ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 6 巻第 6 号（通巻第 46 号・2021 年 12 月）

法と情報研究会　編

（第 2 分冊）

本 号 目 次

規則(EU) 2021/784
[参考訳]

2021 年 12 月 5 日
明治大学法学部教授
夏 井 高 人

＊＊＊

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online（OJ L 172, 17.5.2021, p. 79-109）のテキスト（英語版）に基づき，その和訳を試みた。

規則(EU) 2021/784 の原文のテキストを入手できるサイトの URL は，下記のとおりである。

http://data.europa.eu/eli/reg/2021/784/oj
[2021 年 11 月 26 日確認]

規則(EU) 2021/784 は，2021 年 4 月 29 日に採択され，2021 年 6 月 6 日に発効した。規則(EU) 2021/784 は，2022 年 6 月 7 日から適用される。

―解　説―

1．規則(EU) 2021/784

規則(EU) 2021/784 は，オンラインのテロリストコンテント（terrorist content）の伝達（dissemination）の防止を実効的に実施するための EU の保安行政上の基本的な方策を定める法令である。その方策の中には，テロリストコンテントの伝達の媒体となり得るホスティングサービスプロバイダ等が行うべき様々な対応策とその行政監督も含まれている。

テロリストコンテントに対する刑事法上の対応，特にその処罰に関しては，指令(EU) 2017/541（OJ L 88, 31.3.2017, p.6-21）が適用される。

テロリスト行為（terrorist offence）と関連する構成国の法執行機関等の間における情報交換に関しては，理事会決定 2005/671/JHA（OJ L 253, 29.9.2005, p.22-24）が適用される。VIS に対するテロリスト情報の照会に関しては，理事会決定 2008/633/JHA（OJ L 218, 13.8.2008, p.129-136）が適用される。

規則(EU) 2021/784 の前文は，かなりの分量を費やし，具体例をあげながら，規則(EU) 2021/784 の適用対象となる通信に関して詳細な説明をしている。これは，テロリストコンテントが，物的属性により一律に識別可能なものではなく，一定の価値判断を基礎とし，文脈理解を必須の要素とする意味論上の属性決定を経ることを要するものであることから，自動的に，表現の自由及び思想信条の自由と関係する問題を生じやすいからである。

また，そのようなコンテントを識別して削除またはアクセス不能にする義務等のプロバイダに課される義務は，単にプロバイダの負担を増加させるというだけではなく，様々な側面においてプロバイダの企業活動の自由に対する一定の制限を加えることともなり得る。この点に関し，規則(EU) 2021/784 の前文は，当該プロバイダが当該テロリストコンテントに対して何らの対処もしないことから生ずる社会的な被害や当該プロバイダに対する信頼の喪失という不利益等との比較考量によって，企業活動の自由に対する一定の制限がやむを得ないものであるという価値判断を提示していると理解することが可能である。当然のことながら，テロ行為によって民主主義及び自由主義の社会という政治体制が破壊されてしまうと，企業活動の自由の存立基盤が喪失することとなる結果，企業活動の自由も自動的に消滅する。

それゆえ，以上の諸点に関し，現実の法執行を想定した上で，事前に関連する運用指針（guidelines）を盛り込むという趣旨を含め，その識別基準に関する詳細な記述が起草され，前文中に含められたものと推測される。

規則(EU) 2021/784 は，デジタルサービス規則案（COM/2020/825 final）及び規則(EU) 2021/1232（OJ L 274, 30.7.2021, p. 41-51）と相互に密接な関係をもつ法令の 1 つである。それゆえ，規則(EU) 2021/784 を正確に理解するためには，デジタルサービス規則案（COM/2020/825 final）及び規則(EU) 2021/1232 も一緒に精読・理解する必要性がある。

規則(EU) 2021/784 の適用対象となるテロリストコンテントは，デジタルサービス規則案（COM/2020/825 final）に定める違法なコンテント（illegal content）の主要類型の 1 つである。そして，テロリストコンテントの伝達のための潜在的な中間介在者（intermediaries）となり得る「ホスティングサービスプロバイダ（hosting service providers）」，及び，インターネットサービスプロバイダ（ISPs）のことを意味する「情報社会サービスのプロバイダ（providers of information society services）」の概念に関しては，デジタルサービス規則案（COM/2020/825 final）の定義条項及び前文内の記述を精読・理解し，それらの概念の定義を正確に把握した上で，規則(EU) 2021/784 の中におけるその意義と機能を理解すべきである。

規則(EU) 2021/784 は，テロリストコンテントとして判断され，削除されるコンテント及び関連データに関し，一定の保全義務及び保全命令を定めている（第 6 条参照）。

その義務は，その判断が誤りである場合に，不服申立てのあった関連行政機関の判断または裁判所の判断に従って当のプロバイダが当該コンテントを回復するため，そして，捜査機関がテロリスト行為及びその関係者を捜査するために証拠として利用するために設けられている。

従来，EU においては，テロリスト行為に対する犯罪捜査の目的のためであっても，捜査機関による利用のためのデータ保全（preservation）またはデータ保持（retention）に関しては，消極的な見解が多かった。しかし，規則(EU) 2021/784 が採択され，テロリスト行為に対抗するための犯罪捜査目的によるデータ保全義務が導入されることになった背景事情としては，欧州内において，テロリスト行為が現実かつ継続的に発生しているという事実によることが大きいと思われる。それらの殺傷事件は，様々な情報媒体を通じて報道され続けている。テロリ

スト行為による生命及び身体の安全に対する脅威またはリスクは，欧州における日常的な現実の一部となっている。

規則(EU) 2021/784 の前文は，誤ってオンラインコンテントが削除され，または，アクセス不能にされた場合において，裁判所において不服申立てできることが（表現の自由等の基本的な権利を守るための）安全確保（safeguards）の重要な一部を構成するという位置づけを示している。

このことは，日本国の法制を前提にする限り，なかなか理解しにくいものかもしれない。なぜならば，日本国においては法律によって訴権（訴訟を提起する権利）が定められていなくても，何らかの法益侵害があれば，例えば，民法第 709 条に基づき損害賠償請求訴訟を提起できるからである。行政訴訟の場合であっても，個別の訴権が定められていなくても，一般的な要件に該当し得る場合には，当該行政行為の取消訴訟を提起し得る。

しかし，欧州においては，法律によって実体的な権利及び訴権（訴訟を提起する権利）が定められていなければ訴訟を提起し，裁判所において救済を求めることができないという法制をもつ国が一般的である。

それゆえ，規則(EU) 2021/784 において，法務当局（EU の構成国の裁判所及び関連行政機関）に対して不服申立てできる権利を明確に定めていることが安全確保の一種となるのである。

日本国の標準的な大学レベルの法学教育を受けただけの者が EU 法を理解する際の困難の 1 つは，このような場面においても存在する。

規則(EU) 2021/784 は，欧州連合内に物理的に存在していないプロバイダに対しても適用される。その結果，欧州連合内に拠点をもたない第三国のプロバイダに対しても規則(EU) 2021/784 が適用される。その結果，同規則の適用を受ける第三国のプロバイダは，同規則に基づく様々な義務を負うことになる。そのような第三国のプロバイダの中には日本国に主たる拠点のあるプロバイダも含まれる。

そのような第三国のプロバイダに適用される裁判管轄権（当該構成国の国家主権の及ぶ地理的範囲）に関しては，やや面倒な問題があることは否定できない。この点に関しては，規則(EU) 2021/784 の前文(43)の中で述べられている。また，このような場合における裁判管轄権と密接な関連性をもつ「実質的な接続（substantial connection）」の概念の意義に関しては，規則(EU) 2021/784 の前文(15)及び前文(16)にその説明がある。なお，デジタルサービス規則案（COM/2020/825 final）の前文(7)及び前文(8)にもほぼ同趣旨の説明がある。

2. 参考訳作成における基本方針

この参考訳においては，規則(EU) 2021/784 の前文，条文及び別紙（ANNEX）の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし，原文を表示することが無

意味な部分（特に脚注内）に関しては，原文または訳文の表示を省略した。なお，従来，別紙（ANNEX）に関しては，読みやすさを重視し，原則として，原文の表示を割愛したが，規則(EU) 2021/784 の別紙が非常に重要なものであることに鑑み，読みやすさを犠牲にして，対訳方式によることにした。

この参考訳は，あくまでも規則(EU) 2021/784 の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。

読みやすさを重視し，条文中の号(point)の表記を一部省略した。例えば，「point(a)」は「第(a)号」であるが，「第」と「号」を省略し，「(a)」と表記することにした。

この参考訳は，Eur-lex のデータ二次利用条件を遵守して作成した。

3. 参考訳作成において留意した事項

第 2 条第 7 号柱書の表現は，屋上屋を重ねるような表現であり，そのような表現を採用することの合理性も特に認められない。これは，立法上のミスによる誤記の一種であると判断した。しかし，この参考訳においては，原文のまま訳すことにした。

