない。欧州データ保護監督官は、その独立性が疑問の余地のない者であり、かつ、例えば、彼または彼女が規則(EU) 2016/679 の第 51 条に基づいて設置された監督機関のいずれかに属していたという理由により、欧州データ保護監督官の責務を遂行するために要求される経験及び技能をもつものとして認められている者でなければならない。

(73) 欧州連合全域にわたるデータ保護法令の一貫性のある監視及び執行を確保するため、欧州データ保護監督官は、とりわけ、自然人からの異議申立ての場合における調査の権限、是正権限及び制裁の権限、承認の権限及び助言の権限、並びに、司法裁判所の注意をこの規則の違反行為に向けさせるための権限、及び、一次法に従って訴訟に関与する権限を含め、国内監督機関と同じ職務及び効果的な権限をもつものとしなければならない。そのような権限は、処理の禁

止を含め、処理に対して一時的または恒久的な制限を加える権限も含めなければならない。負の影響を受け得る関係者に関する無駄な費用支出及び行き過ぎた影響を避けるため、欧州データ保護監督官の個々の措置は、個別の事案それぞれの事情を考慮し、かつ、関係する個々の措置が講じられる前に、全ての個人が聴聞を受ける権利を尊重することを条件として、この規則の遵守を確保することに鑑み、適切であり、必要であり、かつ、比例的なものでなければならない。欧州データ保護監督官の法的な拘束力のある個々の措置は、書面によるものとし、明確で紛れがなく、措置の発令日を表示し、欧州データ保護監督官の署名があり、その措置の理由を提供し、かつ、効果的な司法救済の権利を示すものでなければならない。

(74) 欧州データ保護監督官の監督権限は、意思決定を含め、その司法上の職務の遂行における裁判所の独立性を防護するため、その司法上の権限において行動する場合、司法裁判所による個人データの処理に対し、適用してはならない。そのような処理業務に関し、裁判所は、憲章の第 8 条第 3 項に従い、例えば、内部の仕組みにより、独立の監督を設けなければならない。

(75) データ処理業務と関連する適用除外、保証、承認及び条件に関する欧州データ保護監督官の決定は、この規則に定めるように、活動報告書の中で公表されなければならない。年次活動報告書の発行とは別に、欧州データ保護監督官は、個別の事項に関する報告書を発行できる。

(76) 欧州データ保護監督官は、欧州議会及び理事会の規則(EC) No 1049/2001[1]を遵守しなければならない。

(77) 国内監督機関は、自然人の個人データの処理との関係において自然人を保護するため、及び、域内市場の中における個人データの支障のない流れを容易にするため、規則(EU) 2016/679 の適用を監視し、かつ、欧州連合全域におけるその一貫性のある適用に貢献する。構成国内において適用されるデータ保護法令並びに欧州連合の機関及び組織に適用されるデータ保護法令の適用における一貫性を向上させるため、欧州データ保護監督官は、国内監督機関と実効的に協力しなければならない。

(78) 一定の場合において、欧州連合法は、欧州データ保護監督官と国内監督機関との間で共有される調整された監督モデルを定めている。欧州データ保護監督官は、Europol の監督機関でもあり、また、それらの目的のために、諮問機能をもつ協力委員会を介する国内監督機関との間の協力の特別のモデルが設けられた。データ保護の実体規定の効果的な監督及び執行を向上させるため、単一の、整合性のとれた、連携した監督モデルが欧州連合内に導入されなければならない。それゆえ、欧州委員会は、この規則の調整された監督モデルに揃えるため、それが適切なときは、調整された監督モデルを定める欧州連合の法的行為を改正するための立法提案書を提出しなければならない。欧州データ保護委員会は、全ての分野にわたる効果的かつ調整された監督を確保するための単一の場を提供しなければならない。

(79) 全てのデータ主体は、欧州データ保護監督官に異議を申立てる権利をもち、かつ、この規則に基づく彼または彼女の権利が侵害されたとデータ主体が判断する場合、または、欧州データ保護監督官が、異議について何も行動せず、その異議の全部または一部を棄却もしくは却下した場合、または、データ主体の権利を保護するために欧州データ保護監督官の活動が必要であるのに何も活動をしない場合、諸条約に従い、司法裁判所において効果的な司法救済を受ける権

[1] 欧州議会、理事会及び欧州委員会の文書への公衆のアクセスに関する欧州議会及び理事会の 2001 年 5 月 30 日の規則(EC) No 1049/2001（OJ L 145, 31.5.2001, p.43）

利をもつものとしなければならない。異議申立て後の調査は、司法審査に服し、個々の案件において適切な範囲内において実施されなければならない。欧州データ保護監督官は、データ主体に対し、合理的な期間内に、その異議の進捗状況及び結果を通知しなければならない。その案件が国内監督機関との調整を必要とする場合、データ主体に対し、中間的な情報が与えられなければならない。異議の申立てを容易にするため、欧州データ保護監督官は、他の連絡手段を排除することなく、電子的に完了させることもできる異議申立書の提出方式の提供のような措置を講じなければならない。

(80) この規則の違反行為の結果として物的または非物的な損害を被った者は、諸条約に定める条件に従い、管理者または処理者からその被った損害に対する賠償を受ける権利をもつ。

(81) 欧州データ保護監督官の監督上の役割及びこの規則の効果的な執行を強化するため、欧州データ保護監督官は、最後の手段である制裁として、行政罰を加える権限をもつものとしなければならない。この行政罰は、この規則の不遵守に関し、この規則の将来の違反を抑止するため、並びに、欧州連合の機関及び組織内における個人データ保護の文化を育成するため、（個人に対してではなく）欧州連合の機関または組織に対して制裁を加えることを狙いとすべきである。この規則は、行政罰に服する違反行為、並びに、行政罰に設けられる上限額及び基準を示さなければならない。欧州データ保護監督官は、個別の状況における全ての関連する事情を考慮に入れることにより、その違反行為の性質、重大性及び持続期間、その違反行為の結果、並びに、この規則に基づく義務の遵守を確保するため、及び、違反行為の結果を防止もしくは削減するために講じられた措置を適切に配慮し、個々の案件それぞれにおける行政罰の額を決定しなければならない。欧州連合の機関及び組織に対して行政罰を加える場合、欧州データ保護監督官は、その行政罰の額の比例性を検討しなければならない。欧州連合の機関及び組織に対して罰を加える行政手続は、司法裁判所によって解釈されたものとしての欧州連合法の一般原則を尊重しなければならない。

(82) この規則に基づく彼または彼女の権利が侵害されているとデータ主体が判断する場合、彼または彼女は、欧州連合法または構成国法に従って組織され、公共の利益に属する制定法上の目的をもち、個人データの保護の領域において活動する非営利の組織、団体または協会に対し、彼または彼女の代わりに、欧州データ保護監督官に異議の申立てすることを委任する権利をもつものとしなければならない。そのような組織、団体または協会は、データ主体の代わりに司法救済の権利を行使すること、または、データ主体の代わりに損害賠償金を受領する権利を行使することもできるものとすべきである。

(83) この規則に定める義務を遵守しない欧州連合の官吏またはその他の公務員は、理事会規則(EEC, Euratom, ECSC) No 259/68[1]（「職員規則」）に定める欧州連合の官吏の職員規則及び欧州連合のその他の公務員の雇用条件の中で定められている規定及び手続に従い、懲戒事由となる行為またはその他の行為について法的責任を負うものとしなければならない。

(84) この規則の実装のための統一的な要件を確保するため、欧州委員会に対し、実装権限が与えられなければならない。それらの権限は、欧州議会及び理事会の規則(EU) No 182/2011[2]に従って行使されなければならない。その審議手続は、管理者と処理者の間及び処理者間の標準約款の

[1] OJ L 56, 4.3.1968, p.1.

[2] 欧州委員会の実装権限の行使の構成国による監督のための仕組みに関する規則及び一般原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011（OJ L 55, 28.2.2011, p.13）

採択のため、公共の利益において実施される職務の遂行のために個人データの処理をする管理者による欧州データ保護監督官の事前協議を要する処理業務のリストの採択のため、並びに、国際的な移転のための適切な安全性確保措置を定める標準約款の採択のために用いられなければならない。

(85) 公式の欧州統計及び公式の構成国統計の作成のために欧州連合の統計局及び構成国の統計局が収集する機密の情報は、保護されなければならない。欧州統計は、TFEU の第 338 条第 2 項に定める統計原則に従って、開発され、作成され、かつ、配布されなければならない。欧州議会及び理事会の規則(EC) No 223/2009[1]は、欧州統計のための統計上の秘密に関して更に仕様を定めている。

(86) 規則(EC) No 45/2001 並びに欧州議会、理事会及び欧州委員会の決定 No 1247/2002EC[2]は、廃止される。廃止される規則及び決定に対する参照は、この規則に対する参照として解釈されなければならない。

(87) 独立の監督機関の構成員の全面的な独立性を防護するため、現在の欧州データ保護監督官及び現在の副監督官の任期は、この規則によって影響を受けることがない。現在の副監督官は、この規則に定める欧州データ保護監督官の任期満了前の終了事由のどれにも該当しない限り、彼の任期満了までその地位を維持するものとしなければならない。この規則の関連条項は、彼の任期満了まで、副監督官に対して適用されなければならない。

(88) 比例性原則に従い、欧州連合の機関及び組織における個人データの保護に関する法令を定めることは、個人データの処理と関連する自然人の均等なレベルの保護を確保し、かつ、欧州連合の全域における個人データの支障のない移動を確保するという基本的な目的を達成するために必要であり、かつ、適切である。この規則は、TEU の第 5 条第 4 項に従い、その目的を達成するために必要なところを超えることがない。

(89) 欧州データ保護監督官は、規則(EC) No 45/2001 の第 28 条第 2 項に従って協議をし、2017 年 3 月 15 日に意見書を提出した[3]。

---

[1] 欧州統計に関する、並びに、欧州共同体の統計局に対する統計上の秘密に服するデータの送付に関する欧州議会及び理事会の規則(EC, Euratom) No 1101/2008、欧州共同体の統計に関する理事会規則(EC) No 322/97、欧州共同体の統計計画に関する委員会を設置する理事会決定 89/382/EEC, Euratom を廃止する欧州議会及び理事会の 2009 年 3 月 11 日の規則(EC) No 223/2009（OJ L 87, 31.3.2009, p.164）

[2] 欧州データ保護監督官の職務の遂行を規律する要件及び一般的な条件に関する欧州議会、理事会及び欧州委員会の 2002 年 7 月 1 日の決定 No 1247/2002/EC（OJ L 183, 12.7.2002, p.1）

[3] OJ C 164, 24.5.2017, p.2.

第 I 章 総則的な条項

第 1 条 対象事項及び目的

1. この規則は、欧州連合の機関及び組織による個人データの処理と関連する自然人の保護に関する規定、並びに、それらの機関及び組織の間における、または、それ以外の欧州連合内に設けられた取得者に対する個人データの支障のない移動に関する規定を定める。
2. この規則は、自然人の基本的な権利及び自由、とりわけ、彼らの個人データの保護の権利を保護する。
3. 欧州データ保護監督官は、欧州連合の機関または組織によって実施される全ての処理業務に対するこの規則の条項の適用を監視する。

第 2 条 適用範囲

1. この規則は、欧州連合の全ての機関及び組織による個人データの処理に適用される。
2. TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合の欧州連合の組織、事務局及び部局による運用個人データの処理に対しては、この規則の第 3 条及び第 IX 章のみが適用される。
3. この規則は、欧州議会及び理事会の規則(EU) 2016/794[1]並びに理事会規則(EU) 2017/1939[2]がこの規則の第 98 条に従って修正されるまで、Europol 及び欧州検事局による運用個人データの処理に対し、適用してはならない。
4. この規則は、TEU の第 42 条第 1 項、第 43 条及び第 44 条に示す任務による個人データの処理に対し、適用してはならない。
5. この規則は、その全部または一部が自動的な手段による個人データの処理に対し、並びに、自動的な手段以外の方法による個人データの処理であって、ファイリングシステムの一部を構成し、または、ファイリングシステムの一部を構成する予定であるものに対して、適用される。

第 3 条 定義

この規則の目的のために、以下の定義が適用される：

(1) 「個人データ」とは、識別された自然人または識別可能な自然人（「データ主体」）に関する情報を意味し；識別可能な自然人とは、とりわけ、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、または、当該自然人の肉体的、生理的、遺伝的、精神的、経済的、文化的または社会的な同一性を示す 1 または複数の要素を参照することによって、直接的または間接的に、識別され得る者のことであり；

---

[1] 欧州連合法執行協力局（Europol）に関する、並びに、理事会決定 2009/371/JHA、2009/934/JHA、 2009/935/JHA、2009/936/JHA 及び 2009/968/JHA を廃止し、置き換える欧州議会及び理事会の 2016 年 5 月 11 日の規則(EU) 2016/794（OJ L 135, 24.5.2016, p.53）

[2] 欧州検事局（「EPPO」）の設置に関する拡大された協力を実装する 2017 年 10 月 12 日の理事会規則(EU) 2017/1939（OJ L 283, 31.10.2017, p.1）

(2) 「運用個人データ」とは、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合において、欧州連合の組織、事務局または部局を定める適法な法令の中に定める目的及び職務に適合するため、その組織、事務局及び部局によって処理される全ての個人データのことを意味し；

(3) 「処理」とは、それが自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正もしくは変更、検索、参照、使用、送信による開示、配布、または、それら以外に利用可能にすること、整列もしくは結合、制限、削除もしくは破壊のような、個人データもしくは個人データのセットに実施される業務遂行または業務遂行のセットのことを意味し；

(4) 「処理の制限」とは、将来におけるその処理を限定するため、記録保存された個人データに目印をつけることを意味し；

(5) 「プロファイリング」とは、自然人と関連する一定の人格的側面を評価するため、とりわけ、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置または移動に関する側面を分析または予測するための、個人データの利用によって構成される全ての形態の個人データの自動的な処理のことを意味し；

(6) 「仮名化」とは、当該追加情報が分離して保管されており、かつ、その個人データが識別された自然人または識別可能な自然人に割当てられていることを示さないことを確保するための技術上及び組織上の措置の下にあることを条件として、その追加情報を使用することなしには、その個人データが特定のデータ主体に割当てられていることを示すことができないようにする態様により実施される個人データ処理のことを意味し；

(7) 「ファイリングシステム」とは、個人データの構成されたセットであって、機能上または地理上における集中型、放射状型または分散型の別を問わず、特定の基準に従ってアクセス可能なもののことを意味し；

(8) 「管理者」とは、欧州連合の機関もしくは組織、または、事務局長またはそれ以外の組織体であって、単独で、または、他の機関と共同で、個人データの処理の目的及び方法を決定する者のことを意味し；そのような処理の目的及び方法が欧州連合の個別の法令によって定められる場合、管理者またはその指定のための個別の基準は、欧州連合の法律によって定めることができ；

(9) 「欧州連合の機関及び組織以外の管理者」とは、規則(EU) 2016/679 の第 4 条(7)の意味における管理者及び指令(EU) 2016/680 の第 3 条の意味における管理者のことを意味し；

(10) 「欧州連合の機関及び組織」とは、TEU、TFEU または欧州原子力共同体条約によって、または、これらに基づいて設置された欧州連合の機関、組織、事務局及び部局のことを意味し；

(11) 「職務権限を有する機関」とは、公共の安全を妨げる脅威に対する防護及びその防止を含め、犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行の職務権限を有する構成国の行政機関のことを意味し；

(12) 「処理者」とは、管理者の代わりに個人データを処理する自然人もしくは法人、行政機関、部局またはそれ以外の組織のことを意味し；

(13) 「取得者」とは、第三者であるか否かを問わず、個人データの開示を受ける自然人もしくは法人、行政機関、部局またはそれ以外の組織のことを意味する。ただし、欧州連合法または構成国法に従って特別の調査の枠組み内で個人データを取得できる行政機関は、取得者とはみなされず；それらの行政機関によるそのデータの処理は、その処理の目的に従い、適用可能なデー

タ保護の規定を遵守するものとし；

(14) 「第三者」とは、データ主体、管理者、処理者、及び、管理者または処理者の直接の承認の下で個人データ処理が認められている者以外の自然人もしくは法人、行政機関、部局またはそれ以外の組織のことを意味し；

(15) データ主体の「同意」とは、任意に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示であって、それによって、彼もしくは彼女が、その言辞または明確に肯定的な行動により、彼もしくは彼女と関連する個人データ処理の同意を表明するもののことを意味し；

(16) 「個人データ侵害」とは、事故によるまたは違法な、送受信され、記録保存され、または、それ以外の処理が行われる個人データの破壊、喪失、改変、無権限の開示または無権限のアクセスを導く安全性の侵害のことを意味し；

(17) 「生体データ」とは、自然人の生来的または獲得された生体特徴と関連する個人データであって、当該自然人の生理または健康に関するユニークな情報を与えるもの、及び、とりわけ、当の自然人からの生体サンプルの分析から得られるもののことを意味し；

(18) 「遺伝子データ」とは、自然人の身体的、生理的または行動的な特性と関連する特別な技術的処理から得られる個人データであって、顔画像や指紋データのように、当該自然人のユニークな識別をできるようにするもの、または、その識別を確認するもののことを意味し；

(19) 「健康に関するデータ」とは、医療サービスの提供を含め、自然人の身体的または精神的な健康と関連する個人データであって、彼または彼女の健康状態に関する情報を明らかにするもののことを意味し；

(20) 「情報社会サービス」とは、欧州議会及び理事会の指令(EU) 2015/1535[1]の第 1 条第 1 項の(b)に定義するサービスのことを意味し；

(21) 「国際機関」とは、国際法によって規律される組織及びその下部組織、または、それ以外の組織であって、複数の国の間の協定によって、もしくは、その協定に基づいて、設立されるもののことを意味し；

(22) 「国内監督機関」とは、規則(EU) 2016/679 の第 51 条により、または、指令(EU) 2016/680 の第 41 条により、構成国によって設置される独立の行政機関のことを意味し；

(23) 「利用者」とは、欧州連合の機関または組織の管理下にあるネットワークまたは端末装置を使用する自然人のことを意味し；

(24) 「名簿」とは、印刷物であるか電子的な方式であるかを問わず、公衆が利用可能な利用者名簿、または、欧州連合の機関もしくは組織内で利用可能な利用者名簿、または、欧州連合の機関もしくは組織の間で共有される利用者名簿のことを意味し；