別紙 I（ANNEX I）の冒頭に位置する枠内にある「access to which as been disabled」との箇所は，明らかに，「access to which has been disabled」の誤記である。これは，立法上のミスによるものと推測される。この参考訳は，そのように解した上で訳出することにした。

4. 訳語に関する補足的説明

Material

規則(EU) 2021/784 においては，「material」は，テロリストコンテントに該当し得る対象となるコンテント等の存在形態（主としてデジタルデータ）のことを意味する趣旨で用いられている。コンテントを作成するための「素材」を意味するわけではない。オンラインの「material」が存在

する場合，その「material」がテロリストコンテントであるかどうかは，当該「material」の属性評価によって決定されることである。

このような意味での「material」は，様々な訳語を考えることが可能であるが，この参考訳においては，有体物である場合とデジタルデータのような電磁的な状態である場合，更に，音響（音声）や映像そのものである場合を含める趣旨で，「material」を「対象物」と訳すことにした。

Statement of reasons

一般に，「statement of reasons」は，「説明書」と訳し得る。しかし，規則(EU) 2021/784 の中では，本体である命令書の一部として「statement of reasons」を提供することが想定されている。そこで，この参考訳においては，「statement of reasons」を「理由の説明」と訳すことにした。

Judicial redress

「judicial redress」は，裁判所による命令の取消しの場合を含むものであるが，各構成国の法制の相違により，行政不服審査のような行政機関による判定も当然に含むものである。それゆえ，この参考訳においては，裁判所による判断に基づく救済と行政機関による判断に基づく救済の両者を含む趣旨で，「judicial redress」を法務上の救済と訳すことにした。

なお，EU の構成国における「法務」の概念に関しては，後述の参考訳の各冒頭部分で述べたとおりであるが，規則(EU) 2021/784 の前文(35)の第 2 文の中にある「whether they are administrative, law enforcement or judicial」との表現を考えてみれば，日本国憲法の下にある国家体制を前提にして，「行政機関」と「司法機関」を区分するという考え方だけでは正確な理解が不可能であることを知ることができる。

Trust

「trust」は，「信頼」である。法律用語としての「信用」は，決済や電子商取引と関係する分野における予約語の一種であるので，これらの分野と関係をもつ法令においては，混乱を避けるため，「trust」を「信用」と訳してはならない。このことは，実質的には素人である者を除き，法律専門家であれば誰でも熟知していることである。

個人データ保護，個人識別，サービスプロバイダの業務及び責任免除等を含め，サイバー法及び情報法と関連する分野においては，決済や電子商取引と無関係であることは滅多になく，特に，EU のデジタル単一市場に関して適用される法令ではそうである。

それゆえ，この参考訳においては，原則として，「trust」を「信頼」と訳すことにした。

Disable access

規則(EU) 2021/784 の前文中では，文脈上全く同じことを意味しているはずであるのにも拘

らず，「disable access」と表現している箇所と単に「disable」等と表現している箇所とがある。後者は，立法上のミスの可能性もないではないが，省略表現の一種であると解した。

以上を踏まえた上で，この参考訳においては，いずれの表現の場合においても，「アクセス不能化」またはこれと類似の表現で訳出することにした。

Identification

一般に，「identification」は，文脈により，様々な意味をもつ。規則(EU) 2021/784 においては，職務権限のある機関の「identification」は，「識別名」（名称，略称，参照番号等）を意味し，削除命令の中で指示されるテロリストコンテントをプロバイダが特定するという文脈においては，「identification」は，「識別同定」を意味し，プロバイダが自発的にテロリストコンテントを特定するという文脈においては，「identification」は，「発見」を意味する。そのプロバイダの利用者または第三者がテロリストコンテントを見つけ，そのプロバイダまたは関係当局に通報するという文脈においても，「identification」は，「発見」を意味する。

以上を踏まえた上で，この参考訳においては，適宜，訳し分けることにした。

以上のほかは，後掲デジタルサービス規則案（COM/2020/825 final）の参考訳，後掲規則(EU) 2021/1232 の参考訳，後掲規則(EU) 2020/ 1783 の参考訳，後掲規則(EU) 2020/1784 の参考訳，後掲規則(EU) 2021/693 の参考訳，後掲規則(EU) 2021/694 の参考訳，後掲理事会決議(2020/C 342 I/01)の参考訳，後掲 e-Justice 決議 2008/2125 の参考訳，後掲電子識別規則(EU) No 910/2014 の参考訳，後掲人工知能規則案（COM/2021/206 final）の参考訳及び後掲 e-CODEX 規則案の参考訳の各冒頭部分で述べたとおりである。

5. 関連参考訳及び参考文献

指令(EU) 2017/541 の参考訳は，法と情報雑誌 2 巻 8 号 1～29 頁にある。理事会決定 2005/671/JHA の参考訳は，法と情報雑誌 2 巻 8 号 30～40 頁にある。理事会決定 2008/633/JHA の参考訳は，法と情報雑誌 2 巻 8 号 48～66 頁にある。ジオブロッキング規則(EU) 2018/302 の参考訳は，法と情報雑誌 4 巻 5 号 119～142 頁にある。

デジタルサービス規則案（COM/2020/825 final）の参考訳は，法と情報雑誌 6 巻 6 号 1～217 頁にある。規則(EU) 2021/1232 の参考訳は，法と情報雑誌 6 巻 6 号 219～255 頁にある。欧州電子通信法指令(EU) 2018/1972 の参考訳は，法と情報雑誌 4 巻 2 号 1～212 頁にある。指令 2002/21/EC（枠組み指令）の参考訳は，法と情報雑誌 3 巻 7 号 76～108 頁にある。指令 2009/140/EC による改正後の指令 2002/21/EC の参考訳は，法と情報雑誌 3 巻 9 号 31～58 頁にある。電子識別規則(EU) No 910/2014 の参考訳は，法と情報雑誌 2 巻 10 号 147～196 頁にある。規則(EU) 2018/1241 による改正後の Europol 規則(EU) 2016/794 の参考訳は，法と情報雑誌 4 巻 4 号 8～68 頁にある。電子商取引指令 2000/31/EC の参考訳は，法と情報雑誌 3 巻 1 号 110～141 頁にある。視聴覚メディアサービス指令 2010/13/EU の参考訳は，法と情報雑誌 2 巻 12 号 24～72 頁にある。

規則(EU) 2018/1725 の参考訳は，法と情報雑誌 4 巻 1 号 1～81 頁にある。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。規則(EU) 2016/679（一般データ保護規則）の参考訳・再訂版は，法と情報雑誌 3 巻 5 号 1～114 頁にある。指令(EU) 2016/680 の参考訳・改訂版は，法と情報雑誌 6 巻 6 号 339～466 頁にある。

規則(EU) 2020/1783 の参考訳は，法と情報雑誌 6 巻 5 号 1～81 頁にある。規則(EU) 2020/1784 の参考訳は，法と情報雑誌 6 巻 5 号 82～159 頁にある。規則(EU) 2021/693 の参考訳は，法と情報雑誌 6 巻 4 号 440～486 頁にある。規則(EU) 2021/694 の参考訳は，法と情報雑誌 6 巻 1 号 1～104 頁にある。理事会決議(2020/C 342 I/01)の参考訳は，法と情報雑誌 6 巻 4 号 513～537 頁にある。e-Justice 決議 2008/2125 の参考訳は，法と情報雑誌 6 巻 4 号 487～512 頁にある。人工知能規則案（COM/2021/206 final）の参考訳は，法と情報雑誌 6 巻 5 号 320～562 頁にある。e-CODEX 規則案の参考訳は，法と情報雑誌 6 巻 5 号 233～319 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。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。

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。

この参考訳を作成するに際し，濱野恵「オンラインのテロ関連コンテンツ削除を義務付ける規則の公布」外国の立法 288-1 号 12～13 頁を参考にした。

この参考訳は，科学研究費補助金基盤研究(B)（19KT0014）及び科学研究費補助金基盤研究(A)（15H01928）による研究成果の一部である。

＊＊＊

オンラインのテロリストコンテントの伝達への対処に関する欧州議会及び理事会の 2021 年 4 月 29 日の規則(EU) 2021/784

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online

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 114 条に鑑み,
欧州委員会からの提案に鑑み,
立法案を国内議会に送付した後,
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],

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Economic and Social Committee [(1)],
Acting in accordance with the ordinary legislative procedure [(2)],

Whereas:

(1) この規則は, テロリストの目的のためのホスティングサービスの濫用に対処することによって, そして, 欧州連合全域にわたる公共の保安に貢献することによって, 開かれた民主主義社会におけるデジタル単一市場の円滑な稼働を確保することを狙いとしている。デジタル単一市場の稼働は, オンライン環境におけるホスティングサービスプロバイダと利用者の信頼のための法的安定性を強化することによって, 並びに, 開かれた民主主義の社会において情報と思想を受け, 伝達する自由及びメディアの自由と多元主義を含め, 表現の自由のための安全確保を強化することによって, 向上させるべきである。

This Regulation aims to ensure the smooth functioning of the digital single market in an open and democratic society, by addressing the misuse of hosting services for terrorist purposes and

[1] OJ C 110, 22.3.2019, p. 67.
[2] 欧州議会の 2019 年 4 月 17 日付け意見書（官報未搭載）及び理事会の第一読会における 2021 年 3 月 16 日付け意見書（OJ C 135, 16.4.2021, p. 1）。欧州議会の 2021 年 4 月 28 日付け意見書（官報未搭載）.

contributing to public security across the Union. The functioning of the digital single market should be improved by reinforcing legal certainty for hosting service providers and users' trust in the online environment, as well as by strengthening safeguards to the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society and the freedom and pluralism of the media.

(2) オンラインのテロリストコンテントの伝達に対処するための法令上の措置は，社会の過激化の持続的な防止を達成するため，メディアリテラシと批判的な思考を強化すること，代替ナラティブ及び対抗ナラティブの開発，そして，オンラインのテロリストコンテントの影響及びそれに対する脆弱性を低減させるための上記以外の取り組み，並びに，社会活動への投資，影響を受けたコミュニティとの脱過激化の取り組みとその従事を含め，テロリズムに対処するための構成国の戦略によって補完されるべきである。

Regulatory measures to address the dissemination of terrorist content online should be complemented by Member State strategies to address terrorism, including the strengthening of media literacy and critical thinking, the development of alternative and counter narratives, and other initiatives to reduce the impact of and vulnerability to terrorist content online, as well as investment in social work, deradicalisation initiatives and engagement with affected communities, in order to achieve the sustained prevention of radicalisation in society.

(3) オンラインの違法なコンテントというより広範な問題の一部であるオンラインのテロリストコンテントに対処することは，立法措置，非立法措置，及び，基本的な権利を完全に尊重する態様による行政機関とホスティングサービスプロバイダとの間の共働を基礎とする任意の措置の組み合わせを必要とする。

Addressing terrorist content online, which is part of a broader problem of illegal content online, requires a combination of legislative, non-legislative and voluntary measures based on collaboration between authorities and hosting service providers, in a manner that fully respects fundamental rights.

(4) インターネット上において能動的なホスティングサービスプロバイダは，企業と市民とを結びつけることによって，そして，公衆の討論を容易にし，情報，意見及び思想の伝達と受領を容易にし，欧州連合内における技術革新，経済成長及び雇用創出に大きく貢献することによって，デジタル経済において必須の役割を果たしている。しかしながら，ホスティングサービスプロバイダのサービスは，一定の場合において，オンラインの違法な活動を遂行する目的のために第三者によって悪用されている。その中でも特に大きな懸念は，テロリストグループ及びその支援者による，それらの者のメッセージを拡散するため，過激化させ，追従者を勧誘するため，そして，テロリスト活動を容易にし，指揮するため，オンラインのテロリストコンテントを伝達するための，それらのサービスの濫用である。

Hosting service providers active on the internet play an essential role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and receipt of information, opinions and ideas, contributing significantly to innovation, economic growth and job creation in the Union. However, the services of hosting service providers are in certain cases abused by third parties for the purpose of carrying out illegal activities online. Of particular concern is the misuse of those services by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to radicalise and recruit followers, and to facilitate and direct terrorist activity.

(5) それが唯一の要因というではないが，オンラインのテロリストコンテントの存在は，テロリスト行為へと導き得る，個人の過激化のための触媒であることが明らかであり，それゆえ，利用者，市民及び社会の大多数にとって，並びに，そのプロバイダの利用者の信頼を低下させ，そのプロバイダのビジネスモデルを損ねるものであるので，そのようなコンテントをホスティングするオンラインサービスプロバイダにとって，深刻な負の結果をもつ。ホスティングサービスプロバイダが提供するサービスと関係するそのプロバイダの中心的な役割及び技術的手段と能力に照らし，ホスティングサービスプロバイダは，開かれた民主主義の社会において情報と思想を受け，伝達する自由を含め，表現の自由の基本的な重要性を考慮に入れつつ，テロリストによる濫用に対してそのプロバイダのサービスを防護するため，そして，そのプロバイダのオンラインのサービスを介して伝達されたテロリストコンテントへの対処を助けるための特別の社会的責任を負っている。

While not the only factor, the presence of terrorist content online has proven to be a catalyst for the radicalisation of individuals which can lead to terrorist acts, and therefore has serious negative consequences for users, citizens and society at large as well as for the online service providers hosting such content, since it undermines the trust of their users and damages their business models. In light of their central role and the technological means and capabilities associated with the services they provide, hosting service providers have particular societal responsibilities to protect their services from misuse by terrorists and to help address terrorist content disseminated through their services online, while taking into account the fundamental importance of the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society.

(6) オンラインのテロリストコンテントに対抗するための欧州連合レベルの努力は，構成国とホスティングサービスプロバイダとの間の任意の協力の枠組みを通じて，2015 年に開始された。それらの努力は，オンラインのテロリストコンテントのアクセシビリティを更に低減させ，急速に進化する問題に対処するため，明確な立法枠組みによって補完される必要がある。その立法枠組みは，委員会勧告(EU) 2018/334[3]によって強化された任意の努力を基礎とするもの

[3] オンラインの違法なコンテントとの実効的な闘いのための措置に関する 2018 年 3 月 1 日の委員会勧告(EU) 2018/334 (OJ L 63, 6.3.2018, p. 50).

であること，そして，欧州議会及び理事会の指令 2000/31/EC[4]によって設けられた横断的な枠組みに沿って違法で危険なコンテントに対処するための強化された措置を求める欧州議会によって行われた要請，並びに，テロリスト行為を扇動するオンラインのコンテントの検知と削除の向上を求める欧州理事会の要請に応えることを求めている。

Efforts at Union level to counter terrorist content online commenced in 2015 through a framework of voluntary cooperation between Member States and hosting service providers. Those efforts need to be complemented by a clear legislative framework in order to further reduce the accessibility of terrorist content online and adequately address a rapidly evolving problem. The legislative framework seeks to build on voluntary efforts, which were reinforced by Commission Recommendation (EU) 2018/334(3), and responds to calls made by the European Parliament to strengthen measures to address illegal and harmful content online in line with the horizontal framework established by Directive 2000/31/EC of the European Parliament and of the Council(4), as well as by the European Council to improve the detection and removal of content online that incites terrorist acts.

(7) この規則は，指令 2000/31/EC の適用に影響を与えてはならない。とりわけ，個別の措置を含め，この規則を遵守してホスティングサービスプロバイダによって講じられる措置は，それ自体として，同指令に定める責任免除の受益を当該ホスティングサービスプロバイダが失うことを導いてはならない。更に，この規則は，責任免除に関して同指令に定める条件に適合しない場合において，ホスティングサービスプロバイダの法的責任を確定するための国内当局及び裁判所の権限を害さない。

This Regulation should not affect the application of Directive 2000/31/EC. In particular, any measures taken by a hosting service provider in compliance with this Regulation, including any specific measures, should not in themselves lead to that hosting service provider losing the benefit of the liability exemption provided for in that Directive. Moreover, this Regulation does not affect the powers of national authorities and courts to establish the liability of hosting service providers where the conditions set out in that Directive for liability exemption are not met.

(8) この規則と欧州議会及び理事会の指令 2010/13/EU[5]との間で，同指令の第 1 条第 1 項(a)に定義する視聴覚メディアサービスを規律する条項との関係において衝突が生ずる場合，指

[4] 域内市場における情報社会サービスの一定の法的側面，とりわけ電子商取引に関する欧州議会及び理事会の 2000 年 6 月 8 日の指令 2000/31/EC（「電子商取引に関する指令」）(OJ L 178, 17.7.2000, p. 1).

[5] 視聴覚メディアサービスの提供に関し，構成国の法律，規則及び行政活動によって定められる一定の条項の調整に関する欧州議会及び理事会の 2010 年 3 月 10 日の指令 2010/13/EU（視聴覚メディアサービス指令）(OJ L 95, 15.4.2010, p. 1).

令 2010/13/EU が優先する。このことにより，この規則に基づく義務，とりわけ，ビデオ共有プラットフォームプロバイダと関連する義務は，影響を受けないままとすべきである。

In the event of a conflict between this Regulation and Directive 2010/13/EU of the European Parliament and of the Council[5] in relation to provisions governing audiovisual media services as defined in point (a) of Article 1(1) of that Directive, Directive 2010/13/EU should prevail. This should leave the obligations under this Regulation, in particular with regard to video-sharing platform providers, unaffected.