(25) 「電子通信ネットワーク」とは、恒久的なインフラまたは集中管理能力を基礎とするか否かを問わず、送受信システム、並びに、該当するときは、交換装置またはルーティング装置及びそれら以外の資源であって、アクティブではないネットワーク要素を含め、有線により、無線により、光学的手段により、または、それら以外の電磁的な手段により、信号の伝送を許容するもののことを意味し、運搬される情報の種類に拘らず、衛星ネットワーク、固定（インターネットを含め、

[1] 技術標準及び情報社会サービスに関する法令の分野における情報提供の手続を定める欧州議会及び理事会の 2015 年 9 月 9 日の指令(EU) 2015/1535（OJ L 241, 17.9.2015, p.1）

回線交換、パケット交換）及び移動体の地上ネットワーク、信号の送受信の目的のために使用される範囲内で送電線システム、ラジオ放送及びテレビ放送のために使用されるネットワーク、ケーブルテレビネットワークを含めるものとし；

(26) 「端末装置」とは、委員会指令 2008/63/EC[1]の第 1 条(1)に定義する端末装置のことを意味する。

第 II 章 基本原則

第 4 条 個人データの処理に関する基本原則

1. 個人データは：
   (a) データ主体との関係において、適法、公正、かつ、透明性のある態様で処理されなければならない（「適法、公正及び透明性」）；
   (b) 特定され、明示され、かつ、公正な目的のために収集されるものとしなければならず、かつ、これらの目的と適合しない態様で、別の目的のために処理されてはならない；第 13 条に従い、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のための別の目的による処理は、当初の目的と適合しないものとはみなされない（「目的制限」）；
   (c) それが処理される目的との関係において十分であり、関連性があり、かつ、必要なものに限定されなければならない（「データのミニマム化」）；
   (d) 正確であり、かつ、必要なときは、最新のものに維持されなければならない；それが処理される目的を考慮し、不正確な個人データが遅滞なく削除または訂正されることを確保するための全ての合理的な手立てが講じられなければならない（「正確性」）；
   (e) 個人データが処理される目的のために必要な期間内だけデータ主体の識別を許容する方式を維持するものとしなければならない；個人データは、データ主体の権利及び自由を防護するためにこの規則によって求められる適切な技術上及び組織上の措置に服し、第 13 条に従い、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のためにのみ、その個人データが処理される限り、より長い期間のために記録保存され得る（「記録保存制限」）；
   (f) 無権限または違法な処理に対する保護及び事故による喪失に対する保護を含め、適切な技術上または組織上の措置を用いて、個人データを適切に防護する態様で処理されなければならない（「完全性及び機密性」）。
2. 管理者は、第 1 項について責任を負い、その遵守を説明できなければならない（「説明責任」）。

第 5 条 処理の適法性

1. 処理は、以下の中の少なくとも 1 つが適用される場合に限り、かつ、その範囲内においてのみ、適法である：
   (a) 公共の利益において、または、欧州連合の機関または組織に与えられた公的な権限の行使

[1] 電気通信端末装置の市場における競争に関する 2008 年 6 月 20 日の委員会指令 2008/63/EC（OJ L 162, 21.6.2008, p.20）

において実施される職務の遂行のために処理が必要となる場合;
(b) 管理者が服すべき法的義務を遵守するために処理が必要となる場合;
(c) データ主体が当事者となっている契約の履行のため、または、契約の締結前にデータ主体からの申込みに際して手立てを講じるために処理が必要となる場合;
(d) 1 または複数の特定の目的のための彼または彼女の個人データの処理について、データ主体が同意を与えた場合;
(e) データ主体または他の自然人の生存の利益を保護するために処理が必要となる場合。

2. 第 1 項の(a)及び(b)に示す処理のための根拠は、欧州連合法の中において定められる。

第 6 条 同等な別の目的のための処理

その個人データが収集された目的以外の目的のための処理がデータ主体の同意に基づくものではない場合、または、第 25 条第 1 項に示す対象を防護するために民主主義社会において必要かつ比例的な措置を構成する欧州連合法に基づくものではない場合、管理者は、別の目的のための処理が、その個人データが最初に収集された目的と適合するものであるか否かを確認するため、就中、以下の事項を考慮に入れる:

(a) その個人データが収集された目的と、予定されている別の目的による処理の目的との間の関連性;
(b) とりわけ、データ主体と管理者との間の関係に関し、その個人データが収集された経緯;
(c) その個人データの性質、とりわけ、第 10 条により、特別類型の個人データが処理されるか否か、または、第 11 条により、有罪判決及び侵害行為と関係する個人データが処理されるか否か;
(d) 適切な安全性確保措置の存在。それは、暗号化または仮名化を含め得る。

第 7 条 同意の条件

1. 処理が同意に基づく場合、管理者は、データ主体が彼または彼女の個人データの処理について同意をしたことを説明できなければならない。
2. データ主体の同意が、他の事項とも関係する書面による申告の中で与えられる場合、その同意を求める要求は、それ以外の事項と明確に区別することができ、理解しやすく、利用しやすい方式により、明瞭かつ平易な文言を用いる態様で提示されなければならない。この規則の違反を組成するような申告部分は、拘束力をもたない。
3. データ主体は、いつでも、彼または彼女の同意を撤回する権利をもつ。同意の撤回は、その撤回よりも前の同意に基づく処理の適法性に影響を与えない。同意を与える前に、データ主体は、それについて説明を受ける。同意の撤回は、同意の提供と同様に容易なものとする。
4. 同意が任意に与えられたか否かを評価する場合、就中、サービスの提供を含め、当該契約の履行のために必要のない個人データ処理に対する同意を契約履行の条件とするものであるか否かを最大限考慮に入れる。

第 8 条　情報社会サービスと関連する子供の同意に適用される条件

1. 子どもに対する情報社会サービスの直接の提供と関連して第 5 条第 1 項(d)が適用される場合、子どもの個人データの処理は、その子どもが少なくとも 13 歳である場合には適法である。その子どもが 13 歳未満の場合、そのような処理は、その子どもに対する親権者としての責任をもつ者によってその同意が与えられた場合、もしくは、その承認がなされた場合において、その範囲内に限り、適法である。
2. そのような場合においては、管理者は、利用可能な技術を考慮に入れ、子どもに対する親権者としての責任をもつ者によってその同意が与えられていること、または、その承認がなされていることを確認するための合理的な努力を尽くす。
3. 第 1 項は、子どもと関連する契約の有効性、成立または効果に関する規定のような構成国の一般的な契約法に対して影響を与えない。

第 9 条　欧州連合の機関及び組織以外の欧州連合内に設けられた取得者に対する個人データの送付

1. 第 4 条、第 5 条、第 6 条及び第 10 条を妨げることなく、個人データは、以下の場合においてのみ、欧州連合の機関及び組織違背の欧州連合内に設けられた取得者に対して送付される:
   (a) 公共の利益において、もしくは、取得者に与えられた公的な権限の行使において実施される職務の遂行のためにそのデータが必要であることを取得者が証明する場合;または、
   (b) 公共の利益における特別の目的のためにそのデータを送付させる必要性があることを取得者が証明する場合、並びに、データ主体の正当な利益が危険に晒されていると推定すべき理由が存在するときは、様々な競合する利益を説明可能な状態で評定した後、当該特別の目的のために個人データの送付が比例的であることを管理者が証明する場合。
2. 本条に基づく送付を管理者の発意により行う場合、その管理者は、第 1 項の(a)または(b)に定める基準を適用することにより、その個人データの送付が必要であり、かつ、送付の目的にとって比例的であることを説明するものとする。
3. 欧州連合の機関及び組織は、個人データの保護の権利と、欧州連合法による文書へのアクセスの権利とを調和させる。

第 10 条　特別類型の個人データの処理

1. 人種的もしくは民族的な出自、政治的な意見、宗教上もしくは思想上の信条、または、労働組合への加入を明らかにする運用個人データの処理、並びに、自然人をユニークに識別することを目的とする遺伝子データ、生体データ、健康に関するデータまたは自然人の性生活もしくは性的指向に関するデータの処理は、禁止される。
2. 第 1 項は、以下の中の 1 つが適用される場合には、適用されない:
   (a) 第 1 項に示す禁止をデータ主体が解除できないと欧州連合法が定めている場合を除き、1 または複数の特定された目的のためのそれらのデータの処理について、データ主体が明示の同意を与えた場合;

(b) データ主体の基本的な権利及び利益のための適切な安全性確保措置を定める欧州連合法によって認められている範囲内において、雇用及び社会保障並びに社会保護の分野における管理者またはデータ主体の義務を履行する目的、または、それらの者の個別の権利を行使する目的のために処理が必要となる場合;

(c) データ主体が身体的または法的に同意を与えることができない場合において、データ主体または他の者の生存の利益を保護するために処理が必要となる場合;

(d) 政治、思想、宗教または労働組合の目的とし、欧州連合の機関もしくは組織の中で結成される団体を構成する非営利組織によって行われる適切な安全性確保措置を具備する正当な活動の過程において、その処理がその団体の構成員もしくは元構成員、または、その団体の目的と関係してその組織と継続的に接触をもつ者のみに関するものであることを条件とし、かつ、データ主体の同意なくそのデータが当該団体の外部に開示されないことを条件として、処理が実施される場合;

(e) 明らかにデータ主体によって公開のものとされた個人データに関する処理の場合;

(f) 訴えの提起もしくは攻撃防御のため、または、司法裁判所がその司法上の権限において行為する際に処理が必要となる場合;

(g) 求められる目的と比例し、データ保護の権利の本質を尊重し、そして、データ主体の基本的な権利及び利益を防護するための適切な個別の措置を定める欧州連合法を基礎として、重要な公共の利益を理由とする処理が必要となる場合;

(h) 欧州連合法を基礎として、または、医療専門家との契約により、かつ、第 3 項に示す条件及び安全性確保措置に従い、予防医学もしくは産業医学の目的のため、従業者の就労能力の評価、医療上の診断、医療もしくは社会福祉または治療の提供のため、または、医療制度もしくは社会福祉制度及びそのサービスの管理のために処理が必要となる場合;

(i) データ主体の権利及び自由を防護するための適切な個別の措置に関して、とりわけ、職務上の守秘義務に関して定める欧州連合法を基礎として、健康に対する国境を越える重大な脅威に対して防護すること、または、医療及び医薬品もしくは医療機器の高い水準の品質及び安全性を確保することのような、公衆衛生の分野における公共の利益を理由とする処理が必要となる場合;または、

(j) 求められる目的と比例し、データ保護の権利の本質を尊重し、そして、データ主体の基本的な権利及び利益を防護ための適切な個別の措置を定める欧州連合法を基礎として、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のために処理が必要となる場合。

3. 第 1 項に示す個人データは、欧州連合法または構成国法もしくは職務権限を有する国内組織によって定められる法令に基づく職務上の守秘義務に服する専門家によって、または、その専門家の責任の下でその個人データが処理される場合、または、欧州連合法または構成国法もしくは職務権限を有する国内組織によって定められる法令に基づく職務上の守秘義務にも服する別の者によって処理される場合、第 2 項の(h)に示す目的のために処理できる。

第 11 条 有罪判決及び犯罪行為と関連する個人データの処理

第 5 条第 1 項に基づく有罪判決及び犯罪行為または保護措置と関連する個人データの処理は、権

限のある機関の管理の下にある場合、または、データ主体の権利及び自由のための適切な安全性確保措置を定める欧州連合法によってその処理が認められる場合に限り、実施される。

第 12 条　識別を必要としない処理

1. 管理者が個人データを処理する目的が、管理者によるデータ主体の識別を必要としない場合、または、その識別を必要としなくなった場合、その管理者は、この規則の遵守の目的のみのために、データ主体を識別するための追加情報を維持管理し、取得し、または、処理することを義務付けられてはならない。
2. 本条第 1 項に示す場合において、データ主体を識別する立場にないことを管理者が説明できる場合、その管理者は、それが可能なときは、データ主体に対し、しかるべく通知する。そのような場合、データ主体が、それらの条項に基づく彼または彼女の権利の行使の目的のために、彼または彼女の識別ができるようにする追加情報を提供する場合を除き、第 17 条ないし第 22 条を適用してはならない。

第 13 条　公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のための処理と関連する安全性確保措置

公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のための処理は、この規則に従い、データ主体の基本的な権利及び自由のための適切な安全性確保措置に服する。それらの安全性確保措置は、とりわけ、データのミニマム化の原則の尊重を確保するための技術上及び組織上の措置が設けられることを確保する。それらの措置は、それらの処理の目的がそのような態様によって満たされ得る限り、仮名化を含めることができる。データ主体の識別を許容しない、または、許容しなくなった別の目的による処理によってそれらの処理の目的が満たされ得る場合、それらの処理の目的は、その態様において満たされる。

第 III 章　データ主体の権利

第 1 節　透明性及び書式

第 14 条　データ主体の権利の行使のための透明性のある情報提供、連絡及び書式

1. 管理者は、データ主体に対し、明解で、透明性があり、理解しやすく、容易にアクセスできる方式により、明瞭かつ平易な文言を用いて、処理と関連する第 15 条及び第 16 条に示す情報、並びに、第 17 条ないし第 24 条及び第 38 条に基づく連絡を提供するために、とりわけ、子どもに対して格別に対処する情報提供に関し、適切な措置を講じる。その情報は、書面により、または、それが適切であるときは、電子的な方法を含め、その他の方法により、提供される。データ主体から求められたときは、当該データ主体の同一性が他の手段によって証明される場合に限り、その情報を口頭で提供できる。
2. 管理者は、第 17 条ないし第 24 条に基づくデータ主体の権利の行使を容易にする。第 12 条第 2

項に示す場合、管理者は、データ主体を識別する立場にはないということを説明する場合を除き、第 17 条ないし第 24 条に基づく彼または彼女の権利を行使するためのデータ主体からの要請に基づく行為を拒否してはならない。

3. 管理者は、データ主体に対し、不適切な遅滞なく、かつ、いかなる場合においてもその要請を受けた時から 1 か月以内に、第 17 条ないし第 24 条に基づく要請に関して採られた行動に関する情報を提供する。この期間は、必要があるときは、その要請の難易及び数量を考慮に入れた上で、更に 2 か月延長できる。管理者は、データ主体に対し、その要請を受けた時から 1 か月以内に、その遅延の理由と共に、その期間延長を通知する。データ主体が電子的な方式の手段によってその要請を行った場合、データ主体から別の方法によることが求められている場合を除き、それが可能であるときは、電子的な手段によって提供される。
4. 管理者がデータ主体からの要請に応じて何らの行動も執らないときは、その管理者は、データ主体に対し、遅滞なく、かつ、その要請を受けてから遅くとも 1 か月以内に、何も行動を執らない理由、並びに、欧州データ保護監督官に異議を申立てることができること及び司法救済を求めることができることを通知する。
5. 第 15 条及び第 16 条に基づいて提供される情報並びに第 17 条ないし第 24 条及び第 35 条に基づく連絡及びこれらに基づいて執られる行動は、無料で提供される。データ主体からの要請が、特にその反復的な特徴により、明らかに根拠のない場合または過剰なものである場合、管理者は、要請された行動を拒否できる。管理者は、その要請が明らかに根拠のないものであることまたは過剰な性質のものであることについて、説明をする責任を負う。
6. 第 12 条を妨げることなく、第 17 条ないし第 23 条に示す要請をする自然人の同一性に関して管理者が合理的な疑いをもつ場合、その管理者は、そのデータ主体の同一性を確認するために必要となる追加情報の提供を要求できる。
7. 第 15 条及び第 16 条によりデータ主体に対して提供される情報は、容易に視認でき、分かりやすく、明確に理解できる態様により、予定されている処理の意味のある概要を提供するための標準的なアイコンと組み合わせて提供され得る。アイコンが電子的に表示される場合、それらのアイコンは、機械読取可能なものとする。
8. 規則(EU) 2016/679 の第 12 条第 8 項に従い、アイコンによって示される情報及び標準的なアイコンを提供する手続を定める委任された行為を欧州委員会が採択する場合、それが適切なときは、欧州連合の機関及び組織は、そのような標準的なアイコンと組み合わされるこの規則の第 15 条及び第 16 条による情報を提供する。

第 2 節 情報提供及び個人データへのアクセス

第 15 条 データ主体から個人データが収集される場合において提供される情報

1. データ主体と関連する個人データがそのデータ主体から収集される場合、管理者は、その個人データを取得する時に、そのデータ主体に対し、以下の全ての情報を提供する:
   (a) 管理者の識別名及び連絡先;
   (b) データ保護責任者の連絡先;
   (c) 予定されている個人データの処理の目的及びその処理の法的根拠;

(d) 該当するときは、個人データの取得者または取得者の類型;
(e) 該当するときは、管理者が個人データを第三国または国際機関に移転することを予定しているという事実、及び、欧州委員会による十分性の判定の存否、または、第 48 条に示す移転の場合、適切な安全性確保措置または適合する安全性確保措置への参照、または、それらの安全性確保措置の複製を取得するための手段、もしくは、それらを利用できるようにするための手段。

2. 第 1 項に示す情報に加え、管理者は、個人データが取得される時点において、データ主体に対し、公正かつ透明性のある処理を確保するために必要となる以下の追加情報を提供する:
(a) 個人データが記録保存される期間、または、それが不可能なときは、その期間を決定するために用いられる基準;
(b) 個人データへのアクセス、個人データの訂正または削除、または、データ主体と関係する処理の制限をその管理者に対して要求する権利が存在すること、または、それが適切なときは、処理に対して異議を述べる権利、もしくは、データの可搬性の権利が存在すること;
(c) 処理が第 5 条第 1 項の(d)または第 10 条第 2 項の(a)に基づく場合、その撤回の前の同意に基づく処理の適法性に影響を与えることなく、いつでも、同意を撤回する権利が存在すること;
(d) 欧州データ保護監督官に異議を申立てる権利;
(e) 個人データの提供が法律上の義務もしくは契約上の義務、または、契約を締結する際に必要な義務であるか否か、並びに、データ主体がその個人データの提供の義務を負うか否か、及び、そのデータの提供をしない場合に生じ得る結果について;
(f) プロファイリングを含め、第 24 条第 1 項及び第 4 項に示す自動的な判定が存在すること、また、その場合、少なくとも、その判定に含まれている論理、並びに、データ主体に対するそのような処理の影響及びそれによって生ずると想定される結果に関する了解可能な情報。