(9) この規則は，域内市場の円滑な稼働を保証するため，オンラインのテロリストの伝達のためのホスティングサービスの濫用に対処するための規定を定める。それらの規定は，欧州連合において保護される基本的な権利，とりわけ，欧州連合の基本権憲章（「憲章」）によって保障されている権利を完全に尊重すべきである。

This Regulation should set out rules to address the misuse of hosting services for the dissemination of terrorist content online in order to guarantee the smooth functioning of the internal market. Those rules should fully respect the fundamental rights protected in the Union and, in particular, those guaranteed by the Charter of Fundamental Rights of the European Union (the 'Charter').

(10) この規則は，私生活の尊重の権利，個人データの保護の権利，情報を受け，伝達する自由を含め表現の自由，事業活動を営む自由，並びに，実効的な救済の権利を含め，基本的な権利の保護を確保するための適切かつ堅牢な安全確保を構築しつつ，公共の保安の防護に貢献することを求める。更に，いかなる差別も禁止される。多元主義で民主主義の社会の必須の基盤を組成し，欧州連合が立脚する基盤とする価値である，表現と情報伝達の自由及びメディアの自由と多元主義に与えられた特別の重要性を考慮に入れた上で，職務権限のある機関及びホスティングサービスプロバイダは，民主主義の社会の中において必要であり，適切であり，かつ，比例的な措置のみを採択すべきである。表現と情報伝達の自由に影響を与える措置は，適法に情報を受け，伝達する権利を尊重しつつ，法律に従って，公衆の討論，及び，事実，意見及び思想を伝達し，受けることを容易にする上でのホスティングサービスプロバイダの中心的な役割を考慮に入れた上で，オンラインのテロリストコンテントの伝達に対処することに厳格に的を絞るべきである。オンラインのテロリストコンテントに対処するための実効的なオンラインの措置と表現及び情報転達の自由の保護とは，衝突するものではなく，補完的なものであり，互いに補強し合う到達目標である。

This Regulation seeks to contribute to the protection of public security while establishing appropriate and robust safeguards to ensure the protection of fundamental rights, including the right to respect for private life, to the protection of personal data, to freedom of expression, including the freedom to receive and impart information, the freedom to conduct a business, and to an effective remedy. Moreover, any discrimination is prohibited. Competent authorities and hosting service providers

should only adopt measures which are necessary, appropriate and proportionate within a democratic society, taking into account the particular importance accorded to the freedom of expression and information and the freedom and pluralism of the media, which constitute the essential foundations of a pluralist and democratic society and are values on which the Union is founded. Measures affecting the freedom of expression and information should be strictly targeted to address the dissemination of terrorist content online, while respecting the right to lawfully receive and impart information, taking into account the central role of hosting service providers in facilitating public debate and the distribution and receipt of facts, opinions and ideas, in accordance with the law. Effective online measures to address terrorist content online and the protection of freedom of expression and information are not conflicting but complementary and mutually reinforcing goals.

(11) オンラインのテロリストコンテントの伝達に対処するためにホスティングサービスプロバイダと職務権限のある当局の両者が講じるべき行動に関する明確性を提供するため，この規則は，予防的な目的のために，欧州議会及び理事会の指令(EU) 2017/541[6]に基づく関連犯罪の定義を構成する「テロリストコンテント」の定義を設けるべきである。オンラインの最も危険なテロリストプロパガンダに対処する必要性に鑑み，当該定義は，テロリスト行為を実行し，それに寄与し，それに参加することを誰かに対して扇動または勧誘するもの，テロリストグループの活動への参加を誰かに対して勧誘するもの，または，テロリスト攻撃を描写する対象物を伝達することによる場合を含め，テロリスト活動を美化する対象物を包摂すべきである。その定義は，爆発物，銃器もしくはそれ以外の武器，有害もしくは危険な物質，または，化学，生物，放射線及び核（CBRN）の物質の製造もしくは使用に関する指示，または，テロリスト行為の実行する目的もしくはその実行に寄与する目的のための，攻撃対象の選択を含め，上記以外の個別の手法もしくは技法に関する指示を提供する対象物も含めるべきである。そのような対象物は，そのような犯罪行為が更に実行される危険性を生じさせる文，画像，音声録音及び映像，並びに，テロリスト行為のライブ送信を含める。対象物がこの規則の意味におけるテロリストコンテントを組成するか否かを評価する際，職務権限のある機関及びホスティングサービスプロバイダは，言動の性質及び語法，その言動が行われた文脈，及び，それらの言動が，保安と人の安全に関して危険な結果を導く潜在性のような要素を考慮に入れるべきである。テロリスト行為に関与し，制限措置に服している個人，グループ及び法主体の欧州連合のリストに含まれている個人，グループまたは法主体によってその対象物が作成されたという事実，それらの者に属するという事実，または，それらの者の代わりに伝達されているという事実は，その評価における重要な要素を構成すべきである。

In order to provide clarity about the actions that both hosting service providers and competent authorities are to take to address the dissemination of terrorist content online, this Regulation should

[6] テロリズムとの闘いに関する，並びに，理事会枠組み決定 2002/475/JHA を置き換え，及び，理事会決定 2005/671/JHA を改正する欧州議会及び理事会の 2017 年 3 月 15 日の指令(EU) 2017/541 (OJ L 88, 31.3.2017, p. 6).

establish a definition of 'terrorist content' for preventative purposes, consistent with the definitions of relevant offences under Directive (EU) 2017/541 of the European Parliament and of the Council[6]. Given the need to address the most harmful terrorist propaganda online, that definition should cover material that incites or solicits someone to commit, or to contribute to the commission of, terrorist offences, solicits someone to participate in activities of a terrorist group, or glorifies terrorist activities including by disseminating material depicting a terrorist attack. The definition should also include material that provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, as well as chemical, biological, radiological and nuclear (CBRN) substances, or on other specific methods or techniques, including the selection of targets, for the purpose of committing or contributing to the commission of terrorist offences. Such material includes text, images, sound recordings and videos, as well as live transmissions of terrorist offences, that cause a danger of further such offences being committed. When assessing whether material constitutes terrorist content within the meaning of this Regulation, competent authorities and hosting service providers should take into account factors such as the nature and wording of statements, the context in which the statements were made and their potential to lead to harmful consequences in respect of the security and safety of persons. The fact that the material was produced by, is attributable to or is disseminated on behalf of a person, group or entity included in the Union list of persons, groups and entities involved in terrorist acts and subject to restrictive measures should constitute an important factor in the assessment.

(12) 教育，報道，芸術もしくは調査研究の目的またはテロリスト活動に抗する認識向上の目的のために伝達される対象物は，テロリストコンテントと判断されてはならない。この規則に定義する「テロリストコンテント」を組成するコンテント提供者によって提供された対象物であるか否かを判断する際，とりわけ，メディアの自由と多元主義を含め，表現と情報伝達の自由の権利，並びに，芸術と科学の自由が考慮に入れられるべきである。特に，コンテント提供者が編集責任をもつ場合，伝達される対象物の除去に関する判断は，憲章を含め，欧州連合法に従った報道またはメディア法令によって定められたジャーナリズムの基準を考慮に入れるべきである。更に，機微の政治的問題に関する公衆の討議における極端な見解，論争となる見解または特異な見解の表現は，テロリストコンテントと判断されてはならない。

Material disseminated for educational, journalistic, artistic or research purposes or for awareness-raising purposes against terrorist activity should not be considered to be terrorist content. When determining whether the material provided by a content provider constitutes 'terrorist content' as defined in this Regulation, account should be taken, in particular, of the right to freedom of expression and information, including the freedom and pluralism of the media, and the freedom of the arts and sciences. Especially in cases where the content provider holds editorial responsibility, any decision as to the removal of the disseminated material should take into account the journalistic standards established by press or media regulation in accordance with Union law, including the

Charter. Furthermore, the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered to be terrorist content.

(13) オンラインのテロリストコンテントの伝達に実効的に対処するため，個人の私生活の尊重を確保しつつ，この規則は，そのような情報及び対象物の記録保存及び公衆に対する伝達が，技術的で，自動的かつ受動的な性質のものであるか否かに拘らず，要求に応じてそのサービスの利用者から提供された情報及び対象物を記録保存し，公衆に対して伝達する情報社会サービスのプロバイダに対して適用されるべきである。「記録保存」の概念は，物理サーバまたは仮想サーバの記憶領域内でデータを保有することとして理解されるべきである。それゆえ，「単なる導管」または「キャッシング」のプロバイダ，並びに，それら以外の，インターネットインフラの別のレイヤにおいて提供され，レジストリ及びレジストラのような記録保存を包摂しないサービスのプロバイダ，並びに，ドメイン名サービス（DNS）のプロバイダ，決済プロバイダまたは分散サービス拒否攻撃（DDoS）防御サービスのプロバイダは，この規則の適用範囲外とすべきである。

In order to effectively address the dissemination of terrorist content online, while ensuring respect for the private life of individuals, this Regulation should apply to providers of information society services which store and disseminate to the public information and material provided by a user of the service on request, irrespective of whether the storing and dissemination to the public of such information and material is of a mere technical, automatic and passive nature. The concept of 'storage' should be understood as holding data in the memory of a physical or virtual server. Providers of 'mere conduit' or 'caching' services, as well as of other services provided in other layers of the internet infrastructure, which do not involve storage, such as registries and registrars, as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services, should therefore fall outside the scope of this Regulation.

(14) 「公衆に対する伝達」の概念は，潜在的に不特定数の者に対して情報を利用できるようにすること，すなわち，それらの利用者が当の情報に実際にアクセスするか否かに拘らず，そのコンテント提供者による更に別の行動を要求することなく，その情報を利用者に対して一般的に容易にアクセス可能にすることを伴うべきである。従って，情報へのアクセスが利用者グループへの登録またはそれに入るための許可を要するときは，当該情報は，アクセスを与えられる者の人間による判定または選択なしに，その情報へのアクセスを求める利用者が自動的に登録または許可される場合に限り，公衆に対して伝達されていると判断されるべきである。電子メール，プライベートメッセージ送信サービスのような，欧州議会及び理事会の指令(EU) 2018/1972[7]の第 2 条第 5 号に定義する個人間通信サービスは，この規則の適用範囲外とすべきである。そのような行動がコンテント提供者の直接の要求に基づいて遂行されてい

[7] 欧州電子通信法を定める欧州議会及び理事会の 2018 年 12 月 11 日の指令(EU) 2018/1972 (OJ L 321, 17.12.2018, p. 36).

る場合に限り，この規則の意味において情報が記録保存され，公衆に対して伝達されていると判断されるべきである。その結果として，クラウドインフラのような，コンテント提供者以外の者の要求に応じて，かつ，コンテント提供を間接的にのみ受益させる場合に提供されるサービスのプロバイダは，この規則に包摂されるべきではない。この規則は，そのサービスが，コンテント提供者の直接の要求に応じて，記録保存された情報を公衆に利用できるようにするために利用されるものである限り，例えば，ソーシャルメディア，映像，画像及び視聴覚の共有サービス，並びに，ファイル共有サービス及びそれ以外のクラウドサービスを包摂すべきである。ホスティングサービスプロバイダが複数のサービスを提供する場合，この規則は，この規則の適用範囲内にあるサービスに対してのみ適用される。

The concept of ‘dissemination to the public’ should entail the making available of information to a potentially unlimited number of persons, namely making the information easily accessible to users in general, without requiring further action by the content provider, irrespective of whether those persons actually access the information in question. Accordingly, where access to information requires registration or admittance to a group of users, that information should be considered to be disseminated to the public only where users seeking to access the information are automatically registered or admitted without a human decision or selection of whom to grant access. Interpersonal communication services, as defined in point (5) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council(7), such as emails or private messaging services, should fall outside the scope of this Regulation. Information should be considered to be stored and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request of the content provider. Consequently, providers of services, such as cloud infrastructure, which are provided at the request of parties other than the content providers and only indirectly benefit the latter, should not be covered by this Regulation. This Regulation should cover, for example, providers of social media, video, image and audio-sharing services, as well as file-sharing services and other cloud services, insofar as those services are used to make the stored information available to the public at the direct request of the content provider. Where a hosting service provider offers several services, this Regulation should apply only to the services that fall within its scope.

(15) テロリストコンテントは，しばしば，第三国内に拠点のあるホスティングサービスプロバイダから提供されるサービスを介して，公衆に対して伝達される。欧州連合内の利用者を防護するため，そして，デジタル単一市場内で業務遂行している全てのホスティングサービスプロバイダが同じ要件に服することを確保するため，この規則は，そのプロバイダの主たる拠点のある国とは無関係に，欧州連合内において提供される関連サービスの全てのプロバイダに対して適用されるべきである。ホスティングサービスプロバイダは，1 または複数の構成国の自然人または法人に対してそのプロバイダのサービスを利用できるようにしており，かつ，当該 1 または複数の構成国と実質的な接続をもつ場合，欧州連合内においてサービスを提供していると判断されるべきである。

Terrorist content is often disseminated to the public through services provided by hosting service providers established in third countries. In order to protect users in the Union and to ensure that all hosting service providers operating in the digital single market are subject to the same requirements, this Regulation should apply to all providers of relevant services offered in the Union, irrespective of the country of their main establishment. A hosting service provider should be considered offering services in the Union if it enables natural or legal persons in one or more Member States to use its services and has a substantial connection to that Member State or those Member States.

(16) 欧州連合への実質的な接続は，ホスティングサービスプロバイダが欧州連合内に拠点をもち，そのサービスが 1 もしくは複数の構成国の多数の利用者によって利用されている場合，または，そのプロバイダの活動が 1 もしくは複数の構成国に向けて的を絞っている場合，存在するものとすべきである。1 もしくは複数の構成国に向けて活動の的を絞っていることは，関係する構成国において一般的に使用されている言語もしくは通貨の利用，または，そのような構成国から製品もしくはサービスの注文が可能であることのような要素を含め，全ての関連する状況を基礎として判断されるべきである。そのように的を絞っていることは，関連する国内アプリケーション店におけるアプリケーションの可用性から，地域を限った商業宣言広告または当該構成国において一般的に使用される言語による宣伝広告の提供から，または，当該構成国において一般に使用されている言語による顧客サービスの提供による場合のような，顧客関係の取扱いからも導き出され得る。実質的な接続は，欧州議会及び理事会の規則(EU) No 1215/2012[8]の第 17 条第 1 項(c)に定める 1 または複数の構成国に対してホスティングサービスプロバイダがその活動を向けている場合においても推定されるべきである。ホスティングサービスプロバイダの Web サイトの単なるアクセシビリティ，電子メールアドレスのアクセシビリティまたは 1 もしくは複数の構成国における連絡先のアクセシビリティは，そのことのみでは，欧州連合への実質的な接続を構成するために十分であるとしてはならない。更に，欧州議会及び理事会の規則(EU) 2018/302[9]に定める差別禁止を遵守することだけのためのサービスの提供は，そのことのみを根拠として，欧州連合との実質的な接続を構成すると判断されてはならない。

A substantial connection to the Union should exist where the hosting service provider has an establishment in the Union, its services are used by a significant number of users in one or more Member States, or its activities are targeted towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant

[8] 民事及び商事における裁判管轄権並びに判決の承認及び執行に関する欧州議会及び理事会の 2012 年 12 月 12 日の規則(EU) No 1215/2012 (OJ L351, 20.12.2012, p.1).

[9] 域内市場内における正当化されないジオブロッキング及びそれ以外の形態の顧客の国籍、居住地及び事業所所在地を理由とする差別への対処に関する，規則(EC) No 2006/2004 及び規則(EU) 2017/2394 並びに指令 2009/22/EC を改正する欧州議会及び理事会の 2018 年 2 月 28 日の規則(EU) 2018/302 (OJ L 60 I, 2.3.2018, p. 1).

circumstances, including factors such as the use of a language or a currency generally used in the Member State concerned, or the possibility of ordering goods or services from such Member State. Such targeting could also be derived from the availability of an application in the relevant national application store, from providing local advertising or advertising in a language generally used in the Member State concerned, or from the handling of customer relations such as by providing customer service in a language generally used in that Member State. A substantial connection should also be assumed where a hosting service provider directs its activities towards one or more Member States as set out in point (c) of Article 17(1) of Regulation (EU) No 1215/2012 of the European Parliament and of the Council[8]. The mere accessibility of a hosting service provider's website, of an email address or of other contact details in one or more Member States, taken in isolation, should not be sufficient to constitute a substantial connection. Moreover, the provision of a service with a view to mere compliance with the prohibition of discrimination laid down in Regulation (EU) 2018/302 of the European Parliament and of the Council[9] should not, on that ground alone, be considered to constitute a substantial connection to the Union.