3. 当該個人データが収集された際の目的とは別の目的による個人データの処理を管理者が予定している場合、その管理者は、データ主体に対し、当該別の目的による処理を開始する前に、当該別の目的に関する情報及び第 2 項に示す関連追加情報を提供する。

4. 第 1 項、第 2 項及び 3 項は、データ主体が既にその情報をもっている場合、その範囲内において、適用してはならない。

第 16 条 データ主体から個人データが収集されない場合において提供される情報

1. 個人データがデータ主体から取得されない場合、管理者は、データ主体に対し、以下の情報を提供する:
(a) 管理者の識別名及び連絡先;
(b) データ保護責任者の連絡先;
(c) 予定されている個人データの処理の目的及びその処理の法的根拠;
(d) 関係する個人データの類型;
(e) 該当するときは、個人データの取得者または取得者の類型;
(f) 該当するときは、管理者が個人データを第三国または国際機関に移転することを予定しているという事実、及び、欧州委員会による十分性の判定の存否、または、第 48 条に示す移

転の場合、適切な安全性確保措置または適合する安全性確保措置への参照、または、それらの安全性確保措置の複製を取得するための手段、もしくは、どこでそれらが利用できるようにされたか。

2. 第 1 項に示す情報に加え、管理者は、データ主体に対し、データ主体に関する公正かつ透明性のある処理を確保するために必要となる以下の追加情報を提供する:
   (a) 個人データが記録保存される期間、または、それが不可能なときは、その期間を決定するために用いられる基準;
   (b) 個人データへのアクセス、個人データの訂正または削除、または、データ主体と関係する処理の制限をその管理者に対して要求する権利が存在すること、または、それが適切なときは、処理に対して異議を述べる権利、もしくは、データの可搬性の権利が存在すること;
   (c) 処理が第 5 条第 1 項の(d)または第 10 条第 2 項の(a)に基づく場合、その撤回の前の同意に基づく処理の適法性に影響を与えることなく、いつでも、同意を撤回する権利が存在すること;
   (d) 欧州データ保護監督官に異議を申立てる権利;
   (e) どの情報源からその個人データが生じたか、及び、該当するときは、それは公衆がアクセス可能な情報源からのものであるかどうか;
   (f) プロファイリングを含め、第 24 条第 1 項及び第 4 項に示す自動的な判定が存在すること、また、その場合、少なくとも、その判定に含まれている論理、並びに、データ主体に対するそのような処理の影響及びそれによって生ずると想定される結果に関する了解可能な情報。
3. 管理者は、以下の時点において、第 1 項及び第 2 項に示す情報を提供する:
   (a) その個人データが処理される個別の状況を考慮に入れた上で、その個人データを取得した後の合理的な期間内に、ただし、遅くとも 1 か月以内に;
   (b) その個人データがデータ主体との間の連絡のために用いられる場合、遅くとも、当該データ主体に対して最初の連絡がなされる時に;または、
   (c) 他の取得者に対する開示が想定されている場合、遅くとも、その個人データが最初に開示される時点で。
4. 当該個人データが入手された際の目的とは別の目的のための個人データの処理を管理者が予定する場合、その管理者は、データ主体に対し、当該別の目的による処理を開始する前に、当該別の目的に関する情報及び第 2 項に示す関連する追加情報を提供する。
5. 第 1 項ないし第 4 項は、以下の場合には、その範囲内において、適用してはならない:
   (a) データ主体が既にその情報をもっている場合;
   (b) とりわけ、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的、または、統計の目的のための処理に関し、そのような情報の提供が不可能であるか、または、過大な負担を要することが明らかな場合、または、本条の第 1 項に示す義務が当該処理の目的の達成を不可能としてしまうおそれ、または、その達成を大きく妨げるおそれがある範囲内で;
   (c) データ主体の正当な利益を保護するための適切な措置を定める欧州連合法によって、その入手及び開示が明示で定められている場合;または、
   (d) 法律法上の守秘義務を含め、欧州連合法によって規律される職務上の守秘義務により、その個人データを秘密のものとして維持しなければならない場合。

6. 第 5 項の(b)に示す場合において、管理者は、その情報を公衆が利用できるようにすることを含め、データ主体の権利及び自由並びに適正な利益を保護するための適切な措置を講ずる。

第 17 条 データ主体によるアクセスの権利

1. データ主体は、管理者から、彼または彼女に関係する個人データが処理されているか否かの確認を得る権利、並びに、それが処理されている場合、その個人データ及び下記の情報にアクセスする権利をもつ：
   (a) 処理の目的;
   (b) 関係する個人データの類型;
   (c) 個人データが開示された、または、開示される取得者もしくは取得者の類型、とりわけ、第三国または国際機関の取得者;
   (d) それが可能であるときは、個人データが記録保存されることが予定されている期間、または、それが不可能なときは、その期間を決定するために用いられる基準;
   (e) 個人データの訂正または削除、データ主体と関係する個人データの処理の制限をその管理者に対して要求する権利が存在すること、または、その処理に対して異議を述べる権利が存在すること;
   (f) 欧州データ保護監督官に異議を申立てる権利;
   (g) 個人データがデータ主体から収集されたものではない場合、その収集源に関する利用可能な全ての情報;
   (h) プロファイリングを含め、第 24 条第 1 項及び第 4 項に示す自動的な判定が存在すること、また、その場合、少なくとも、その判定に含まれている論理、並びに、データ主体に対するそのような処理の影響及びそれによって生ずると想定される結果に関する了解可能な情報。
2. 個人データが第三国または国際機関に移転される場合、データ主体は、その移転に関して、第 48 条による適切な安全性確保措置の通知を受ける権利をもつ。
3. 管理者は、処理中の個人データの複製物を提供する。データ主体が電子的な方法によってその要求を行う場合、データ主体から別異の要求がある場合を除き、その情報は、一般的に用いられる電子的な方式を用いて提供される。
4. 第 3 項に示す複製物を得る権利は、他の者の権利及び自由を害してはならない。

第 3 節 訂正及び削除

第 18 条 訂正の権利

データ主体は、管理者から、不適切な遅滞なく、彼または彼女と関係する不正確な個人データの訂正を得る権利をもつ。処理の目的を考慮に入れた上で、データ主体は、補足的な文言を提供する方法による場合を含め、不完全な個人データを完全なものとさせる権利をもつ。

第 19 条 削除の権利(「忘れられる権利」)

1. 以下の根拠のいずれかが適用される場合、データ主体は、管理者から、不適切な遅滞なく、彼または彼女に関する個人データの削除を得る権利をもち、そして、管理者は、不適切な遅滞なく、個人データを削除すべき義務を負う:
   (a) 個人データが、それが収集された目的またはそれ以外の処理がされた目的との関係において、必要のないものとなっている場合;
   (b) データ主体が、第 5 条第 1 項の(d)または第 10 条第 2 項の(a)に従い、その処理の根拠となっている同意を撤回し、かつ、その処理のための法的根拠が他に存在しない場合;
   (c) データ主体が、第 23 条第 1 項によって、処理に対する異議を述べ、かつ、その処理のための優越する正当な法的根拠が存在しない場合;
   (d) 個人データが違法に処理された場合;
   (e) 管理者が服する法的義務を遵守するため、その個人データが削除されなければならない場合;
   (f) 個人データが、第 8 条第 1 項に示す情報社会サービスの提供との関係において収集された場合。
2. 管理者が個人データを公開のものとしており、かつ、第 1 項によってその個人データを削除すべき義務を負う場合、その管理者は、利用可能な技術及びその実装費用を考慮に入れた上で、その個人データを処理している管理者に対し、または、その個人データを処理している欧州連合の機関及び組織以外の管理者に対し、そのデータ主体が、そのデータ主体の個人データへのリンクまたはそのコピーもしくは複製物がその管理者によって削除されることを請求した旨の通知をするための、技術上の措置を含め、合理的な手立てを講ずる。
3. 第 1 項及び第 2 項は、以下のために処理が必要となる範囲内において、適用してはならない:
   (a) 表現の自由及び情報提供の自由の権利の行使のため;
   (b) 管理者が服する法律上の義務の遵守のため、または、公共の利益において、もしくは、その管理者に与えられた公的な権限の行使において実施される職務の遂行のため;
   (c) 第 10 条第 2 項の(h)及び(i)並びに第 10 条第 3 項に従い、公衆衛生の分野における公共の利益上の理由のため;
   (d) 本条の第 1 項に示す権利が当該目的の達成を不可能としてしまうおそれ、または、その達成を大きく妨げるおそれがある範囲内で、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のため;または、
   (e) 訴えの提起、攻撃防御のため。

第 20 条 処理の制限の権利

1. データ主体は、以下のいずれかが適用される場合、管理者から、処理の制限を得る権利をもつ:
   (a) 個人データの正確性についてデータ主体から疑義が提示されている場合、完全性を含め、その個人データの正確性について管理者が確認することができるようにする期間内において;
   (b) 処理が違法であり、かつ、データ主体が個人データの削除に反対し、その代わりに、そのデ

ータの利用の制限を求めている場合;

(c) 管理者がその処理の目的のためにはその個人データを必要としないが、訴訟の提起及び攻撃防御のためにそのデータがデータ主体から要求されている場合;

(d) データ主体が、管理者の正当性の根拠がデータ主体の正当性の根拠よりも優越するか否かの確認を争い、第 23 条第 1 項により、処理に対する異議を申立てている場合。

2. 第 1 項に基づいて処理が制限された場合、そのような個人データは、記録保存の場合を除き、データ主体の同意がある場合、または、訴えの提起及び攻撃防護のための場合、または、他の自然人もしくは法人の権利を保護するための場合、または、欧州連合もしくは構成国の重要な公共の利益上の理由による場合においてのみ、処理される。

3. 第 1 項により処理の制限を得たデータ主体は、その処理の制限が解除される前に、管理者からその通知を受ける。

4. 自動的なファイリングシステムにおいて、処理の制限は、原則として、技術的な手段によって確保される。個人データが制限されているという事実は、その個人データを使用できないことが分かるような態様で、そのシステムの中で表示される。

第 21 条 個人データの訂正もしくは削除または処理の制限に関する通知義務

管理者は、それが不可能であること、または、過大な負担を要することが明らかである場合を除き、そのデータの開示を受けた個々の取得者に対し、第 18 条、第 19 条第 1 項及び第 20 条に従って実施された個人データの訂正もしくは削除または処理の制限を通知する。管理者は、データ主体に対し、そのデータ主体がそれを求めるときは、その取得者に関して情報提供する。

第 22 条 データの可搬性の権利

1. データ主体は、以下の場合においては、彼または彼女が管理者に対して提供した彼または彼女と関係する個人データを、構成され、一般に用いられ、かつ、機械読取可能なフォーマットで受信する権利をもち、また、その個人データの提供を受けた管理者から妨げられることなく、別の管理者に対してその個人データを送信する権利をもつ:

(a) その処理が第 5 項第 1 項の(d)もしくは第 10 条第 2 項の(a)による同意、または、第 5 条第 1 項の(c)による契約に基づくものであり;かつ、

(b) その処理が自動的な手段によって実施される場合。

2. 第 1 項による彼または彼女のデータの可搬性の権利を行使する際、データ主体は、それが技術的に実現可能な場合、ある管理者から、別の管理者に対し、または、欧州連合の機関もしくは組織以外の管理者に対し、直接にその個人データを送信させる権利をもつ。

3. 本条の第 1 項に示す権利の行使は、第 19 条を妨げない。この権利は、公共の利益において実施される職務、または、管理者に与えられた公的な権限の行使において実施される職務の遂行のために必要となる処理に適用してはならない。

4. 第 1 項に示す権利は、他の者の権利及び自由に対して負の影響を与えてはならない。

第 4 節　異議を述べる権利及び自動的な個人の判定

第 23 条　異議の権利

1. データ主体は、彼または彼女の特別な状況と関連する根拠に基づき、第 5 条第 1 項の(a)に基づく彼または彼女と関係する個人データの処理に対して、同条項に基づくプロファイリングの場合を含め、いつでも、異議を述べる権利をもつ。管理者は、データ主体の利益、基本的な権利及び自由よりも優越する処理に関する、または、訴えの提起及び攻撃防御に関する強制的な正当化根拠をその管理者が説明しない限り、以後、その個人データを処理してはならない。
2. 遅くともデータ主体への最初の連絡の時点において、第 1 項に示す権利は、明示でデータ主体の注意を引くようにされ、かつ、他の情報とは明確に区別して表示されるものとする。
3. 第 36 条及び第 37 条を妨げることなく、情報社会サービスの利用の過程において、データ主体は、技術仕様を用いる自動的な手段によって彼または彼女の異議の権利を行使できる。
4. 科学調査もしくは歴史調査の目的または統計の目的で個人データが処理される場合、データ主体は、公共の利益上の理由によって実施される職務の遂行のためにその処理が必要となる場合を除き、彼または彼女と関係する個人データの処理に対して異議を述べる権利をもつ。

第 24 条　プロファイリングを含め、自動化された個人の判定

1. データ主体は、プロファイリングを含め、自動的な処理のみを基礎とし、彼もしくは彼女に関する法的効果を発生させ、または、彼もしくは彼女に対して類似の大きな影響を及ぼす判定の対象とされない権利をもつ。
2. 第 1 項は、その判定が以下に該当する場合には、適用してはならない：
   (a) データ主体とデータの管理者の間の契約の締結またはその履行のために必要となる場合；
   (b) データ主体の権利及び自由並びに正当な利益を防護するための適切な措置も定める欧州連合法によって認められる場合；または、
   (c) データ主体の明示の同意に基づく場合。
3. 第 2 項の(a)及び(c)に示す場合、管理者は、データ主体の権利及び自由並びに正当な利益、少なくとも、管理者の側における人間の関与を得る権利、彼または彼女の見解を表明する権利及びその判定を争う権利を防護するための適切な措置を実装する。
4. 第 10 条第 2 項の(a)または(g)が適用され、かつ、データ主体の権利及び自由並びに正当な利益を防護するための適切な措置が設けられている場合を除き、第 2 項に示す判定は、第 10 条第 1 項に示す特別類型の個人データを基礎としてはならない。

第 5 節　制限

第 25 条　制限

1. 諸条約に基づいて採択された法的行為、または、欧州連合の機関及び組織の業務遂行と関連する事項に関し、欧州連合の機関及び組織によって定められた内部規則は、その制限が基本的な

権利及び自由の本質的を尊重し、かつ、以下の対象を防護するために民主主義社会において必要かつ比例的な措置である場合、第 14 条ないし第 22 条に定める権利及び義務にそれらの法令の条項が対応する範囲内において、第 14 条ないし第 22 条、第 35 条及び第 36 条並びに第 4 条の適用を制限できる：

(a) 構成国の国家安全保障、公共の安全または国防；
(b) 公共の安全への脅威に対する防護を含め、犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行；
(c) 欧州連合または構成国の一般的な公共の利益の上記以外の重要な対象、とりわけ、欧州連合の共通対外政策及び安全保障政策、または、出納、予算及び税務上の事項、公衆衛生及び社会保障を含め、欧州連合または構成国の重要な経済的な利益もしくは財政上の利益、；
(d) その電子通信ネットワークを含め、欧州連合の機関及び組織の内部的な安全性；
(e) 司法権の独立及び司法手続の保護；
(f) 規制を受ける職業における倫理違背行為の防止、捜査、検知及び訴追；
(g) (a)ないし(c)に示す場合において、一時的なものを含め、公的な権限の行使と関係する監視、監査及び規制の権能；
(h) データ主体の保護、または、それ以外の者の権利及び自由の保護；
(i) 民事法上の請求の執行。

2. とりわけ、第 1 項に示す法的行為または内部規則は、それが適切なときは、以下と関連する個別の条項を含める：
(a) 処理の目的；
(b) 個人データの類型；
(c) 導入される制限の適用範囲；
(d) 濫用または違法アクセスまたは移転に対する安全性確保措置；
(e) 管理者の指定または管理者の類型；
(f) 記録保存の期間、並びに、処理の性質、範囲及び目的または処理の類型を考慮に入れた上で適用される安全性確保措置；
(g) データ主体の権利及び自由に対するリスク。

3. 科学調査もしくは歴史調査の目的または統計の目的で個人データが処理される場合、欧州連合法（欧州連合の機関及び組織の業務遂行と関連する事項に関してそれらの機関及び組織によって採択された内部規則を含めることができる。）は、その権利がそれらの目的の達成を不可能としてしまうおそれ、または、その達成を大きく妨げるおそれがあり、かつ、そのような特例がそれらのこれらの目的を満たすために必要となる範囲内で、第 13 条に示す条件及び安全性確保措置に従い、第 17 条、第 18 条、第 20 条及び第 23 条に示す権利の特例を定めることができる。

4. 公共の利益におけるアーカイブの目的のために個人データが処理される場合、欧州連合法（欧州連合の機関及び組織の業務遂行と関連する事項に関してそれらの機関及び組織によって採択された内部規則を含めることができる。）は、その権利がそれらの目的の達成を不可能としてしまうおそれ、または、その達成を大きく妨げるおそれがあり、かつ、そのような特例がそれらの目的を満たすために必要な範囲内で、第 13 条に示す条件及び安全性確保措置に従い、第 17 条、第 18 条、第 20 条、第 21 条、第 22 条及び第 23 条に示す権利の特例を定めることができる。

5. 第 1 項、第 3 項及び第 4 項に示す内部規則は、データ主体それぞれとの間において法的効果を発生させることを予定し、欧州連合の機関及び組織の最も高いレベルの運営体によって採択され、かつ、EU 官報上で公示され、一般的な適用のある明確かつ詳細な法令とする。
6. 第 1 項による制限が加えられる場合、データ主体は、欧州連合法に従い、その制限の適用が根拠とする主要な理由、及び、欧州データ保護監督官に異議を申立てる彼または彼女の権利の通知を受ける。
7. 第1項によって加えられる制限がデータ主体に対するアクセスの拒否に基づく場合、欧州データ保護監督官は、その異議を調査した上で、彼または彼女に対し、そのデータが正確に処理されたか否か、及び、そうでない場合には、必要な訂正が行われたか否かを通知する。
8. 第 6 項及び第 7 項並びに第 45 条第 2 項に示す情報提供は、本条第 1 項により加えられた制限の効果が失われる可能性がある場合、延期され、省略され、または、拒否され得る。

第 IV 章　管理者及び処理者

第 1 節　一般的な義務

第 26 条　管理者の責任

1. 処理の性質、範囲、過程及び目的、並びに、自然人の権利及び自由に対する様々な発生確率と深刻度のリスクを考慮に入れた上で、管理者は、この規則に従って処理が遂行されることを確保し、かつ、そのことを説明できるようにするための適切な技術上及び組織上の措置を実装する。それらの措置は、見直され、そして、必要があるときは、最新のものに改められる。
2. 処理活動との関係において比例的である場合、第 1 項に示す措置は、適切なデータ保護方針の管理者による実装を含める。
3. 規則(EU) 2016/679 の第 42 条に示す承認された認証方法によることは、管理者の義務の遵守を説明するための要素の 1 つとして使用され得る。

第 27 条　バイデザイン及びバイデフォルトによるデータ保護

1. 最新技術、実装費用、処理の性質、範囲、過程及び目的、並びに、処理によって示される自然人の権利及び自由に対する様々な発生確率と深刻度のリスクを考慮に入れた上で、管理者は、この規則の要件に適合するため、及び、データ主体の権利を保護するため、処理の方法を決定する時点及び処理それ自体の時点の両時点において、データのミニマム化のようなデータ保護の基本原則を効果的な態様で実装し、かつ、その処理の中に必要な安全性確保措置を統合するために設計された、仮名化のような、適切な技術上及び組織上の措置を実装する。
2. 管理者は、個々の個別の処理の目的のために必要となる個人データのみが処理されることをデフォルトで確保するための適切な技術上及び組織上の措置を実装する。この義務は、収集される個人データの分量、その処理の範囲、その記録保存の期間及びアクセシビリティに対して適用される。とりわけ、そのような措置は、デフォルトで、人間が関与することなく、不特定数の自然人に対して個人データがアクセス可能とされないことを確保する。

3. 規則(EU) 2016/679 の第 42 条に示す承認された認証方法によることは、本条の第 1 項及び第 2 項の遵守を説明するための要素の 1 つとして使用され得る。

第 28 条 共同管理者

1. 複数の管理者が、または、欧州連合の機関及び組織以外の 1 もしくは複数の管理者と共に 1 または複数の管理者が処理の目的及び方法を決定する場合、それらの管理者は、共同管理者となる。それらの管理者は、共同管理者が服する欧州連合法または構成国法によって共同管理者それぞれの職責が定められていない限り、その範囲内において、それらの管理者間の覚書により、データ保護義務の遵守に関する、とりわけ、データ主体の権利の行使に関するそれらの管理者それぞれの職責を透明性のある態様で決定する。その覚書は、データ主体のための連絡部局を指定できる。
2. 第 1 項に示す覚書は、共同管理者それぞれの役割、及び、共同管理者各自とデータ主体との間の関係を適正に反映するものとする。覚書の要旨は、データ主体が利用できるようにされる。
3. 第 1 項に示す覚書の条件に拘らず、データ主体は、個々の管理者との関係において、及び、個々の管理者を相手方として、この規則に基づく彼または彼女の権利を行使できる。

第 29 条 処理者

1. 管理者の代わりの者によって処理が実施される場合、その管理者は、この規則の要件に処理が適合するような態様で適切な技術上及び組織上の措置を実装すること、並びに、データ主体の権利の保護を確保することについて十分な保証を提供する処理者のみを用いる。
2. 処理者は、管理者から、書面による個別的または一般的な事前承認を得ることなく、別の処理者を業務に従事させてはならない。書面による一般的な承認の場合、その処理者は、管理者に対し、別の処理者の追加または交代に関する変更予定を通知する。それによって、その管理者は、そのような変更に異議を述べる機会が与えられる。
3. 処理者による処理は、管理者との関係において処理者を拘束し、かつ、処理の対象及び期間、処理の性質及び目的、個人データの種類及びデータ主体の類型、並びに、管理者の義務及び権利を定める契約によって、または、それ以外の、欧州連合法もしくは構成国法に基づく法的行為によって規律される。契約またはそれ以外の法的行為は、とりわけ、処理者が以下のことを行うことを定める：
   (a) 処理者が服する欧州連合法または構成国法がそのようにすることを要求する場合を除き、個人データの第三国または国際機関への移転と関連するものを含め、管理者からの文書化された指示のみに基づいて個人データを処理すること；そのような場合、処理者は、管理者に対し、そのような公共の利益上の重要な法的根拠に関する通知を当該の法律が禁止している場合を除き、処理の前に、当該法律上の義務について通知する；
   (b) 個人データの処理を承認された者が自ら守秘義務を課し、または、適切な法律上の守秘義務に服することを確保すること；
   (c) 第 33 条によって求められる全ての措置を講ずること；
   (d) 別の処理者を業務に従事させるために、第 2 項及び第 4 項に示す条件を尊重すること；

(e) 第 III 章に定めるデータ主体の権利の行使に関する求めに対応すべき管理者の義務を満たすため、処理の性質を考慮に入れた上で、可能な限り、適切な技術上及び組織上の措置によって管理者を補助すること;

(f) 処理の性質及び処理者にとって利用可能な情報を考慮に入れた上で、第 33 条ないし第 40 条による義務の遵守において、管理者を補助すること;

(g) 処理と関連するサービスの提供が終了した後、管理者の選択により、全ての個人データを消去し、または、その管理者に返還すること、及び、欧州連合法または構成国法が個人データの記録保存を要求する場合を除き、存在している複製物を削除すること;

(h) 本条に定める義務の遵守を説明するため、及び、管理者によって実施され、または、管理者から委任された別の監査人によって実施される検査を含め、監査を可能とし、監査に資するために必要となる全ての情報を、管理者が利用できるようにすること。

第 1 副項の(h)に関し、処理者は、その見解において、指示がこの規則またはそれ以外の欧州連合または構成国のデータ保護法令の条項に違反する場合、直ちに、そのことを管理者に通知する。

4. 管理者の代わりに特定の処理を実施するために、処理者が別の処理者を業務に従事させる場合、契約によって、または、欧州連合法もしくは構成国法に基づくそれ以外の法的行為によって、とりわけ、その処理がこの規則の義務に適合するような態様で適切な技術上及び組織上の措置を実装する十分な保証を提供することによって、当該別の処理者に対し、第 3 項に示す管理者及び処理者間の契約もしくはそれ以外の法的行為に定めるのと同じデータ保護上の義務が課される。当該別の処理者がそのデータ保護の義務を満たさない場合、当初の処理者は、当該別の処理者の義務の履行について、その管理者に対する法的責任を全面的に負ったままとする。

5. 処理者が欧州連合の機関または組織ではない場合、その処理者が、規則(EU) 2016/679 の第 40 条第 5 条に示す承認された行動準則または規則(EU) 2016/679 の第 42 条に示す承認された認証方法によることは、本条の第 1 項及び第 4 項に示す十分な保証を説明するための要素の 1 つとして、これを用いることができる。

6. 管理者と処理者との間の個々の契約を妨げることなく、第 3 項もしくは第 4 項に示す契約またはそれ以外の法的行為は、規則(EU) 2016/679 の第 42 条によって欧州連合の機関もしくは組織以外の処理者に対して与えられる認証の一部分となる場合を含め、その全部または一部について、本条の第 7 項及び第 8 項に示す標準約款を基礎とすることができる。

7. 欧州委員会は、本条の第 3 項及び第 4 項に示す事項のために、かつ、第 96 条第 2 項に示す審議手続に従い、標準約款を定めることができる。

8. 欧州データ保護監督官は、本条の第 3 項及び第 4 項に示す事項のために、標準約款を採択できる。

9. 第 3 項及び第 4 項に示す契約またはそれ以外の法的行為は、電子的な方式による場合を含め、書面によるものとする。

10. 第 65 条及び第 66 条を妨げることなく、処理の目的及び方法を定めることによって処理者がこの規則に違反する場合、その処理者は、当該処理との関係においては、管理者とみなされる。

第 30 条 管理者または処理者の承認の下における処理

処理者、並びに、管理者の承認または処理者の承認の下で行動し、個人データにアクセスする者は、欧州連合法または構成国法がそのようにすることを要求する場合を除き、管理者からの指示がない限り、その個人データを処理してはならない。

第 31 条 処理活動の記録

1. 個々の管理者は、その責任において、処理活動の記録を維持管理する。その記録は、以下の情報の全てを含める:
   (a) 管理者、データ保護責任者の名称及び連絡先、並びに、該当するときは、処理者及び共同管理者の名称及び連絡先;
   (b) 処理の目的;
   (c) データ主体の類型の記述及び個人データの類型の記述;
   (d) 構成国内、第三国内または国際機関内の取得者を含め、個人データが開示された取得者または開示される取得者の類型;
   (e) 該当するときは、当該第三国もしくは国際機関の識別名及び適切な安全性確保措置文書を含め、第三国または国際機関に対する個人データの移転;
   (f) 可能であるときは、異なる類型のデータの削除のために予定されている期限;
   (g) 可能であるときは、第 33 条に示す技術上及び組織上の防護措置の一般的な記述。
2. 個々の処理者は、管理者の代わりに実施される全ての類型の処理の記録を維持管理する。以下の事項を含める:
   (a) 処理者の名称及び連絡先及びその処理者がその代わりに活動している個々の管理者の名称及び連絡先、並びに、データ保護責任者の名前及び連絡先;
   (b) 個々の管理者の代わりに実施される処理の類型;
   (c) 該当するときは、当該第三国または国際機関の識別名及び適切な安全性確保措置文書を含め、第三国または国際機関に対する個人データの移転;
   (d) 可能であるときは、第 33 条に示す技術上及び組織上の防護措置の一般的な記述。
3. 第 1 項及び第 2 項に示す記録は、電子的な方式による場合を含め、書面による。
4. 欧州連合の機関及び組織は、要請に応じて、欧州データ保護監督官が記録を利用できるようにする。
5. 欧州連合の機関または組織の規模を考慮に入れ、それが適切ではない場合を除き、欧州連合の機関及び組織は、その処理活動の記録を中央登録所の中で保管する。その機関及び組織は、公衆がその登録所にアクセスできるようにする。

第 32 条 欧州データ保護監督官への協力

欧州連合の機関及び組織は、要請に応じて、彼または彼女の職務の遂行において欧州データ保護監督官に協力する。

第 2 節 個人データの安全性

第 33 条 処理の安全性

1. 最新技術、実装費用、処理の性質、範囲、過程及び目的、並びに、自然人の権利及び自由に対する様々な発生確率と深刻度のリスクを考慮に入れた上で、管理者及び処理者は、リスクに適切に対応する一定のレベルの安全性を確保するため、とりわけ、以下のものを含め、適切な技術上及び組織上の措置をしかるべく実装する:
   (a) 個人データの仮名化または暗号化;
   (b) 処理システム及び処理サービスの現在の機密性、完全性、可用性及び回復力を確保する能力;
   (c) 物的または技術的なインシデントが発生した場合、適時な態様で、個人データの可用性及びアクセシビリティを復旧する能力;
   (d) 処理の安全性を確保するための技術上及び組織上の措置の実効性の継続的な試験、評価及び評定のための手順。
2. 評価の際、適切なレベルの安全性が考慮に入れられるものとし、とりわけ、処理によって示されるリスク、とりわけ、送受信、記録保存またはそれ以外の処理が行われる個人データの偶発的または違法な破壊、喪失、改変、無権限の開示または無権限のアクセスからのリスクが考慮に入れられるものとする。
3. 管理者及び処理者は、管理者または処理者の承認の下で行動し、個人データにアクセスする自然人が、彼または彼女が欧州連合法によってそのようにすることが要求される場合を除き、管理者の指示がない限り、その個人データを処理しないことを確保するための手立てを講ずる。
4. 規則(EU) 2016/679 の第 42 条に示す承認された認証方法によることは、本条の第 1 項に定める要件の遵守を説明するための要素の 1 つとして使用され得る。

第 34 条 欧州データ保護監督官に対する個人データ侵害の通知

1. 個人データ侵害が発生した場合、管理者は、その個人データ侵害が自然人の権利及び自由に対するリスクを発生させるおそれがない場合を除き、不適切な遅滞なく、かつ、それが実施可能であるときは、その侵害に気づいた時から遅くとも 72 時間以内に、欧州データ保護監督官に対し、その個人データ侵害を通知する。欧州データ保護監督官への通知が 72 時間以内に行われない場合、その通知は、その遅延の理由を付す。
2. 処理者は、個人データ侵害に気づいた後、不適切な遅滞なく、管理者に対して通知する。
3. 第 1 項の通知は、少なくとも、以下のとおりとする:
   (a) それが可能であるときは、関係するデータ主体の類型及び概数、並びに、関係する個人データ記録の類型及び概数を含め、その個人データ侵害の性質を記述し;
   (b) データ保護責任者の名前及び連絡先を連絡し;
   (c) その個人データ侵害の結果として発生する可能性のある事態を記述し;
   (d) それが適切なときは、それによって発生し得る負の影響の拡大を削減するための措置を含め、その個人データ侵害に対処するために管理者によって講じられた措置または講ずる準

備のされた措置を記述する。

4. 同時に情報を提供することができない場合、その範囲内において、その情報は、更なる不適切な遅滞なく、その状況に応じて提供できる。
5. 管理者は、データ保護責任者に対し、その個人データ侵害を通知する。
6. 管理者は、第 1 項に示す全ての個人データ侵害について、その個人データ侵害に関する事実関係、その影響及び復旧措置を含め、文書化する。その文書は、本条の遵守を検証するため、欧州データ保護監督官が利用できるものとされる。

第 35 条 データ主体に対する個人データ侵害の連絡

1. 個人データ侵害が自然人の権利及び自由に対する高度なリスクを発生させるおそれがある場合、管理者は、そのデータ主体に対し、不適切な遅滞なく、その個人データ侵害を連絡する。
2. 本条第 1 項に示すデータ主体に対する連絡は、明確かつ平易な文言により、その個人データ侵害の性質を記述し、かつ、少なくとも、第 34 条第 3 項の(b)、(c)及び(d)に示す情報及び措置を含める。
3. 以下の条件に該当する場合、第 1 項に示すデータ主体に対する連絡を要しない：
   (a) 管理者が適切な技術上及び組織上の防護措置を実装し、かつ、それらの措置、とりわけ、暗号のような、承認を受けていない者にとってその運用個人データを知覚不可能なものとする措置が、個人データ侵害によって害を受けた個人データに適用された場合；
   (b) 管理者が、第 1 項に示すデータ主体の権利及び自由に対する高度なリスクが現実化するおそれがないことを確保する事後的な措置を講じた場合；
   (c) それが過大な負担を要するような場合。そのような場合、データ主体が平等に効果的な方法で情報伝達される公衆通信またはそれに類する手段によって代えられる。
4. 管理者がデータ主体に対して個人データ侵害をまだ連絡していない場合、欧州データ保護監督官は、その個人データ侵害が高度なリスクを発生させるおそれについて検討した上で、その管理者に対し、そのようにすべきことを要求することができ、または、第 3 項に示す条件のいずれかの該当を判断できる。

第 3 節 電子通信の秘密

第 36 条 電子通信の秘密

欧州連合の機関及び組織は、とりわけ、それらの電子通信ネットワークを防護することによって、電子通信の秘密を確保する。

第 37 条 利用者の端末装置に送信され、その中に記録保存され、それによって処理され、その中から収集される情報の保護

欧州連合の機関及び組織は、指令 2002/58/EC の第 5 条第 3 項に従い、公衆が利用可能な Web サイトにアクセスする端末装置及びモバイルアプリケーションに送信され、その中に記録保存され、それ

によって処理され、その中から収集される情報を保護する。

第 38 条 利用者名簿

1. 利用者名簿の中に含まれている個人データ及びそのような名簿に対するアクセスは、その名簿の特定の目的のために厳格に必要なものに限定される。
2. 欧州連合の機関及び組織は、その名簿が公衆にとってアクセス可能であるか否かを問わず、その名簿の中に含まれている個人データがダイレクトマーケティングのために用いられることを防止するために必要となる全ての措置を講ずる。

第 4 節 データ保護影響評価及び事前協議

第 39 条 データ保護影響評価

1. 処理の性質、範囲、過程及び目的を考慮に入れた上で、ある種類の処理、特に新たな技術を用いる処理が、自然人の権利及び自由に対して高度なリスクをもたらすおそれがある場合、管理者は、処理を開始する前に、個人データの保護に対する予定された処理業務の影響の評価を実施する。類似の高度のリスクを示す類似の処理業務のセットを単一の評価の対象とすることができる。
2. 管理者は、データ保護影響評価を実施する際、データ保護責任者から助言を求める。
3. 第 1 項に示すデータ保護影響評価は、とりわけ、以下の場合において要求される:
   (a) プロファイリングを含め、自動的な処理を基礎とし、かつ、それに基づく判断が自然人と関係する法的効果を発生させ、または、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面のシステムによる拡張的な評価の場合;
   (b) 第 10 条に示す特別類型のデータまたは第 11 条に示す有罪判決及び犯罪行為と関連する個人データの大規模な処理の場合;または、
   (c) 公衆がアクセス可能な領域の、システムによる大規模な監視の場合。
4. 欧州データ保護監督官は、第 1 項によるデータ保護影響評価の義務に服する処理業務の種類のリストを作成し、公表する。
5. 欧州データ保護監督官は、データ保護影響評価を要しない処理業務の種類のリストを作成し、これを公表することもできる。
6. 本条の第 4 項及び第 5 項に示すリストを採択する前に、欧州データ保護監督官は、欧州連合の機関及び組織以外の 1 または複数の管理者と共同して行動する管理者による処理業務をそれらのリストが指示する場合、規則(EU) 2016/679 の第 68 条によって設置される欧州データ保護委員会が、同規則の第 70 条第 1 項の(e)によるようなリストを検討することを求める。
7. 評価は、少なくとも以下の事項を含める:
   (a) 予定されている処理業務及び処理の目的の体系的な記述;
   (b) 目的との関係におけるその処理業務の必要性及び比例性の評価;
   (c) 第 1 項に示すデータ主体の権利及び自由に対するリスクの評価;並びに、
   (d) データ主体及び他の関係者の権利及び正当な利益を考慮に入れた上で、個人データの保護を確保するための、及び、この規則の遵守を説明するための安全性確保措置、防護措置