(17) 職務権限のある機関による評価の後にホスティングサービスプロバイダに対してテロリストコンテントの削除またはアクセス不能化を要求する削除命令をもたらす手続及び義務は，整合化されるべきである。オンラインサービス全体にわたりテロリストコンテントが伝達される速度に鑑み，ホスティングサービスプロバイダに対し，削除命令の中で指示されたテロリストコンテントが，その削除命令を受領した時から 1 時間以内に，削除されまたは全ての構成国においてそのコンテントへのアクセスが不可能にされることを確保すべき義務を負わせるべきである。適正に正当化される緊急の場合を除き，職務権限のある機関は，ホスティングサービスプロバイダに対し，当該ホスティングサービスプロバイダに対する最初の削除命令の発令前に，手続及び少なくとも 12 時間の適用可能な期限に関する情報を提供すべきである。適正に正当化される緊急の場合は，人の生命もしくは身体の完全性に対する差し迫った脅威のある状況のような，削除命令の受領後 1 時間以上経後のテロリストコンテントの削除またはアクセス不能化によって，重大な危険を生じさせ得る場合，または，そのようなコンテントが，人の生命もしくは身体の完全性に対する危険をもたらす事態が進行中であることを描写している場合に発生する。職務権限のある機関は，その場合が緊急の場合を構成するかどうかを判断し，かつ，その削除命令の中でその判断を適正に正当化すべきである。ホスティングサービスプロバイダが，客観的に正当化し得る技術上の理由または業務遂行上の理由を含め，不可抗力または事実上不可能であることを根拠として，その命令の受領から 1 時間以内に削除命令を遵守できない場合，そのプロバイダは，可能な限り速やかに発令元である職務権限のある機関に連絡し，かつ，その状況が解決次第速やかに，その削除命令を遵守すべきである。

The procedure and obligations resulting from removal orders requiring hosting service providers to remove or disable access to terrorist content, following an assessment by the competent authorities, should be harmonised. Given the speed at which terrorist content is disseminated across online

services, an obligation should be imposed on hosting service providers to ensure that the terrorist content identified in the removal order is removed or access to it is disabled in all Member States within one hour of receipt of the removal order. Except for in duly justified cases of emergency, the competent authority should provide the hosting service provider with information on procedures and applicable deadlines at least 12 hours in advance of issuing for the first time a removal order to that hosting service provider. Duly justified cases of emergency occur where the removal of or disabling of access to the terrorist content later than one hour after receipt of the removal order would result in serious harm, such as in situations of an imminent threat to the life or physical integrity of a person, or when such content depicts ongoing events resulting in harm to the life or physical integrity of a person. The competent authority should determine whether cases constitute emergency cases and duly justify its decision in the removal order. Where the hosting service provider cannot comply with the removal order within one hour of its receipt, on grounds of *force majeure* or *de facto* impossibility, including for objectively justifiable technical or operational reasons, it should inform the issuing competent authority as soon as possible and comply with the removal order as soon as the situation is resolved.

(18) 削除命令は，削除されるべき対象物またはそれへのアクセスが不能化されるべき対象をテロリストコンテントとして分類した理由の説明を含めるべきであり，かつ，正確な URL を示すことにより，及び，それが必要なときは，当のコンテントのスクリーンショットのような URL 以外の付加的な情報によって，当該コンテントの所在場所に関する十分な情報を提供すべきである。当該理由の説明は，そのホスティングサービスプロバイダが，そして，最終的には，そのコンテント提供者が，それらの者の法務上の救済の権利を実効的に行使できるようにすべきである。提供される理由は，進行中の捜査を危険に晒し得る機微の情報の開示を意味するものであってはならない。

The removal order should contain a statement of reasons qualifying the material to be removed or access to which is to be disabled as terrorist content and provide sufficient information for the location of that content, by indicating the exact URL and, where necessary, any other additional information, such as a screenshot of the content in question. That statement of reasons should allow the hosting service provider and, ultimately, the content provider to effectively exercise their right to judicial redress. The reasons provided should not imply the disclosure of sensitive information which could jeopardise ongoing investigations.

(19) 職務権限のある機関は，この規則の目的のためにホスティングサービスプロバイダによって指定され，または，設けられた連絡場所に対して直接に，個人データの保護に関する欧州連合法に従い，そのホスティングサービスプロバイダによって利用できるようにされているものを含め，安全な電子メールもしくはプラットフォームまたはそれ以外の安全な経路による場合のような，その命令の送受信の日時の正確性を含め，そのホスティングサービスプロバイダがその命令の真正性を確認できる条件の下で，書面による記録を生成可能な電子的な手

段によって，削除命令を送付すべきである。就中，欧州議会及び理事会の規則(EU) No 910/2014[10]に定める適格電子登録配達サービスの利用により，当該要件に適合させ得るべきである。発令元である職務権限のある機関の構成国とは別の構成国内にホスティングサービスプロバイダの主たる拠点またはその法律上の代理者の居住地もしくは拠点がある場合，当該別の構成国の職務権限のある機関に対し，その削除命令書の副本が同時に送付されるべきである。

The competent authority should submit the removal order directly to the contact point designated or established by the hosting service provider for the purposes of this Regulation by any electronic means capable of producing a written record under conditions that allow the hosting service provider to establish the authenticity of the order, including the accuracy of the date and the time of sending and receipt thereof, such as by secured email or platforms or other secured channels, including those made available by the hosting service provider, in accordance with Union law on the protection of personal data. It should be possible for that requirement to be met through the use of, inter alia, qualified electronic registered delivery services as provided for by Regulation (EU) No 910/2014 of the European Parliament and of the Council(10). Where the hosting service provider's main establishment is or its legal representative resides or is established in a Member State other than that of the issuing competent authority, a copy of the removal order should be submitted simultaneously to the competent authority of that Member State.

(20) ホスティングサービスプロバイダの主たる拠点がある構成国またはその法律上の代理者の居住地もしくは拠点がある構成国の職務権限のある機関は，その削除命令がこの規則または憲章に掲げられた基本的な権利に重大または明白に違反するかどうかを判断するため，他の構成国の職務権限のある機関から発令された削除命令を精査できるものとすべきである。コンテント提供者及びホスティングサービスプロバイダの両者は，ホスティングサービスプロバイダの主たる拠点がある構成国またはその法律上の代理者の居住地もしくは拠点がある構成国の職務権限のある機関によるそのような精査を要請する権利をもつべきである。そのような要請が行われた場合，当該職務権限のある機関は，その削除命令がそのような違反を含むか否かに関する決定を採択すべきである。当該決定がそのような違反を結論づける場合，その削除命令は，法的効果をもつことを終えるべきである。その精査は，可能な限り速やかに，誤って削除されたコンテントまたは利用不可能にされたコンテントが回復されることを確保するため，迅速に遂行されるべきである。

It should be possible for the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established to

10 域内市場における電子的なやりとりのための電子識別及び信頼サービスに関する，並びに，指令 1999/93/EC を廃止する欧州議会及び理事会の 2014 年 7 月 23 日の規則(EU) No 910/2014 (OJ L 257, 28.8.2014, p. 73).

scrutinise the removal order issued by competent authorities of another Member State to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights enshrined in the Charter. Both the content provider and the hosting service provider should have the right to request such scrutiny by the competent authority in the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established. Where such a request is made, that competent authority should adopt a decision on whether the removal order comprises such an infringement. Where that decision finds such an infringement, the removal order should cease to have legal effects. The scrutiny should be carried out swiftly so as to ensure that erroneously removed or disabled content is reinstated as soon as possible.

(21) テロリストコンテントの危険に晒されているホスティングサービスプロバイダは，そのプロバイダが利用約款をもつ場合，公衆に対するテロリストコンテントの伝達のためのそのプロバイダのサービスの濫用に対処するための条項をその利用約款の中に含める。それらのプロバイダは，勤勉であり，透明性があり，かつ，非差別な態様で，それらの条項を適用する。

Hosting service providers that are exposed to terrorist content should, where they have terms and conditions, include therein provisions to address the misuse of their services for the dissemination to the public of terrorist content. They should apply those provisions in a diligent, transparent, proportionate and non-discriminatory manner.

(22) 問題の規模，及び，テロリストコンテントを実効的に識別同定及び削除するために必要な速度に鑑み，実効的かつ比例的な特別の措置は，オンラインのテロリストコンテントに対処する上で，必須の要素の 1 つである。そのプロバイダのサービスの上にあるテロリストコンテントのアクセシビリティを低減させるため，テロリストコンテントの危険に晒されているホスティングサービスプロバイダは，テロリストコンテントの危険に晒されているリスク及びレベル，並びに，第三者の利益に対して与える影響及び情報の公共の利益を考慮に入れた上で，特別の措置を設けるべきである。ホスティングサービスプロバイダは，テロリストコンテントの識別同定及び削除のためにどのような適切，実効的かつ比例的な特別の措置が設けられるべきかを判断すべきである。特別の措置は，テロリストコンテントを識別同定し，迅速に削除またはアクセス不能化するための職員配置または技術的措置のような，適切な技術上または運用上の措置または能力，テロリストコンテントであると主張するコンテントを通報または警報するための利用者のための仕組み，または，そのプロバイダのサービス上にあるテロリストコンテントの可用性に対処するために適切かつ実効的であるとそのホスティングサービスプロバイダが判断する上記以外の措置を含め得る。

Given the scale of the problem and the speed necessary to effectively identify and remove terrorist content, effective and proportionate specific measures are an essential element in addressing terrorist content online. With a view to reducing the accessibility of terrorist content on their services, hosting service providers exposed to terrorist content should put in place specific measures taking into

account the risks and level of exposure to terrorist content as well as the effects on the rights of third parties and the public interest to information. Hosting service providers should determine what appropriate, effective and proportionate specific measure should be put in place to identify and remove terrorist content. Specific measures could include appropriate technical or operational measures or capacities such as staffing or technical means to identify and expeditiously remove or disable access to terrorist content, mechanisms for users to report or flag alleged terrorist content, or any other measures the hosting service provider considers appropriate and effective to address the availability of terrorist content on its services.