及び仕組みを含め、リスクに対処するために用意されている手段。

8. とりわけ、データ保護影響評価の目的のために、欧州連合の機関及び組織以外の関係する処理者によって規則(EU) 2016/679 の第 40 条に示す承認された行動準則が遵守されることは、とりわけ、データ保護影響評価の目的にために、そのような処理者によって遂行される処理業務の影響を評価するに際し、これを十分に考慮に入れるものとする。
9. それが適切であるときは、公共の利益または処理業務の安全性を妨げることなく、管理者は、予定されている処理に関し、データ主体またはその代理者から意見を求める。
10. 第 5 条第 1 項の(a)または(b)による処理が、諸条約に基づいて採択された法的行為の中に法的根拠をもつ場合であって、その法的行為が、当の特定の処理業務または処理業務のセットを規律している場合、及び、当該法的行為の採択の前に、一般的な影響評価の一部として個人データ保護影響評価が既に実施されている場合、欧州連合法に別異の定めがある場合を除き、第 1 項ないし第 6 項を適用してはならない。
11. 必要があるときは、管理者は、遅くとも処理業務によって示されるリスクの変化がある時点において、データ保護影響評価に従って処理が遂行されているか否かを評価するために、見直しを実施する。

第 40 条 事前協議

1. 第 39 条に基づくデータ保護影響評価が、そのリスクを削減するための安全性確保措置、防護措置及び仕組みがなければ、自然人の権利及び自由に対する高度のリスクをもたらすおそれがあることを示しており、かつ、管理者が、利用可能な技術及び実装費用の面において、合理的な手段によってはそのリスクを削減できないとの見解をもつ場合、その管理者は、その処理を開始する前に、欧州データ保護監督官と協議する。管理者は、事前協議の要否に関し、データ保護責任者から助言を求める。
2. 欧州データ保護監督官が、第 1 項に示す予定された処理がこの規則に違反しているとの見解をもつ場合、とりわけ、管理者がそのリスクの特定及び削減を十分にしていない場合、欧州データ保護監督官は、協議の要請を受けた時から 8 週間以内に、その管理者に対し、及び、該当するときは、その処理者に対し、書面による助言を提示し、また、第 58 条に示す彼または彼女の権限を行使できる。この期限は、予定された処理の複雑性を考慮に入れた上で、6 週間まで延長され得る。欧州データ保護監督官は、管理者に対し、及び、該当するときは、処理者に対し、協議の要請を受けた時から 1 か月以内に、その遅延の理由と共に、その期限の延長を通知する。これらの期限は、その協議の目的のために必要とする情報を欧州データ保護監督官が入手するまでの間、進行停止とされ得る。
3. 第 1 項により欧州データ保護監督官と協議する場合、管理者は、欧州データ保護監督官に対し、以下の情報を提供する：
   (a) 該当するときは、その処理に関与する管理者、共同管理者及び処理者のそれぞれの職責；
   (b) 予定されている処理の目的及び方法；
   (c) この規則によりデータ主体の権利及び自由を保護するために提供される措置及び安全性確保措置；
   (d) データ保護責任者の連絡先；

(e) 第 39 条に定めるデータ保護影響評価;並びに、
(f) 欧州データ保護監督官から求められた上記以外の情報。

4. 欧州委員会は、実装行為により、社会保護及び公衆衛生と関連するようなデータの処理を含め、公共の利益において管理者によって実施される職務の遂行のための処理に関し、管理者が欧州データ保護監督官と協議すべき場合及び欧州データ保護監督官から事前の承認を得るべき場合のリストを定めることができる。

第 5 節 情報提供及び立法上の協議

第 41 条 情報提供及び協議

1. 欧州連合の機関及び組織は、単独であるか他の機関及び組織と共同であるかを問わず、個人データの処理と関連する行政上の措置及び内部規則を策定する場合、欧州データ保護監督官に対し、その情報を提供する。
2. 欧州連合の機関及び組織は、第 25 条に示す内部規則を策定する場合、欧州データ保護監督官と協議する。

第 42 条 立法上の協議

1. 欧州委員会は、立法行為案の採択、勧告案の採択、もしくは、TFEU の第 218 条による理事会に対する提案の採択の後、または、委任される行為または実装行為を準備する際、それらが個人データの処理と関連する個人の権利及び自由の保護に対して影響を及ぼすときは、欧州データ保護監督官と協議する。
2. 第 1 項に示す行為が個人データの処理と関連する個人の権利及び自由の保護にとって特に重要なものである場合、欧州委員会は、欧州データ保護委員会とも協議できる。そのような場合、欧州データ保護監督官及び欧州データ保護委員会は、共同意見書を発するため、それらの仕事を調整する。
3. 第 1 項及び第 2 項に示す助言は、第 1 項及び第 2 項に示す協議の要請を受けた時から 8 週間以内に、書面により提供される。緊急の場合、または、それ以外の適切な場合、欧州委員会は、その回答期限を短縮できる。
4. 本条は、規則(EU) 2016/679 により欧州委員会が欧州データ保護委員会と協議することを要する場合、適用してはならない。

第 6 節 データ保護責任者

第 43 条 データ保護責任者の任命

1. 欧州連合の機関または組織は、データ保護責任者を任命する。
2. 欧州連合の機関及び組織は、それらの機関及び組織の組織構造及び規模を考慮に入れた上で、複数の機関または組織のための単一のデータ保護責任者を任命できる。

3. データ保護責任者は、専門家としての資質、及び、とりわけ、データ保護の法令及び実務に関する専門知識並びに第 45 条に示す職務を充足するための能力に基づいて任命される。
4. データ保護責任者は、欧州連合の機関または組織の職員である。その機関または組織の規模を考慮に入れ、かつ、第 2 項を執行できない場合、欧州連合の機関及び組織は、サービス契約に基づいて彼または彼女の職務を充足させるデータ保護責任者を任命できる。
5. 欧州連合の機関及び組織は、データ保護責任者の連絡先を公表し、かつ、欧州データ保護監督官に対し、それを連絡する。

第 44 条　データ保護責任者の地位

1. 欧州連合の機関及び組織は、個人データの保護と関連する全ての問題について、適正かつ適時にデータ保護責任者が関与することを確保する。
2. 欧州連合の機関及び組織は、その職務を実施し、個人データ及び処理業務にアクセスし、並びに、彼または彼女の専門知識を維持するために必要となる資源を提供することにより、第 45 条に示す職務の遂行において、データ保護責任者を支援する。
3. 欧州連合の機関及び組織は、データ保護責任者が、その職務の遂行に関して、いかなる指示も受けないことを確保する。彼または彼女は、彼または彼女の職務遂行のゆえに、管理者または処理者から解任され、または、制裁を受けるものとしてはならない。データ保護責任者は、最も高い職位にある管理者または処理者に直属する。
4. データ主体は、その個人データの処理と関連する全ての問題に関し、及び、この規則に基づくその権利の行使と関連する全ての問題に関し、データ保護責任者と連絡をとることができる。
5. データ保護責任者及び彼または彼女の職員は、欧州連合法に従い、彼または彼女の職務の遂行と関係する秘密または機密を厳守する。
6. データ保護責任者は、上記以外の職務及び責務を満たすことができる。管理者または処理者は、そのような職務及び責務が利益相反とならないことを確保する。
7. データ保護責任者は、公式の経路を経ることなく、この規則の解釈または適用に関する事項に関し、管理者及び処理者から、職員委員会から及び個人から相談を受けることができる。いかなる者も、この規則の条項の違反が発生していると主張して、職務権限を有するデータ保護責任者の注意を向けさせたことのゆえに、不利益を受けるものとしてはならない。
8. データ保護責任者は、3 年ないし 5 年の任期で任命され、再任されることができる。データ保護責任者は、彼または彼女の責務を満たすために求められる条件を充足しなくなったときは、欧州データ保護監督官の同意がある場合に限り、彼または彼女を任命した欧州連合の機関または組織によってその地位を解任され得る。
9. データ保護責任者は、彼または彼女の任命の後、彼または彼女を任命した欧州連合の機関または組織によって、欧州データ保護監督官に登録される。

第 45 条　データ保護責任者の職務

1. データ保護責任者は、以下の職務をもつ：
   (a)　管理者または処理者及び処理を行う従業者に対し、この規則または欧州連合のデータ保護

法令による彼らの責務について情報提供し、かつ、助言をすること;

(b) 独立の態様で、この規則の内部的な適用を確保すること;処理業務に関与する職員の責任の割当て、意識向上及び訓練、並びに、関連する監査を含め、この規則の遵守、データ保護条項を含む他の適用可能な欧州連合法の遵守、並びに、個人データの保護と関連する管理者及び処理者の基本方針の遵守を監視すること;

(c) データ主体が、この規則による彼らの権利及び義務の情報提供を受けることを確保すること;

(d) その要請があるときは、第 34 条及び第 35 条による個人データ侵害の連絡または連絡の要否に関し、助言を提供すること;

(e) その要請があるときは、第 39 条によるデータ保護影響評価に関し、助言を提供し、及び、その遂行を監視し、並びに、データ保護影響評価の要否に関し、疑問のある場合に欧州データ保護監督官と協議すること

(f) その要請があるときは、第 40 条による欧州データ保護監督官との事前協議の要否に関し、助言を提供すること;事前協議の要否に関し、疑問のある場合に欧州データ保護監督官と協議すること;

(g) 欧州データ保護監督官からの要請に対応すること;彼または彼女の職務権限の範囲内で、欧州データ保護監督官の要請に応じて、または、彼または彼女の発意により、欧州データ保護監督官と協力及び協議すること;

(h) データ主体の権利及び自由が処理業務によって負の影響を受けないことを確保すること。

2. データ保護責任者は、管理者及び処理者に対し、データ保護の実務上の向上のための勧告を行うことができ、また、彼らに対し、データ保護の条項の適用に関する事項に関し、助言できる。更に、彼または彼女は、彼もしくは彼女の発意により、または、管理者もしくは処理者、関係する職員委員会もしくは個人の要請に応じて、彼または彼女の職務と直接に関連する事項及び出来事または彼または彼女が認知した事項及び出来事について調査し、そして、その調査を依頼した者に対し、または、管理者もしくは処理者に対し、その結果報告を返すことができる。

3. 欧州連合の機関または組織によって、データ保護責任者に関する個別の実装規則が採択される。その実装規則は、とりわけ、データ保護責任者の職務、責務及び権限に関するものとする。

第 V 章 第三国または国際機関に対する個人データの移転

第 46 条 移転のための一般原則

第三国または国際機関から別の第三国または国際機関に対する個人データの転送の場合を含め、第三国または国際機関に対する移転の後に現に処理されている個人データまたは処理される予定の個人データは、この規則の他の条項に従い、本章に定める条件が管理者及び処理者によって遵守される場合に限り、これを行うことができる。本章の全ての条項は、この規則によって保証される自然人保護のレベルが低下しないことを確保するために適用される。

第 47 条　十分性の判定に基づく移転

1. 欧州委員会が、規則(EU)2016/679 の第 45 条第 3 項または指令(EU) 2016/680 の第 36 条第 3 項により、当の第三国、第三国内の地域または 1 もしくは複数の特定の部門、または、国際機関の中において、十分なレベルの保護が確保されており、かつ、その処理を行う管理者の職務権限の範囲内にある職務を遂行することができるようにするためにのみ、その個人データが移転されると判定した場合、第三国または国際機関に対する個人データの移転を行うことができる。
2. 欧州連合の機関及び組織は、当の第三国、第三国内の地域または 1 もしくは複数の特定の部門、または、国際機関が第 1 項の意味における十分なレベルの保護を確保していないと判断するときは、欧州委員会及び欧州データ保護監督官に対し、その案件について、通知する。
3. 欧州連合の機関及び組織は、欧州委員会が、規則(EU)2016/679 の第 45 条第 3 項もしくは第 5 項、または、指令(EU) 2016/680 の第 36 条第 3 項もしくは第 5 項により、第三国または国際機関が十分なレベルの保護を確保していること、または、確保していないことを確認した場合に欧州委員会によって行われる判定を遵守するために必要となる措置を講ずる。

第 48 条　適切な安全性確保措置による移転

1. 規則(EU)2016/679 の第 45 条第 3 項または指令(EU) 2016/680 の第 36 条第 3 項による判定がない場合、管理者または処理者は、その管理者または処理者が適切な安全性確保措置を提供しており、かつ、データ主体の執行可能な権利及びデータ主体のための効果的な司法救済が利用可能なことを条件としてのみ、第三国または国際機関に対して個人データを移転できる。
2. 第1項に示す適切な安全性確保措置は、欧州データ保護監督官からいかなる個別の承認も求められることなく、以下のいずれかによって提供され得る：
   (a) 行政機関または行政組織の間の法的拘束力及び執行力のある文書;
   (b) 第 96 条第 2 項に示す審議手続に従って欧州委員会によって採択された標準データ保護約款;
   (c) 欧州データ保護監督官によって採択され、第 96 条第 2 項に示す審議手続に従って欧州委員会によって承認された標準データ保護約款;
   (d) 処理者が欧州連合の機関または組織ではない場合、規則(EU)2016/679 の第 46 条第 2 項の(b)、(e)及び(f)による拘束的企業準則、行動準則及び認証方法。
3. 欧州データ保護監督官の承認を条件として、第 1 項に示す安全性確保措置は、とりわけ、以下の方法によっても提供され得る：
   (a) 管理者または処理者と、第三国または国際機関内の管理者、処理者または個人データの取得者との間の契約条項;または、
   (b) 行政機関または行政組織の間の業務覚書の中に入れられる条項であって、執行可能かつ効果的なデータ主体の権利を含むもの。
4. 規則(EC) No 45/2001 の第 9 条第 7 号に基づく欧州データ保護監督官による承認は、それが必要なときは、欧州データ保護監督官によって改正され、置き換えられ、または、廃止されるまでは、その有効性を維持する。
5. 欧州連合の機関及び組織は、欧州データ保護監督官に対し、本条が適用された案件の類型を

通知する。

第 49 条　欧州連合の法律によって承認されない移転または開示

管理者または処理者に対して個人データの移転または開示を命ずる第三国の裁判所もしくは法廷の判決及び行政機関の決定は、本章による移転のためのそれ以外の法的根拠を妨げることなく、司法共助条約のような、要請元である第三国と欧州連合との間で有効な国際的な合意に基づく態様の場合に限り、承認または執行され得る。

第 50 条　特別の場合における特例

1. 規則(EU)2016/679 の第 45 条第 3 項もしくは指令(EU) 2016/680 の第 36 条第 3 項による判定がない場合、または、この規則の第 48 条による適切な安全性確保措置がない場合、以下の条件中のいずれか 1 つに基づいてのみ、第三国または国際機関に対する個人データまたは個人データのセットの移転を行うことができる:
   (a) データ主体が、十分性の判定及び適切な安全性確保措置がないために、そのような移転がそのデータ主体に対して発生させる可能性のあるリスクについて説明を受けた後に、その予定された移転に明示で同意した場合;
   (b) データ主体と管理者との間の契約の履行のためにその移転が必要となる場合、または、データ主体の求めにより、契約締結前の措置を実装するためにその移転が必要となる場合;
   (c) 管理者とそれ以外の自然人もしくは法人との間でデータ主体の利益のために結ばれる契約の締結またはその契約の履行のために移転が必要となる場合;
   (d) 公共の利益上の重要な理由のためにその移転が必要となる場合;
   (e) 訴訟の提起、攻撃防御のためにその移転が必要となる場合;
   (f) データ主体が身体的または法的に同意を与えることができない場合において、データ主体またはその他の者の生存の利益を保護するために移転が必要となる場合;または、
   (g) 欧州連合法に従い、公衆に対して情報を提供することを予定するものであり、かつ、公衆一般及び正当な利益があることを説明することのできる者の両者からの照会に対して開かれているが、特別の場合においては、照会に関する欧州連合法に定める条件が満たされる範囲内に限定されている登録所から移転が行われる場合。
2. 第 1 項の(a)、(b)及び(c)は、その機関及び組織の公権力の行使において欧州連合の機関及び組織によって実施される活動に対して、適用してはならない。
3. 第 1 項の(d)に示す公共の利益は、欧州連合法において認められるものとする。
4. 第 1 項の(g)による移転は、欧州連合法によって認められる場合を除き、その登録所に収録されている個人データ全体または全ての類型の個人データの移転の場合を含まない。その登録所が正当な利益をもつ者からの照会を予定するものである場合、その移転は、それらの者が求める部分に限定して、または、それらの者が取得者となる場合に限定して、行われる。
5. 十分性の判定がない場合、欧州連合法は、公共の利益上の重要な理由のために、第三国または国際機関に対する特別類型の個人データの移転に明示で制限を加えることができる。
6. 欧州連合の機関及び組織は、欧州データ保護監督官に対し、本条が適用された案件を通知する。

第 51 条 個人データ保護のための国際協力

第三国及び国際機関との関係において、欧州データ保護監督官は、欧州委員会及び欧州データ保護委員会と協力し、以下の適切な手立てを講ずる:

(a) 個人データの保護のための立法の効果的な執行を促進するための国際協力の仕組みを構築すること;
(b) 個人データ並びにその他の基本的な権利及び自由の保護のための適切な安全性確保措置に従い、連絡、苦情相談、調査の支援及び情報交換を介する場合を含め、個人データ保護のための立法の執行において、国際的な共助を提供すること;
(c) 利害関係者と意見交換を行うこと、及び、個人データ保護のための立法の執行における国際協力の拡大を目的とする活動をすること;
(d) 第三国との裁判管轄権の抵触を含め、個人データ保護の立法及び実務の交換及び文書化を促進すること。

第 VI 章 欧州データ保護監督官

第 52 条 欧州データ保護監督官

1. ここに欧州データ保護監督官が設置される。
2. 個人データの保護に関し、欧州データ保護監督官は、自然人の基本的な権利及び自由、とりわけ、自然人のデータ保護の権利が欧州連合の機関及び組織によって尊重されることを確保することについて、職責を負う。
3. 欧州データ保護監督官は、この規則の条項の適用、並びに、欧州連合の機関または組織による個人データの処理と関連する自然人の基本的な権利及び自由の保護と関連する他の欧州連合法の適用を監視し、かつ、確保することについて職責を負い、かつ、個人データの処理と関係する全ての事柄に関し、欧州連合の機関及び組織並びにデータ主体に対して助言することについて職責を負う。それらの目的のために、欧州データ保護監督官は、第 57 条に定める職務を遂行し、第 58 条において与えられる権限を行使する。
4. 規則(EC) No 1049/2001 は、欧州データ保護監督官が管理する文書に適用される。欧州データ保護監督官は、それらの文書に関連して、規則(EC) No 1049/2001 の適用に関する細則を採択する。

第 53 条 欧州データ保護監督官の任命

1. 欧州議会及び理事会は、候補者の公募の後に欧州委員会によって作成されるリストに基づき、一致した意見によって、5 年の任期で欧州データ保護監督官を任命する。候補者の募集に対しては、欧州連合内の全ての関係者がその応募書を提出できる。欧州委員会によって作成される候補者のリストは、公表され、かつ、少なくとも 3 名の候補者によって構成される。欧州委員会によって作成されるリストに基づき、欧州議会の職務権限を有する委員会は、欧州議会がその希望を表明できるようにするために、聴聞会の開催を決定できる。
2. 第 1 項に示すリストは、その独立性に疑問の余地がなく、かつ、データ保護の専門知識並びにデ

ータ保護監督官の職務を遂行するために要する経験及び技能をもつと認められる者をとりまとめて作成される。

3. 欧州データ保護監督官の任期は、1 度だけ更新される。
4. 欧州データ保護監督官の責務は、以下の場合においては、終了する:
   (a) 欧州データ保護監督官が交代となる場合;
   (b) 欧州データ保護監督官が辞任する場合;
   (c) 欧州データ保護監督官が解任され、または、強制的な退任を命ぜられる場合。
5. 欧州データ保護監督官は、彼または彼女が彼または彼女の責務を遂行するために要求される条件を満たさなくなった場合、または、彼または彼女が重大な非違行為により有罪となる場合において、欧州議会、理事会または欧州委員会の求めにより、司法裁判所によって、解任され、または、年金もしくはその代価となる収入を受ける彼または彼女の権利を剥奪され得る。
6. 通常の交代または任意の辞任の場合、欧州データ保護監督官は、その責務が終了となっても、彼または彼女が交代となるまでの間、その執務室に留まる。
7. 欧州連合の特権及び免除に関する議定書の第 11 条ないし第 14 条及び第 17 条は、欧州データ保護監督官に対して適用される。

第 54 条 欧州データ保護監督官の責務、職員及び資金を規律する規則及び一般的な条件

1. 欧州データ保護監督官は、報酬、手当、退職年金、並びに、報酬の代価となるその他の収入の決定に関し、司法裁判所の判事と均等と判断される。
2. 予算総局は、欧州データ保護監督官が、彼または彼女の職務を遂行するために必要となる人的資源及び資金を提供されることを確保する。
3. 欧州データ保護監督官の予算は、欧州連合の一般予算の行政上の支出の節の標題で区分された予算の中に示される。
4. 欧州データ保護監督官は、事務局の補佐を受ける。事務局の官吏及びその他の職員は、欧州データ保護監督官によって任命され、かつ、欧州データ保護監督官が彼らの上司となる。彼らは、専ら、彼または彼女の指示に服する。その員数は、毎年、予算手続の一部として決定される。規則(EU) 2016/679 の第 75 条第 2 項は、欧州連合法によって欧州データ保護委員会に与えられた職務を実施することに関与する欧州データ保護監督官の職員に対して適用される。
5. 欧州データ保護監督官の事務局の官吏及びそれ以外の職員は、欧州連合の官吏及びその他の公務員に適用される法令及び規則に服する。
6. 欧州データ保護監督官は、ブリュッセルにその本拠地をもつ。

第 55 条 独立性

1. 欧州データ保護監督官は、この規則に従い、彼または彼女の職務を遂行する際、及び、彼または彼女の権限を行使する際、完全に独立して行動する。
2. 欧州データ保護監督官は、この規則に従い、彼または彼女の職務を遂行する際、及び、彼または彼女の権限を行使する際、直接または間接を問わず、外部からの影響を受けることなく、かつ、誰に対しても指示を求めず、また、誰からの指示も受けない。

3. 欧州データ保護監督官は、彼または彼女の責務と適合しない行動を慎み、かつ、彼または彼女の在任中は、有償であるか否かを問わず、その職務と適合しない職業に就くことを控える。
4. 欧州データ保護監督官は、彼または彼女の任期を終えた後においても、任命及び収入を受諾したことに関して、誠実かつ慎重に行動する。

第 56 条 職業上の守秘義務

欧州データ保護監督官及び彼または彼女の職員は、彼または彼女の在任中及び彼らの任期を終えた後のいずれにおいても、彼らの公的な責務を遂行する過程において彼らが認知した全ての秘密情報に関して、職務上の守秘義務に服する。

第 57 条 職務

1. この規則の下で定められている他の職務を妨げることなく、欧州データ保護監督官は:
   (a) その司法上の権限において活動する司法裁判所による個人データの処理を除き、欧州連合の機関または組織によるこの規則の適用を監視し、かつ、それを執行する;
   (b) 処理と関連するリスク、法令、安全性確保措置及び権利について、公衆の意識及び理解を向上させる。特に、子ども向けの活動に格別の注意を払う;
   (c) この規則に基づく管理者及び処理者の義務について、管理者及び処理者の意識を向上させる;
   (d) 要請に応じて、この規則に基づく彼らの権利の行使に関し、いかなるデータ主体に対しても情報を提供し、また、それが適切であるときは、その目的のために、国内監督機関と協力する;
   (e) データ主体によって申立てられた異議、または、第 67 条に従い、組織、団体もしくは協会から申立てられた異議を取扱い、かつ、適切な範囲内で、異議申立てのあった事項について調査し、かつ、とりわけ、更に調査することまたは他の監督官と協力することが必要な場合、合理的な期間内に、異議申立人に対し、その調査の進捗状況及び結果を通知する;
   (f) 他の監督機関または他の行政機関から取得した情報に基づく場合を含め、この規則の適用に関する調査を行う;
   (g) 彼または彼女の発意により、または、要請に応じて、欧州連合の全ての機関及び組織に対し、個人データの処理と関連する自然人の権利及び自由の保護と関連する立法措置及び行政措置に関し、助言する;
   (h) 個人データの保護に対して影響をもつものである限り、関連する発展、とりわけ、情報通信技術の発展を監視する;
   (i) 第 29 条第 8 項及び第 48 条第 2 項の(c)に示す標準約款を採択する;
   (j) 第 39 条第 4 項によるデータ保護影響評価の要件に関するリストを策定し、維持管理する;
   (k) 欧州データ保護委員会の活動に参加する;
   (l) 規則(EU)2016/679 の第 75 条に従い、欧州データ保護委員会のための事務局を提供する;
   (m) 第 40 条第 2 項に示す処理に関し、助言を与える;
   (n) 第 48 条第 3 項に示す契約条項及び条項を承認する;

(o) この規則の違反行為の内部記録及び第 58 条第 2 項に従って講じられた措置に関する内部記録を保管する;
(p) 個人データの保護と関連する上記以外の職務を満たす;並びに、
(q) 彼または彼女の手続規則を策定する。

2. 欧州データ保護監督官は、他の連絡手段を排除することなく、電子的に完了させることもできる異議申立書の提出方式によって、第 1 項の(e)に示す異議の申立てを容易にする。
3. 欧州データ保護監督官の職務の遂行は、データ主体に関しては、無料とする。
4. 特にその反復的な特徴により、明らかに根拠のない場合または過剰なものである場合、欧州データ保護監督官は、要請された行動を拒否できる。欧州データ保護監督官は、その要請が明らかに根拠のないものであることまたは過剰な性質のものであることについて、説明をする責任を負う。

第 58 条 権限

1. 欧州データ保護監督官は、以下の調査権限をもつ:
   (a) 管理者及び処理者に対し、欧州データ保護監督官が彼または彼女の職務を遂行するために必要とする情報の提供を命ずること;
   (b) データ保護監査の方式により、調査を実施すること;
   (c) 管理者及び処理者に対し、主張されているこの規則の違反行為を連絡すること;
   (d) 管理者及び処理者から、その職務を遂行する上で必要とする全ての個人データ及び全ての情報へのアクセスを得ること;
   (e) 欧州連合法に従い、データ処理の装置及び手段へのアクセスを含め、管理者及び処理者の全ての施設へのアクセスを得ること。
2. 欧州データ保護監督官は、以下の是正権限をもつ:
   (a) 管理者または処理者に対し、予定されている処理業務がこの規則の条項に違反するおそれがあるとの警告を発すること;
   (b) 処理業務がこの規則の条項に違反した場合、管理者または処理者に対し、譴責を発すること;
   (c) 関係する管理者または処理者に対し、事項の照会をすること、及び、必要があるときは、欧州議会、理事会及び欧州委員会に対し、事項の照会をすること;
   (d) 管理者または処理者に対し、この規則による彼または彼女の権利を行使するためのデータ主体の要求に従うように命ずること;
   (e) 管理者または処理者に対し、それが適切であるとき、指定した態様により及び指定した期間内に、処理業務をこの規則の条項を遵守するものとさせることを命ずること;
   (f) 管理者に対し、個人データ侵害をデータ主体に連絡するように命ずること;
   (g) 処理の禁止を含め、一時的な制限または確定的な制限を加えること;
   (h) 第 18 条、第 19 条及び第 20 条により個人データの訂正もしくは削除または処理の制限を命ずること、並びに、第 19 条第 2 項及び第 21 条により個人データの開示を受けた取得者に対して、そのような行為の連絡をするよう命ずること;
   (i) 欧州連合の機関または組織による場合において、個々の事案の個別状況の相違に応じて、

本項の(d)ないし(h)及び(j)のいずれかの措置に加え、第 66 条による行政罰を科すこと;

(j) 構成国、第三国または国際機関の取得者に対するデータ移転の停止を命ずること。

3. 欧州データ保護監督官は、以下の承認の権限及び助言の権限をもつ:
   (a) データ主体に対し、彼らの権利の行使の際に助言すること;
   (b) 第 40 条に示す事前協議手続に従い、及び、第 41 条第 2 項に従い、管理者に対し、助言すること;
   (c) 彼もしくは彼女の発意により、または、要請に応じて、個人データの保護と関連する全ての問題に関し、欧州連合の機関及び組織並びに公衆に対して、意見書を発行すること;
   (d) 第 29 条第 8 項及び第 48 条第 2 項(c)に示す標準データ保護約款を採択すること;
   (e) 第 48 条第 3 項の(a)に示す契約条項を承認すること;
   (f) 第 48 条第 3 項の(b)に示す業務覚書を承認すること;
   (g) 第 40 条第 4 項に基づいて採択された実装行為による処理業務を承認すること。
4. 欧州データ保護監督官は、諸条約に定める条件に基づき、司法裁判所に対して事項の照会をする権限、及び、司法裁判所に提起された訴訟に関与する権限をもつ。
5. 本条によって欧州データ保護監督官に与えられた権限の行使は、効果的な司法救済及び適正手続を含め、欧州連合法に定める適切な安全性確保措置に服する。

第 59 条　問題に対応すべき管理者及び処理者の義務

欧州データ保護監督官が第 58 条第 2 項の(a)、(b)及び(c)に定める権限を行使する場合、関係する管理者または処理者は、それぞれの事案の諸事情を考慮に入れた上で、欧州データ保護監督官から指定された合理的な期間内に、欧州データ保護監督官に対し、その意見を通知する。該当するときは、欧州データ保護監督官の見解への返信の中において、その返答は、講じられた措置の記述も含める。

第 60 条　活動報告

1. 欧州データ保護監督官は、欧州議会、理事会及び欧州委員会に対し、彼または彼女の活動に関する年次報告書を送付し、かつ、それと同時に、その報告書を公表する。
2. 欧州データ保護監督官は、上記以外の欧州連合の機関及び組織に対し、第 1 項に示す報告書を転送する。それらの機関及び組織は、欧州議会におけるその報告書の検討があり得るという観点から、意見書を発することができる。

第 VII 章　協力及び一貫性

第 61 条　欧州データ保護監督官と国内監督機関との間の協力

欧州データ保護監督官は、それらの機関それぞれの職務を遂行するために必要な範囲内において、とりわけ、それぞれの機関の情報を相互に交換し、相互にその機関の権限の行使を要請し、または、それぞれの別の機関からの要請に応答することによって、国内監督機関及び理事会決定 2009/917/

JHA[1]の第 25 条に基づいて設置された共同監督機関と協力する。

第 62 条　欧州データ保護監督官及び国内監督機関による調整された監督

1. 欧州連合の法令が本条を参照する場合、欧州データ保護監督官及び国内監督機関は、それらの機関それぞれの職務権限の適用範囲内で行動し、大規模 IT システムの効果的な監督または欧州連合の組織、事務局及び部局の効果的な監督を確保するため、それらの機関の職責の枠組み内において積極的に協力する。
2. 欧州データ保護監督官及び国内監督機関は、必要に応じて、それらの機関それぞれの職務権限の範囲内において、及び、それらの機関の職責の枠組み内でそれぞれ活動し、関連情報を交換し、監査及び調査を実施する際に相互に補助し、この規則及びそれ以外の欧州連合法の解釈もしくは適用上の課題を検討し、独立の監督の実施上の問題またはデータ主体の権利の行使上の問題を研究し、問題解決するための整合性のある提案を策定し、そして、データ保護の権利の意識を向上させる。
3. 第 2 項に定める目的のために、欧州データ保護監督官及び国内監督機関は、欧州データ保護委員会の枠組み内において、少なくとも年 2 回、会合する。これらの目的のために、欧州データ保護委員会は、必要に応じて、更に別の作業手法を策定できる。
4. 欧州データ保護委員会は、欧州議会、理事会及び欧州委員会に対し、2 年毎に、調整された監督の共同報告書を送付する。

第 VIII 章　救済、責任及び制裁

第 63 条　欧州データ保護監督官に異議を申立てる権利

1. 司法上の救済、行政上の救済または非司法上の救済を妨げることなく、全てのデータ主体は、そのデータ主体が彼または彼女と関係する個人データの処理がこの規則に違反すると判断するときは、欧州データ保護監督官に異議を申立てる権利をもつ。
2. 欧州データ保護監督官は、その申立人に対し、第64条による司法救済が可能であることを含め、その異議の進捗状況及び結果を通知する。
3. 欧州データ保護監督官がその申立てを取扱わない場合、または、3 か月以内にデータ主体に対してその申立ての進捗状況もしくは結果を通知しない場合、欧州データ保護監督官が消極的な決定をしたものとみなされる。

第 64 条　効果的な司法救済を受ける権利

1. 司法裁判所は、損害賠償請求を含め、この規則の条項と関連する全ての紛争について、聴聞するための管轄権をもつ。
2. 第63 条第3 項に基づく決定を含め、欧州データ保護監督官の決定を不服とする訴訟は、司法裁

[1] 税関のための情報技術の利用に関する 2009 年 11 月 30 日の理事会決定 2009/917/JHA（OJ L 323, 10.12.2009, p.20）

判所において提起される。

3. 司法裁判所は、第 66 条に示す行政罰を見直すための無制限の管轄権をもつ。司法裁判所は、第 66 条の制限の範囲内において、それらの行政罰を取消し、減額し、または、増額できる。

第 65 条 損害賠償の権利

この規則の違反行為の結果として物的または非物的な損害を被った者は、諸条約に定める条件に従い、欧州連合の機関または組織から、その被った損害に対する賠償を受ける権利をもつ。

第 66 条 行政罰

1. 欧州データ保護監督官は、欧州連合の機関及び組織が第 58 条第 2 項の(d)ないし(h)及び(j)による欧州データ保護監督官からの命令を遵守しない場合、個々の案件の事情の相違に応じて、欧州連合の機関及び組織に対し、行政罰を加えることができる。個々の案件それぞれにおいて、行政罰を加えるべきか否か、及び、その行政罰の額を判断する際、以下の諸事項に適切に配慮する:
   (a) 関係する処理の性質、範囲及び目的を考慮に入れた上で、その違反行為の性質、重大性及び持続期間、並びに、その違反行為よって被害を受けたデータ主体の人数及び被った損害の程度;
   (b) データ主体が被った損失を軽減するために欧州連合の機関または組織によって講じられた措置;
   (c) 第 27 条及び第 33 条によりそれらの機関によって実装された技術上及び組織上の措置を考慮に入れた上で、欧州連合の機関または組織の責任の程度;
   (d) 欧州連合の機関または組織による従前の類似の違反行為;
   (e) 違反行為を解消し、違反行為による負の影響の拡大の可能性を削減するための、欧州データ保護監督官との協力の程度;
   (f) 違反行為によって影響を受けた個人データの類型;
   (g) その違反行為が欧州データ保護監督官の知るところとなった態様、とりわけ、欧州連合の機関または組織がその違反行為を連絡したか否か、及び、その場合には、どの範囲で連絡したのか;
   (h) その措置と同じ事項に関連して、従前に、関係する欧州連合の機関または組織に対して命ぜられた第 58 条に示す措置のいずれかの遵守。これらの罰を加えるための手続は、その案件の事情によって合理的な期間内に、かつ、第 69 条に示す関連訴訟及び訴訟手続を考慮に入れた上で、実施される。
2. 第 8 条、第 12 条、第 27 条ないし第 35 条、第 39 条、第 40 条、第 43 条、第 44 条及び第 45 条による欧州連合の機関または組織の義務の違反行為は、本条第 1 項に従い、各違反行為につき 25,000 ユーロ以下の行政罰、及び、年合計 250,000 ユーロ以下の行政罰とする。
3. 欧州連合の機関または組織の以下の条項の義務違反行為は、第 1 項に従い、各違反行為につき 50,000 ユーロ以下の行政罰、及び、年合計 500,000 ユーロ以下の行政罰とする:
   (a) 同意の条件を含め、第 4 条、第 5 条、第 7 条及び第 10 条による処理の基本原則;