(23) 特別の措置を設ける際，ホスティングサービスプロバイダは，憲章の下で保護されるものとしての利用者の表現及び情報伝達の自由並びにメディアの自由と多元主義が保護されることを確保すべきである。個人データの保護に関する立法を含め，法律に定める要件に加え，ホスティングサービスプロバイダは，テロリストコンテントではないコンテントの削除またはそのコンテントへのアクセスの不能化を導く意図的ではない判断または誤った判断を避けるため，それが適切なときは，人間による監視及び検証を含め，デューディリジェンスをもって行動し，かつ，安全確保を実装すべきである。

When putting in place specific measures, hosting service providers should ensure that users' right to freedom of expression and information as well as the freedom and pluralism of the media as protected under the Charter are preserved. In addition to any requirement laid down in the law, including legislation on the protection of personal data, hosting service providers should act with due diligence and implement safeguards, where appropriate, including human oversight and verifications, to avoid any unintended or erroneous decision leading to the removal of or disabling of access to content that is not terrorist content.

(24) その措置が実効的かつ比例的であるか否か，並びに，自動化された手段が使用される場合，そのホスティングサービスプロバイダが人間による監視及び検証のために必要となる能力をもっているか否かを当該機関が判断できるようにするため，ホスティングサービスプロバイダは，職務権限のある機関に対し，設けられた特別の措置を報告すべきである。その措置の実効性及び比例性の評価において，職務権限のある機関は，そのホスティングサービスに対して発令された削除命令の数，そのホスティングサービスプロバイダの規模及び経済的能力，例えば，欧州連合内における利用者数を基礎として，テロリストコンテントの伝達におけるそのプロバイダのサービスの影響力，並びに，オンラインのテロリストコンテントの伝達のためのそのプロバイダのサービスの濫用に対処するために設けられた安全確保を含め，関連するパラメータを考慮に入れるべきである。

The hosting service provider should report to the competent authority on the specific measures in place in order to allow that authority to determine whether the measures are effective and proportionate and whether, if automated means are used, the hosting service provider has the

necessary capacity for human oversight and verification. In assessing the effectiveness and proportionality of the measures, competent authorities should take into account relevant parameters, including the number of removal orders issued to the hosting service provider, the size and economic capacity of the hosting service provider and the impact of its services in disseminating terrorist content, for example on the basis of the number of users in the Union, as well as the safeguards put in place to address the misuse of its services for the dissemination of terrorist content online.

(25) 設けられた特別の措置がリスクに対処するためには不十分であると職務権限のある機関が判断する場合，その職務権限のある機関は，付加的な，適切であり，実効的であり，かつ，比例的な特別の措置を採択することを要求できるべきである。そのような付加的な特別の措置の実装を求める要求は，指令 2000/31/EC の第 15 条第 1 項の意味における一般的な監視義務もしくは積極的に事実の発見に従事すべき義務，または，自動化されたツールを利用すべき義務を導いてはならない。ただし，オンラインのテロリストコンテントの伝達のためのそのプロバイダのサービスの濫用に実効的に対処するために自動化されたツールが適切かつ必要であるとそのプロバイダが判断するときは，ホスティングサービスプロバイダは，自動化されたツールを利用できるべきである。

Where the competent authority considers that the specific measures put in place are insufficient to address the risks, it should be able to require the adoption of additional appropriate, effective and proportionate specific measures. The requirement to implement such additional specific measures should not lead to a general obligation to monitor or to engage in active fact-finding within the meaning of Article 15(1) of Directive 2000/31/EC or to an obligation to use automated tools. However, it should be possible for hosting service providers to use automated tools if they consider this to be appropriate and necessary to effectively address the misuse of their services for the dissemination of terrorist content.

(26) 特別の目的のために，かつ，必要な期間に限り，ホスティングサービスプロバイダの削除されたコンテント及び関連データを保全すべき義務が定められるべきである。当のテロリストコンテントの削除の結果としてそのような関連データもまた失われ得る範囲内で，保全の要件を関連データまで拡大する必要性がある。関連データは，そのコンテント提供者に対してインターネットアクセスサービスプロバイダによって割当てられた IP アドレスと共に，加入者データ，とりわけ，コンテント提供者の識別名を含めているデータ，並びに，コンテント提供者による利用及びそのホスティングサービスのログオンとログオフの日と時に関するデータを含め，アクセスデータのようなデータを含め得る。

The obligation on hosting service providers to preserve removed content and related data should be laid down for specific purposes and limited to the period necessary. There is a need to extend the preservation requirement to related data to the extent that any such data would otherwise be lost as a consequence of the removal of the terrorist content in question. Related data can include data such

as subscriber data, in particular data pertaining to the identity of the content provider, as well as access data, including data about the date and time of use by the content provider and the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the content provider.

(27) そのコンテントが削除されまたはそのコンテントへのアクセスが不能化されたコンテント提供者のために実効的な救済が設けられることを確保する必要性，及び，行政上または法務上の手続の結果次第により，当該コンテントの回復を確保する必要性という観点から，行政上または法務上の見直し手続のためにそのコンテントを保全すべき義務は，必要であり，かつ，正当化される。テロリスト活動を破壊または防止する目的のためのその対象物がもち得る価値という観点から，捜査または訴追の目的のために対象物を保全すべき義務は，正当化され，かつ，必要である。それゆえ，テロリスト行為の防止，検知，捜査及び訴追の目的のための削除されるテロリストコンテントの保全も正当化されると判断されるべきである。テロリストコンテント及び関連データは，法執行機関が当該テロリストコンテントを点検し，それらの目的のためにそのコンテントが必要となり得るか否かを判断できるようにするために必要な期間内に限り，記録保存されるべきである。テロリスト行為の防止，検知，捜査及び訴追の目的のために，要求されるデータの保全は，テロリスト行為との結びつきをもつ可能性があり，かつ，それゆえ，テロリスト行為の訴追または公共の保安に対する重大なリスクを防止することに貢献し得るデータに限定されるべきである。ホスティングサービスプロバイダが，とりわけ，そのプロバイダ自身の特別の措置により，対象物を削除またはアクセス不能化する場合，そのプロバイダは，職務権限のある機関に対し，直ちに，生命に対する差し迫った脅威またはテロリスト行為の疑いを含む情報を含むコンテントを連絡すべきである。

The obligation to preserve the content for administrative or judicial review proceedings is necessary and justified in view of the need to ensure that effective remedies are in place for content providers whose content has been removed or access to which has been disabled, as well as to ensure the reinstatement of that content, depending on the outcome of those proceedings. The obligation to preserve material for investigative or prosecutorial purposes is justified and necessary in view of the value the material could have for the purpose of disrupting or preventing terrorist activity. Therefore, the preservation of removed terrorist content for the purposes of prevention, detection, investigation and prosecution of terrorist offences should also be considered to be justified. The terrorist content and the related data should be stored only for the period necessary to allow the law enforcement authorities to check that terrorist content and decide whether it would be needed for those purposes. For the purposes of the prevention, detection, investigation and prosecution of terrorist offences, the required preservation of data should be limited to data that are likely to have a link with terrorist offences, and could therefore contribute to prosecuting terrorist offences or to preventing serious risks to public security. Where hosting service providers remove or disable access to material, in particular through their own specific measures, they should inform the competent authorities promptly of content that contains information involving an imminent threat to life or a suspected

terrorist offence.

(28) 比例性を確保するため，その保全の期間は，コンテント提供者が行政上または法務上の見直し手続を開始するために十分な期間を許容するため，そして，テロリスト行為の捜査及び訴追のために法執行機関が関連データにアクセスできるようにするための 6 か月に限定されるべきである。ただし，その期間は，職務権限のある機関または裁判所の要求により，その 6 か月の間にそれらの手続が開始されたけれども終結していない場合において必要な長さの期間だけ延長され得るものとすべきである。保全の期間の長さは，基本的な権利とのバランスを確保しつつ，捜査及び訴追と関係して必要な対象物を法執行機関が保全できるために十分なものとすべきである。

To ensure proportionality, the period of preservation should be limited to six months to allow content providers sufficient time to initiate administrative or judicial review proceedings and to enable access by law enforcement authorities to relevant data for the investigation and prosecution of terrorist offences. However, upon the request of the competent authority or court, it should be possible to extend that period for as long as necessary in cases where those proceedings are initiated but not finalised within that six-month period. The duration of the period of preservation should be sufficient to allow law enforcement authorities to preserve the necessary material in relation to investigations and prosecutions, while ensuring the balance with the fundamental rights.