(b) 第 14 条ないし第 24 条によるデータ主体の権利;
(c) 第 46 条ないし第 50 条による第三国または国際機関内の取得者に対する個人データの移転。

4. 欧州連合の機関または組織が、同じ処理業務または関連する処理業務または継続的な処理業務について、この規則の複数の条項に違反する場合、または、この規則の同じ条項に複数回違反する場合、その行政罰の総額は、その最も重大な違反行為について定められた金額を超過してはならない。
5. 本条による決定が行われる前に、欧州データ保護監督官は、欧州データ保護監督官によって行われた手続の対象である欧州連合の機関または組織に対し、欧州データ保護監督官が異議をとりあげた事柄に関して聴取を受ける機会を与える。欧州データ保護監督官は、関係する当事者が意見を述べることのできた異議のみをその決定の根拠とする。異議申立人は、その手続に緊密に関与する。
6. 関係する当事者の防御権は、その手続において、全面的に尊重される。その当事者の個人データ及び企業秘密の保護における個人または企業の正当な利益に従い、その当事者は、欧州データ保護監督官のファイルへアクセスする権利をもつ。
7. 本条の罰を加えることによって得られた資金は、欧州連合の一般予算の収入となる。

第 67 条 データ主体の代理者

データ主体は、欧州連合法または構成国法に従って適法に組織され、公共の利益に属する制定法上の目的を有し、かつ、その個人データの保護と関連するデータ主体の権利及び自由の保護の分野において活動する非営利の組織、団体または協会に対し、彼または彼女の代わりに欧州データ保護監督官に異議を申立てること、彼または彼女の代わりに第 63 条及び第 64 条に示す権利を行使すること、並びに、彼または彼女の代わりに第 65 条に示す損害賠償を受ける権利を行使することを委任する権利をもつ。

第 68 条 欧州連合の職員による不服申立

欧州連合の機関または組織によって雇用された者は、公式の経路を経ずに行動する場合を含め、この規則の条項の違反行為の主張に関し、欧州データ保護監督官に異議を申立てることができる。いかなる者も、そのような違反行為を主張して欧州データ保護監督官に異議を申立てたことのゆえに、不利益を受けるものとしてはならない。

第 69 条 制裁

それが彼または彼女の側において意図的なものであるか過失によるものであるかを問わず、欧州連合の官吏またはその他の公務員がこの規則に定める義務を遵守しない場合、関係する官吏またはその他の公務員は、職員規則に定める規定及び手続に従い、懲戒事由となる行為またはその他の行為について法的責任を負う。

第 IX 章 TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合の欧州連合の組織、事務局及び部局による運用個人データの処理

第 70 条 章の適用範囲

本章は、欧州連合のそのような組織、事務局または部局に対して適用される個別のデータ保護法令を妨げることなく、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合の欧州連合の組織、事務局及び部局による運用個人データの処理に対してのみ、適用される。

第 71 条 運用個人データの処理と関連する基本原則

1. 運用個人データは:
   (a) 適法かつ公正に処理される(「適法性及び公正性」);
   (b) 特定され、明示であり、かつ、正当な目的のために収集されるものとし、かつ、その目的に適合しないような別の目的のために処理してはならない(「目的による制限」);
   (c) 個人データが処理される目的との関係において、十分であり、関連性があり、かつ、過剰ではないこと(「データのミニマム化」);
   (d) 正確であり、かつ、それが必要なときは、最新のものに維持される;当該運用個人データが処理される目的を考慮した上で、遅滞なく、不正確な運用個人データが削除または訂正されることを確保するための全ての合理的な手立てが講じられなければならない(「正確性」);
   (e) その運用個人データが処理される目的のために必要な期間だけ、データ主体の識別を許容する方式を維持する(「記録保存の制限」);
   (f) 無権限の処理もしくは違法な処理に対して、並びに、事故による喪失、破壊または加害に対して、適切な技術上または組織上の措置を用いて行われる防護を含め、運用個人データの適切な安全性を確保する態様で処理される(「完全性及び機密性」)。
2. 運用個人データが収集される欧州連合の組織、事務局または部局以外の欧州連合の組織、事務局または部局を設置する法的行為の中に定める目的のいずれかのための同じ管理者または別の管理者による処理は、以下の場合には許容される:
   (a) 欧州連合法に従い、その管理者が、そのような目的のためのそのような運用個人データを処理するための承認を得ており;かつ、
   (b) 欧州連合法に従い、その処理が必要であり、かつ、当該他の目的と比例的である場合。
3. 同じまたは別の管理者による処理は、データ主体の権利及び自由のための適切な安全性確保措置に服し、欧州連合の組織、事務局または部局を設置する法的行為の中に定める目的のための、公共の利益におけるアーカイブ、科学調査上の使用または統計上の使用または歴史調査上の使用を含めることができる。
4. 管理者は、第 1 項、第 2 項及び第 3 項について職責を負い、かつ、それらの項の遵守を説明できなければならない。

第 72 条　運用個人データの処理の適法性

1. 運用個人データの処理は、その処理が、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合の欧州連合の組織、事務局及び部局によって実施される職務の遂行のために必要であり、かつ、欧州連合法に基づくものである場合に限り、その範囲内においてのみ、適法であるものとする。
2. 本章の適用範囲内にある処理を規律する欧州連合の個別の法的行為は、少なくとも、処理の対象、処理される運用個人データ、処理の目的、及び、その運用個人データの記録保存の期限、または、その運用個人データを更に記録保存するための必要性の定期的な見直しの期限を定めるものとする。

第 73 条　異なる類型のデータ主体の区別

管理者は、それが適用可能であり、かつ、それが可能な限り、欧州連合の組織、事務局及び部局を設置する法的行為の中に列挙する類型のような、異なる類型のデータ主体の運用個人データ間の明確な区分を設ける。

第 74 条　運用個人データの間の区別及び運用個人データの品質の確認

1. 管理者は、可能な限り、事実を基礎とする運用個人データと、個人の評価を基礎とする運用個人データとを区別する。
2. 管理者は、不正確、不完全または最新ではない運用個人データが送信され、または、利用可能とされないことを確保するための全ての合理的な手立てを講じる。この目的のために、管理者は、実施可能な限り、かつ、それが関連する場合、それらが送信され、または、利用可能とされる前に、例えば、そのデータの送信元である職務権限を有する機関と協議することにより、運用個人データの品質を確認する。管理者は、運用個人データの全ての送信に際し、可能な限り、運用個人データの正確性、完全性及び信頼性の程度を評価し、並びに、そのデータが更新されている範囲を取得者が評価できるようにするために必要となる情報を付加する。
3. 不正確な運用個人データが送信された場合、または、運用個人データが違法に送信された場合、取得者は、遅滞なく、その通知を受ける。そのような場合、その運用個人データは、訂正または削除され、または、第 82 条に従ってその処理が制限される。

第 75 条　個別の処理条件

1. 送信元である管理者に適用される欧州連合法が、処理のための個別の条件を定めている場合、その管理者は、その運用個人データの取得者に対し、それらの条件及びそれを遵守すべき義務を通知する。
2. 管理者は、指令(EU) 2016/680 の第 9 条第 3 項及び第 4 項に従い、送信元である職務権限を有する機関によって定められた個別の処理条件を遵守する。

第 76 条　特別の類型の運用個人データの処理

1. 人種的もしくは民族的な出自、政治的な意見、宗教上もしくは思想上の信条、または、労働組合への加入を明らかにする運用個人データの処理、並びに、自然人をユニークに識別することを目的とする遺伝子データ、生体データ、健康または自然人の性生活もしくは性的指向に関する運用個人データの処理は、業務遂行上の目的のために厳格に必要であり、関係する欧州連合の組織、事務局または部局の任務の範囲内であり、かつ、データ主体の権利及び自由のための適切な安全性確保措置に服する場合に限り、認められる。そのような個人データに基づく自然人に対する差別は、禁止される。
2. データ保護責任者は、不適切な遅滞なく、本条によることの通知を受ける。

第 77 条　プロファイリングを含め、個人の自動的な判定

1. 管理者が服すべき欧州連合法によって認められており、かつ、その欧州連合法がデータ主体の権利及び自由のための適切な安全性確保措置を定めている場合、少なくとも、管理者の側における人間の関与を得る権利を定めている場合を除き、プロファイリングを含め、自動的な処理のみを基礎とし、データ主体に関して不利な法的効果を発生させ、または、彼もしくは彼女に対して重大な影響を及ぼす判定は、禁止される。
2. 本条の第 1 項に示す判定は、データ主体の権利、自由及び正当な利益を防護するための適切な措置が設けられている場合を除き、第 76 条に示す特別類型の個人データを基礎としてはならない。
3. 第 76 条に示す特別類型の個人データを基礎として自然人に対する差別をもたらすプロファイリングは、欧州連合法に従い、禁止される。

第 78 条　データ主体の権利の行使のための連絡及び書式

1. 管理者は、第 79 条に示す全ての情報を提供するため、並びに、データ主体の個人データの処理に関する第 80 条ないし第 84 条及び第 92 条と関連する連絡を、明解で、理解しやすく、かつ、容易にアクセスし得る方式により、明瞭で平易な表現を用いるものとするための合理的な手立てを講ずる。その情報は、電子的な方法を含め、適切な方法によって提供される。管理者は、原則として、要求があったときは、同様の方式により、情報を提供する。
2. 管理者は、第 79 条ないし第 84 条に基づくデータ主体の権利の行使を容易にする。
3. 管理者は、データ主体に対し、彼または彼女の要求の事後対応に関し、不適切な遅滞なく、かつ、データ主体から要求を受領した時から遅くとも 3 か月以内に、書面により、通知する。
4. 管理者は、第 79 条に基づく情報及び第 80 条ないし第 84 条及び第 92 条に従って行われる連絡または講じられる措置を無料で提供する。管理者は、その要求が明らかに根拠のないもの、または、過剰なものであるという特徴を説明する責任を負う。
5. 管理者が、第 80 条または第 82 条に示す要求をしている自然人の同一性に関して合理的な疑いをもつ場合、その管理者は、そのデータ主体の同一性を確認するために必要となる追加情報の提供を要求できる。

第 79 条　データ主体に対して利用できるようにされ、または、与えられる情報

1. 管理者は、データ主体が少なくとも以下の情報を利用できるようにする：
   (a) 欧州連合の組織、事務局または部局の識別名及び連絡先；
   (b) データ保護責任者の連絡先；
   (c) 運用個人データが予定する処理の目的；
   (d) 欧州データ保護監督官に対して異議を述べる権利及び彼または彼女の連絡先；
   (e) 管理者に対し、運用個人データへのアクセス、その訂正または削除、及び、データ主体と関係する運用個人データの処理の制限を求める権利の存在。
2. 第 1 項に示す情報に加え、欧州連合法によって想定されている個々の場合において、管理者は、データ主体に対し、彼または彼女がその権利を行使することができるようにするための以下の情報を更に提供する：
   (a) 処理の法的根拠；
   (b) 運用個人データが記録保存される期間、または、それが可能でない場合、その期間を決定するために用いられる基準；
   (c) 該当するときは、第三国または国際機関を含め、運用個人データの取得者の類型；
   (d) 必要があるときは、とりわけ、データ主体が認識しない間に運用個人データが収集される場合、更に別の情報。
3. 管理者は、以下のために、関係する自然人の基本的な権利及び正当な利益に適切に配慮し、そのような措置が、民主主義社会において必要かつ比例的な措置を構成する範囲内において、かつ、その限りにおいて、第 2 項によるデータ主体に対する情報の提供を延期し、制限し、または、省略することができる：
   (a) 公的な照会もしくは法律上の照会、調査または手続の支障となることを避けるため；
   (b) 犯罪行為の防止、検知、捜査もしくは訴追または刑罰の執行の阻害となることを避けるため；
   (c) 構成国の公共の安全を防護するため；
   (d) 構成国の国家安全保障を防護するため；
   (e) 被害者及び証人のような、他の者の権利及び自由を保護するため。

第 80 条　データ主体によるアクセスの権利

データ主体は、彼または彼女に関する運用個人データが処理されているか否かに関する確認をその管理者から得る権利、並びに、その個人データが処理されている場合、その個人データ及び以下の情報へアクセスする権利をもつ：

(a) 処理の目的及び法的根拠；
(b) 関係する運用個人データの類型；
(c) 運用個人データが開示された取得者または取得者の類型、とりわけ、第三国または国際機関の取得者；
(d) 可能なときは、運用個人データが記録保存される予定期間、または、それが不可能なときは、その期間を決定するために用いられる基準；
(e) 運用個人データの訂正または削除及びデータ主体と関係する運用個人データの処理の制

限を管理者に対して求める権利の存在;
(f) 欧州データ保護監督官に対して異議を述べる権利及び彼または彼女の連絡先;
(g) 処理中の運用個人データの連絡、及び、その入手元に関する利用可能な情報。

第 81 条 アクセスの権利の制限

1. 管理者は、以下のために、関係する自然人の基本的な権利及び正当な利益に適切に配慮し、そのような全部または一部の制限が、民主主義社会において必要かつ比例的な措置を構成する範囲内において、かつ、その限りにおいて、データ主体のアクセスの権利の全部または一部を制限できる:
   (a) 公的な照会もしくは法律上の照会、調査または手続の支障となることを避けるため;
   (b) 犯罪行為の防止、検知、捜査もしくは訴追または刑罰の執行の阻害となることを避けるため;
   (c) 構成国の公共の安全を防護するため;
   (d) 構成国の国家安全保障を防護するため;
   (e) 被害者及び証人のような、他の者の権利及び自由を保護するため。
2. 第 1 項に示す場合において、管理者は、データ主体に対して、不適切な遅滞なく、書面により、アクセスの拒否または制限及びその拒否または制限の理由を通知する。それを提供することによって第 1 項の目的を損ねるおそれがある場合、その通知は、省略され得る。管理者は、データ主体に対し、欧州データ保護監督官に異議を申し立てることができること、または、司法裁判所において司法救済を求めることができることを通知する。当該情報は、要請に応じて、欧州データ保護監督官に対して利用できるようにされる。

第 82 条 運用個人データの訂正または削除の権利及び処理の制限

1. データ主体は、不適切な遅滞なく、彼または彼女に関する不正確な運用個人データの訂正をその管理者から得る権利をもつ。処理の目的を考慮に入れた上で、データ主体は、補足的な文言を提供する方法による場合を含め、不完全な運用個人データを完全なものとさせる権利をもつ。
2. 処理が、第 71 条、第 72 条第 1 項もしくは第 76 条に違反する場合、または、管理者が服すべき法律上の義務を遵守するために運用個人データが削除されなければならない場合、管理者は、不適切な遅滞なく、運用個人データを削除するものとし、また、データ主体は、不適切な遅滞なく、彼または彼女に関する運用個人データの削除をその管理者から得る権利をもつ。
3. 以下の場合、管理者は、削除の代わりに、処理を制限する:
   (a) その個人データの正確性がデータ主体によって争われており、かつ、その正確性または不正確性を確認できない場合;または、
   (b) その個人データが証拠の目的のために維持されなければならない場合。
   第 1 副項の(a)によって処理が制限される場合、その管理者は、その処理の制限を解除する前に、そのデータ主体に対して通知する。
   制限されたデータは、その削除を防止する目的のためにのみ、処理される。
4. 管理者は、データ主体に対し、書面により、運用個人データの削除または処理の制限の拒否及びその拒否の理由を通知する。管理者は、以下のために、関係する自然人の基本的な権利及び

正当な利益に適切に配慮し、そのような制限が、民主主義社会において必要かつ比例的な措置を構成する範囲内において、かつ、その限りにおいて、データ主体のアクセスの権利の全部または一部を制限できる:

(a) 公的な照会もしくは法律上の照会、調査または手続の支障となることを避けるため;
(b) 犯罪行為の防止、検知、捜査もしくは訴追または刑罰の執行の阻害となることを避けるため;
(c) 構成国の公共の安全を防護するため;
(d) 構成国の国家安全保障を防護するため;
(e) 被害者及び証人のような、他の者の権利及び自由を保護するため。

管理者は、データ主体に対し、欧州データ保護監督官に異議を申し立てることができること、または、司法裁判所において司法救済を求めることができることを通知する。

5. 管理者は、その不正確な運用個人データの入手元である職務権限を有する機関に対し、不正確な個人データの訂正を連絡する。
6. 管理者は、運用個人データが第 1 項、第 2 項及び第 3 項によって訂正され、削除され、または、その処理が制限された場合、取得者に対して連絡し、かつ、その取得者が、その取得者の責任において、当該運用個人データを訂正し、削除し、または、その処理を制限しなければならないことを通知する。

第 83 条 犯罪捜査及び刑事手続におけるアクセスの権利

運用個人データが職務権限を有する機関を入手元とする場合、欧州連合の組織、事務局及び部局は、データ主体のアクセスの権利に関して判断する前に、当該職務権限を有する機関の構成国内における犯罪捜査及び刑事手続の過程において処理された司法判断もしくは記録または事件ファイルの中にその個人データが含まれているか否かを確認する。それに該当する場合、アクセスの権利に関する判断は、関係する職務権限を有する機関との間の協議を経た上で、かつ、その職務権限を有する機関と緊密に協力して、行われる。

第 84 条 データ主体による権利の行使及び欧州データ保護監督官による確認

1. 第 79 条第 3 項、第 81 条及び第 82 条第 4 項に示す場合において、データ主体の権利は、欧州データ保護監督官を介して行使できる。
2. 管理者は、データ主体に対し、第 1 項により、欧州データ保護監督官を介して、彼または彼女の権利を行使できることを通知する。
3. 第 1 項に示す権利が行使される場合、欧州データ保護監督官は、少なくとも、彼または彼女によって必要な全ての確認が行われた旨をそのデータ主体に対して通知する。欧州データ保護監督官は、データ主体に対し、司法裁判所において司法救済を求める彼または彼女の権利を通知する。

第 85 条　バイデザイン及びバイデフォルトのデータ保護

1. 最新技術、実装費用、処理の性質、範囲、過程及び目的、並びに、処理によって示される自然人の権利及び自由に対する様々な発生確率と深刻度のリスクを考慮に入れた上で、管理者は、この規則の要件及びそれを定める法的行為に適合するため、並びに、データ主体の権利を保護するため、処理の方法を決定する時点及び処理それ自体の時点の両時点において、データのミニマム化のようなデータ保護の基本原則を効果的な態様で実装し、かつ、その処理の中に必要な安全性確保措置を統合するために設計された、仮名化のような、適切な技術上及び組織上の措置を実装する。
2. 管理者は、処理の目的との関係において十分であり、関連性があり、かつ、過剰ではない運用個人データのみが処理されることをデフォルトで確保する適切な技術上及び組織上の措置を実装する。この義務は、収集される運用個人データの分量、その処理の範囲、その記録保存の期間及びアクセシビリティに対して適用される。とりわけ、そのような措置は、デフォルトで、人間が関与することなく、不特定数の自然人に対して運用個人データがアクセス可能とされないことを確保する。

第 86 条　共同管理者

1. 複数の管理者が、または、欧州連合の機関及び組織以外の 1 もしくは複数の管理者と共に 1 または複数の管理者が処理の目的及び方法を決定する場合、それらの管理者は、共同管理者となる。それらの管理者は、共同管理者が服する欧州連合法または構成国法によって共同管理者それぞれの職責が定められていない限り、その範囲内において、それらの管理者間の覚書により、データ保護義務の遵守に関する、とりわけ、データ主体の権利の行使に関するそれらの管理者それぞれの職責を透明性のある態様で決定し、並びに、第 79 条に示す情報を提供すべきそれらの管理者それぞれの義務を決定する。その覚書は、データ主体のための連絡部局を指定できる。
2. 第 1 項に示す覚書は、共同管理者それぞれの役割、及び、共同管理者各自とデータ主体との間の関係を適正に反映するものとする。覚書の要旨は、データ主体が利用できるようにされる。
3. 第 1 項に示す覚書の条件に拘らず、データ主体は、個々の管理者との関係において、及び、個々の管理者を相手方として、この規則に基づく彼または彼女の権利を行使できる。

第 87 条　処理者

1. 管理者の代わりの者によって処理が実施される場合、その管理者は、この規則及び管理者を設置する法的行為の要件に処理が適合するような態様で適切な技術上及び組織上の措置を実装すること、並びに、データ主体の権利の保護を確保することについて十分な保証を提供する処理者のみを用いる。
2. 処理者は、管理者から、書面による個別的または一般的な事前承認を得ることなく、別の処理者を業務に従事させてはならない。書面による一般的な承認の場合、その処理者は、管理者に対し、別の処理者の追加または交代に関する変更予定を通知する。それによって、その管理者は、そ

のような変更に異議を述べる機会が与えられる。

3. 処理者による処理は、管理者との関係において処理者を拘束し、かつ、処理の対象及び期間、処理の性質及び目的、運用個人データの種類及びデータ主体の類型、並びに、管理者の義務及び権利を定める契約によって、または、それ以外の、欧州連合法もしくは構成国法に基づく法的行為によって規律される。契約またはそれ以外の法的行為は、とりわけ、処理者が以下のことを行うことを定める:
   (a) 管理者からの指示のみに基づいて行動すること;
   (b) 運用個人データの処理を承認された者が自ら守秘義務を課し、または、適切な法律上の守秘義務に服することを確保すること;
   (c) データ主体の権利に関する条項の遵守を確保するため、適切な方法によって管理者を補助すること;
   (d) 処理と関連するサービスの提供が終了した後、管理者の選択により、全ての運用個人データを消去し、または、その管理者に返還すること、及び、欧州連合法または構成国法が運用個人データの記録保存を要求する場合を除き、存在している複製物を削除すること;
   (e) 本条に定める義務の遵守を説明するために必要となる全ての情報を管理者が利用できるようにすること;
   (f) 他の処理者の業務従事に関し、第 2 項及び本項に示す条件を遵守すること。
4. 第 3 項に示す契約またはそれ以外の法的行為は、電子的な方式を含め、書面によるものとする。
5. 処理の目的及び方法を定めることによって処理者がこの規則にまたは管理者を設置する法的行為に違反する場合、その処理者は、当該処理との関係においては、管理者とみなされる。

第 88 条 ログ(履歴)

1. 管理者は、自動的な処理システムにおける、以下の全ての処理業務に関する履歴(ログ)を保管する:すなわち、運用個人データの収集、修正、参照、移転を含め開示、結合及び削除である。参照及び開示の履歴は、そのような業務遂行の正当化事由、日時、並びに、運用個人データを参照した者または開示を受けた者の識別名、及び、そのような運用個人データの取得者の識別名を可能な限り確定できるようにする。
2. 履歴は、処理の適法性の検証、自己監視、運用個人データの完全性及び安全性の確保のため、並びに、刑事手続のためにのみ使用される。そのような履歴は、現在進行中の管理のために必要なものでない限り、3 年後に削除される。
3. 管理者は、要請に応じて、データ保護責任者及び欧州データ保護監督官に対し、その履歴を利用できるようにする。

第 89 条 データ保護影響評価

1. 処理の性質、範囲、過程及び目的を考慮に入れた上で、ある種類の処理、特に新たな技術を用いる処理が、自然人の権利及び自由に対して高度なリスクをもたらすおそれがある場合、管理者は、処理を開始する前に、運用個人データの保護に対する予定された処理業務の影響の評価を実施する。

2. 第1項に示す評価は、少なくとも、予定された処理業務の一般的な記述、データ主体の権利及び自由に対するリスクの評価、それらのリスクに対応するために予定された措置、並びに、データ主体及びそれ以外の関係者の権利及び正当な利益を考慮に入れた上で、運用個人データの保護を確保するため、及び、データ保護法の遵守を説明するための安全性確保措置、防護措置及び仕組みを含める。

第 90 条 欧州データ保護監督官の事前協議

1. 以下の場合、新たに編成されるファイリングシステムの一部を構成する処理を行う前に、管理者は、欧州データ保護監督官と協議する:
   (a) 第 89 に基づくデータ保護影響評価の結果が、リスクを削減するために管理者によって講じられる措置が欠けていると、その処理が高度のリスクをもたらすおそれがあることを示す場合;または、
   (b) その種類の処理が、とりわけ、新しい技術、仕組みまたは手順を用いる場合、データ主体の権利及び自由に対する高度のリスクを含んでいる場合。
2. 欧州データ保護監督官は、第 1 項による事前協議の対象となる処理業務のリストを作成できる。
3. 管理者は、欧州データ保護監督官に対し、第 89 条に示すデータ保護影響評価を提供し、また、その要求に応じて、欧州データ保護監督官が、処理の法令遵守について評価し、とりわけ、データ主体の運用個人データの保護に対するリスク及び関連する安全性確保措置を評価できるようにするために、上記以外の情報を提供する。
4. 欧州データ保護監督官が、本条の第 1 項に示す予定された処理がこの規則または欧州連合の組織、事務局もしくは部局を設置する法的行為に違反するとの意見をもつ場合、とりわけ、管理者がそのリスクの特定及び削減を十分にしていない場合、欧州データ保護監督官は、協議の要請を受けた時から 6 週間以内に、その管理者に対し、書面による助言を提示する。この期限は、予定された処理の複雑性を考慮に入れた上で、1 か月まで延長され得る。欧州データ保護監督官は、管理者に対し、協議の要請を受けた時から 1 か月以内に、その遅延の理由と共に、その期限の延長を通知する。

第 91 条 運用個人データの処理の安全性

1. 管理者及び処理者は、最新技術、実装費用、処理の性質、範囲、過程及び目的並びに自然人の権利及び自由に対する様々な発生確率と深刻度のリスクを考慮に入れた上で、そのリスクに適切に対応する一定のレベルの安全性を確保するため、とりわけ、特別類型の運用個人データの処理に関して、適切な技術上及び組織上の措置を実装する。
2. 自動的な処理に関し、管理者及び処理者は、リスク評価の後、以下のとおり設計された措置を実装する:
   (a) 処理のために使用されるデータ処理装置への無権限の者のアクセスの拒否(「装置アクセス管理」);
   (b) データ媒体の無権限の閲読、複製、改変または除去の防止(「データ媒体管理」);
   (c) 運用個人データの無権限の入力、及び、記録保存された運用個人データの無権限の調査、

改変または削除の防止(「記録保存管理」);

(d) データ通信装置を用いて行われる無権限の者による自動的な処理システムの利用の防止(「利用者管理」);

(e) 自動的な処理システムの利用を承認された者が、そのアクセス承認を受けた範囲内にある運用個人データに対してのみアクセスをもつことの確保(「データアクセス管理」);

(f) データ通信装置を用いて、どの組織に対して運用個人データが送信されたか、送信されたかもしれないか、または、利用可能とされたかを検証し、確定できることの確保(「通信管理」);

(g) どの運用個人データが自動的な処理システムに入力されたのか、及び、いつ誰によってそのデータが入力されたのかを事後的に検証し、確定できることの確保(「入力管理」);

(h) 運用個人データの移転中またはデータ媒体の輸送中における運用個人データの無権限の閲読、複製、改変または削除の防止(「輸送管理」);

(i) 侵害があった場合において、設置されたシステムが復元されることの確保(「復旧」);

(j) システムの機能が発揮されること、機能の異常の発生が報告されることの(「信頼性」)、及び、記録保存された運用個人データがシステムの不正操作によって損なわれ得ないことの確保(「完全性」)。

第 92 条 欧州データ保護監督官に対する個人データ侵害の通報

1. 個人データ侵害が発生した場合、その個人データ侵害が自然人の権利及び自由に対するリスクをもたらすおそれがない場合を除き、管理者は、不適切な遅滞なく、かつ、実施可能であるときは、その侵害に気づいた時から遅くとも 72 時間以内に、欧州データ保護監督官に対し、その個人データ侵害を連絡する。欧州データ保護監督官に対する連絡が 72 時間以内に行われない場合、その連絡には遅延の理由を付す。
2. 第 1 項に示す連絡は、少なくとも:
   (a) それが可能であるときは、関係するデータ主体の類型及び概数、並びに、関係する運用個人データ記録の類型及び概数を含め、その個人データ侵害の性質を記述し;
   (b) データ保護責任者の名前及び連絡先を連絡し;
   (c) その個人データ侵害の予想される結果を記述し;
   (d) それが適切なときは、それによって発生し得る負の影響の拡大を削減するための措置を含め、その個人データ侵害に対処するために管理者によって講じられた措置または講ずる準備のされた措置を記述する。
3. 第 2 項に示す情報を同時に提供できない場合、その限りにおいて、その情報は、更に不適切に遅滞することなく、その状況に応じて提供され得る。
4. 管理者は、第 1 項に示す全ての個人データ侵害について、その個人データ侵害に関する事実関係、その影響及び復旧措置を含め、文書化する。その文書は、本条の遵守を検証するため、欧州データ保護監督官が利用できるものとされる。
5. その個人データ侵害が、他の管理者から送付された運用個人データ、または、他の管理者に対して送付された運用個人データを含む場合、管理者は、関係する職務権限を有する機関に対し、不適切な遅滞なく、第 2 項に示す情報を連絡する。

第 93 条　データ主体に対する個人データ侵害の連絡

1. 個人データ侵害が自然人の権利及び自由に対する高度なリスクを発生させるおそれがある場合、管理者は、そのデータ主体に対し、不適切な遅滞なく、その個人データ侵害を連絡する。
2. 本条の第 1 項に示すデータ主体への連絡は、明確かつ平易な文言により、その個人データ侵害の性質を記述し、かつ、少なくとも、第 92 条第 2 項の(b)、(c)及び(d)に定める情報及び勧告を含める。
3. 以下の条件に該当する場合、第 1 項に示すデータ主体に対する連絡を要しない：
   (a) 管理者が適切な技術上及び組織上の防護措置を実装し、かつ、それらの措置、とりわけ、暗号のような、承認を受けていない者にとってその運用個人データを知覚不可能なものとする措置が、個人データ侵害によって害を受けた運用個人データに適用された場合；
   (b) 管理者が、第 1 項に示すデータ主体の権利及び自由に対する高度なリスクが現実化するおそれがないことを確保する事後的な措置を講じた場合；
   (c) それが過大な負担を要するような場合。そのような場合、データ主体が平等に効果的な方法で情報伝達される公衆通信またはそれに類する手段によって代えられる。
4. 管理者がデータ主体に対して個人データ侵害をまだ連絡していない場合、欧州データ保護監督官は、その個人データ侵害が高度なリスクを発生させるおそれについて検討した上で、その管理者に対し、そのようにすべきことを要求することができ、または、第 3 項に示す条件のいずれかの該当を判断できる。
5. 本条の第 1 項に示すデータ主体への連絡は、第 79 条第 3 項に示す条件及び根拠により、延期し、制限し、または、省略できる。

第 94 条　第三国及び国際機関に対する運用個人データの移転

1. 欧州連合の組織、事務局または部局を設置する法的行為の中で定める制限及び条件に従い、管理者は、その移転が管理者の職務の遂行のために必要であり、かつ、本条に定める条件、すなわち、以下に適合する場合に限り、第三国の機関または国際機関に対し、運用個人データを移転できる：
   (a) 欧州委員会が、指令(EU) 2016/680 の第 36 条第 3 項に従い、当の第三国または当該第三国の地域もしくは処理部門または国際機関が十分なレベルの保護を確保していると判定する十分性の判定を採択した場合；
   (b) (a)に基づく欧州委員会の十分性の判定がない場合、欧州連合と当該第三国または国際機関との間において、プライバシー及び基本的な権利並びに個人の自由の保護に関する十分な安全性確保措置を掲げる TFEU 第 218 条による国際協定が締結された場合；
   (c) (a)に基づく欧州委員会の十分性の判定または(b)に基づく国際協定がない場合、欧州連合の組織、事務局または部局と当の第三国との間において、欧州連合の関係する組織、事務局または部局を設置する法的行為の適用の日よりも前に、運用個人データの交換を認める協力協定が締結されていた場合。
2. 欧州連合の組織、事務局及び部局を設置する法的行為は、運用個人データの国際移転のための条件に関し、とりわけ、適切な安全性確保措置及び特定の状況のための例外の方法による移

転に関し、より細目的な条項を維持または導入できる。

3. 管理者は、第 1 項(a)に示す十分性の判定、協定、行政上の覚書、及び、第 1 項に従う運用個人データの移転と関連するその他の法律文書のリストをその管理者の Web サイト上で公表し、かつ、それを最新の状態に保つ。
4. 管理者は、本条によって行われた全ての移転の詳細な記録を保管する。

第 95 条 刑事上の捜査及び刑事手続の秘密

TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する欧州連合の組織、事務局または部局を設置する法的行為は、欧州データ保護監督官に対し、彼または彼女の監督権限の行使において、欧州連合法または構成国法に従い、刑事上の捜査及び刑事手続の秘密を最大限考慮に入れることを義務付け得る。

第 X 章 実装行為

第 96 条 委員会の手続

1. 欧州委員会は、規則(EU) 2016/679 の第 93 条によって設置される委員会から補佐を受ける。その委員会は、規則(EU) No 182/2011 の意味における委員会となる。
2. 本項への参照がある場合、規則(EU) No 182/2011 の第 5 条が適用される。

第 XI 章 見直し

第 97 条 見直しの条項

遅くとも 2022 年 4 月 30 日以前に、かつ、その後は 5 年毎に、欧州委員会は、欧州議会及び理事会に対し、それが必要なときは、適切な立法提案書を添えて、この規則の適用に関する報告書を提出する。

第 98 条 欧州連合の法的行為の見直し

1. 欧州委員会は、2022 年 4 月 30 日までに、以下のために、諸条約に基づいて採択され、TFEU の第 III 部第 V 款の第 4 章及び第 5 章の適用範囲内にある活動を実施する場合の欧州連合の組織、事務局または部局による運用個人データの処理を規律する法的行為を見直す:
   (a) 指令(EU) 2016/680 及びこの規則の第 IX 章との一貫性の評価;
   (b) 同分野の活動を実施する場合の欧州連合の組織、事務局または部局と職務権限を有する機関との間の運用個人データの交換を妨げ得る相違点の指摘; 並びに、
   (c) 欧州連合内におけるデータ保護立法の法的断片化をつくり出し得る相違点の指摘。
2. 欧州委員会は、その評価を基礎として、処理と関連する自然人の統一的かつ一貫性のある保護を確保するため、とりわけ、この規則の第 IX 章を Europol 及び欧州検事局に適用するため、及

び、それが必要なときは、この規則の第 IX 章の修正を含めるため、適切な立法提案書を送付できる。

第 XII 章　最終条項

第 99 条　規則(EC) No 45/2001 及び決定 No 1247/2002/EC の廃止

規則(EC) No 45/2001 及び決定 No 1247/2002/EC は、2018 年 12 月 11 日に発効するものとして、廃止される。廃止される規則及び指令に対する参照は、この規則に対する参照として解釈される。

第 100 条　移行措置

1. 欧州議会及び理事会の決定 2014/886/EU[1]及び欧州データ保護監督官及び副監督官の現在の任期は、この規則により影響を受けない。
2. 副監督官は、報酬、手当、退職年金及びそれ以外の報酬の代価としての収入は、司法裁判所の事務局長と均等のものとみなされる。
3. この規則の第 53 条の第 4 項、第 5 項及び第 7 項並びに第 55 条及び第 56 条は、彼の任期終了まで、現在の副監督官に対して適用される。
4. 副監督官は、2019 年 12 月 5 日の彼の任期終了まで、欧州データ保護監督官の職務について、欧州データ保護監督官を補佐し、かつ、欧州データ保護監督官を補佐が不在の場合またはその職務の遂行に支障がある場合には、その代行者として活動する。

第 101 条　発効及び適用

1. この規則は、EU 官報上において公示された翌日から 20 日目に発効する。
2. ただし、この規則は、Eurojust による個人データの処理に対しては、2019 年 12 月 22 日から適用される。

この規則は、その全部について拘束力があり、かつ、全ての構成国において直接に適用される。

2018 年 10 月 23 日にストラスブールにおいて行われた。

欧州議会として	理事会として
議長　A. Tajani	議長　K. Edtstadler

[1] データ保護監督官及び副監督官を任命する欧州議会及び理事会の 2014 年 12 月 4 日の決定 2014/886/EU（OJ L 351, 9.12.2014, p.9）