(29) この規則は，欧州連合法または国内法によって規律されている，テロリスト行為の捜査及び訴追の目的のために保全されたコンテント及び関連データへのアクセスと関連する手続保障または捜査手続上の措置を害してはならない。

This Regulation should not affect the procedural guarantees or procedural investigation measures related to access to content and related data preserved for the purposes of the investigation and prosecution of terrorist offences, as regulated under Union or national law.

(30) テロリストコンテントと関係するホスティングサービスプロバイダの基本方針の透明性は，そのプロバイダの利用者に向けたそのプロバイダの説明責任を拡大するため，そして，デジタル単一市場における市民の信頼を強化するために，必須である。当の暦年内にこの規則による行動を行ったホスティングサービスプロバイダまたはその行動とることを要求されたホスティングサービスプロバイダは，テロリストコンテントの識別同定及び削除と関係して行われた行動に関する情報を含む年次透明性報告書を公表すべきである。

The transparency of hosting service providers' policies in relation to terrorist content is essential to enhance their accountability towards their users and to reinforce trust of citizens in the digital single market. Hosting service providers that have taken action or were required to take action pursuant to this Regulation in a given calendar year should make publicly available annual transparency reports

containing information about action taken in relation to the identification and removal of terrorist content.

(31) 職務権限のある機関は，削除命令の数，命令が執行されなかった案件の数，特別の措置と関係する決定の数，行政上または法務上の見直し手続に服する案件の数，及び，制裁を科す決定の数を含む年次透明性報告書を公表すべきである。

The competent authorities should publish annual transparency reports containing information on the number of removal orders, the number of cases where an order was not executed, the number of decisions concerning specific measures, the number of cases subject to administrative or judicial review proceedings and the number of decisions imposing penalties.

(32) 欧州連合条約（TEU）の第 19 条及び憲章の第 47 条には，実効的な救済の権利が掲げられている。個々の自然人及び法人は，この規則によって講じられた措置であって，当該の者の権利に負の影響を与え得るものを不服として，職務権限のある国内裁判所において実効的な救済を求める権利をもつ。その権利は，とりわけ，削除命令またはこの規則に基づいて削除命令から生ずる決定に対し，その国の職務権限のある機関が削除命令を発令し，または，決定を行った構成国の裁判所において，ホスティングサービスプロバイダ及びコンテント提供者が実効的に不服申立てできること，並びに，ホスティングサービスプロバイダに関しては，その国の職務権限のある機関が当該決定を行った構成国の裁判所において，特別の措置または制裁と関連する決定に対し，実効的に不服申立てできることを含めるべきである。

The right to an effective remedy is enshrined in Article 19 of the Treaty on European Union (TEU) and in Article 47 of the Charter. Each natural or legal person has the right to an effective remedy before the competent national court against any of the measures taken pursuant to this Regulation which can adversely affect the rights of that person. That right should include, in particular, the possibility for hosting service providers and content providers to effectively challenge the removal orders or any decisions resulting from the scrutiny of removal orders under this Regulation before a court of the Member State whose competent authority issued the removal order or took the decision, as well as for hosting service providers to effectively challenge a decision relating to specific measures or penalties before a court of the Member State whose competent authority took that decision.

(33) 不服申立手続は，そのようなコンテントが表現及び情報伝達の自由の下で保護されている場合において，オンラインのコンテントが誤って削除またはアクセス不能化されたことに抗するための安全確保を構成する。それゆえ，ホスティングサービスプロバイダは，ユーザフレンドリな不服申立ての仕組みを設け，そして，迅速に，かつ，コンテント提供者に向けて完全に透明性のある状態で，不服申立てが取り扱われることを確保すべきである。誤って削除されまたはそのアクセスが不能化されたコンテントを回復するためのホスティングサービスプロバ

イダの要件は，そのホスティングサービスプロバイダが，そのプロバイダ自身の利用約款を執行することを害してはならない。

Complaint procedures constitute a necessary safeguard against the erroneous removal of or disabling of access to content online where such content is protected under the freedom of expression and information. Hosting service providers should therefore establish user-friendly complaint mechanisms and ensure that complaints are dealt with expeditiously and in full transparency towards the content provider. The requirement for the hosting service provider to reinstate content that has been removed or access to which has been disabled in error should not affect the possibility for the hosting service provider to enforce its own terms and conditions.

(34) TEU の第 19 条及び憲章の第 47 条に従った実効的な法律上の保護は，コンテント提供者が提供したコンテントが削除またはアクセス不能にされた理由を，そのコンテント提供者が確認できることを要求する。その目的のために，そのホスティングサービスプロバイダは，そのコンテント提供者に対し，削除またはアクセス不能化に不服を申立てるための情報を利用できるようにすべきである。状況の別に応じて，ホスティングサービスプロバイダは，この規則に従って当該コンテントが削除されまたはそのアクセスが不能化されたことを示すメッセージによって，削除またはアクセス不能化されたコンテントを置き換え得る。コンテント提供者の要求に応じて，削除またはアクセス不能化の理由及びその削除またはアクセス不能化に対する救済に関する情報がそのメッセージとは別に提供されるべきである。職務権限のある機関が，捜査の過程を含め，削除またはアクセス不能化のコンテント提供者に対して直接に通知することが適切ではなく，または，逆効果である場合，その職務権限のある機関は，そのホスティングサービスプロバイダに対し，しかるべく連絡する。

Effective legal protection in accordance with Article 19 TEU and Article 47 of the Charter requires that content providers are able to ascertain the reasons upon which the content they provide has been removed or access to which has been disabled. For that purpose, the hosting service provider should make available to the content provider information for challenging the removal or the disabling. Depending on the circumstances, hosting service providers could replace content which has been removed or access to which has been disabled with a message indicating that the content has been removed or access to it has been disabled in accordance with this Regulation. Further information about the reasons for the removal or disabling as well as the remedies for the removal or disabling should be provided upon request of the content provider. Where the competent authorities decide that for reasons of public security, including in the context of an investigation, it is inappropriate or counterproductive to directly notify the content provider of the removal or disabling, they should inform the hosting service provider accordingly.

(35) この規則の目的のために，構成国は，職務権限のある機関を指定すべきである。このことは，新たな機関の設置を必ずしも意味するものではなく，この規則に定める権限をもつ既存の組

織に対して委託することを可能とすべきである。この規則は，指定される職務権限をもつ機関の数，及び，その機関を行政機関，法執行機関または法務機関のいずれとするかを各構成国が決定できるべきものとしつつ，削除命令を発令すること，削除命令を精査すること，特別の措置を監督すること，及び，制裁を科すことに関して職務権限をもつ機関の指定を要求する。構成国は，職務権限のある機関が，客観的かつ非差別の態様でその職務を満たし，かつ，この規則に基づく職務の行使と関係して他の組織に対して指示を求めることも他の組織から指示を受けることもないことを確保すべきである。このことは，国内憲法に従った監督を排除してはならない。構成国は，欧州委員会に対し，この規則に基づいて指定した職務権限のある機関を通知すべきであり，また，欧州委員会は，職務権限のある機関を列挙する登録簿をオンラインで公表すべきである。そのオンラインの登録簿は，ホスティングサービスプロバイダによる削除命令の真正性の迅速な検証を容易にするため，容易にアクセスできるものとすべきである。

For the purposes of this Regulation, Member States should designate competent authorities. This should not necessarily imply the establishment of a new authority and it should be possible to entrust an existing body with the functions provided for in this Regulation. This Regulation should require the designation of authorities competent for issuing removal orders, scrutinising removal orders, overseeing specific measures and imposing penalties, while it should be possible for each Member State to decide on the number of competent authorities to be designated and whether they are administrative, law enforcement or judicial. Member States should ensure that the competent authorities fulfil their tasks in an objective and non-discriminatory manner and do not seek or take instructions from any other body in relation to the exercise of the tasks under this Regulation. This should not prevent supervision in accordance with national constitutional law. Member States should communicate the competent authorities designated under this Regulation to the Commission, which should publish online a register listing the competent authorities. That online register should be easily accessible to facilitate the swift verification of the authenticity of removal orders by the hosting service providers.

(36) 仕事の重複及びあり得る捜査への干渉を避けるため，そして，影響を受けるホスティングサービスプロバイダの負担をミニマム化するため，職務権限のある機関は，削除命令を発令する前に，相互に，及び，それが適切なときは，Europol との間で，情報交換し，調整及び協力すべきである。削除命令を発令すべきか否かを判断する際，職務権限のある機関は，捜査上の利益への干渉の通知（干渉回避）を適正に検討すべきである。職務権限のある機関が，別の構成国の職務権限のある機関から既存の削除命令について連絡を受けた場合，その職務権限のある機関は，同一の対象事項に関して削除命令を発令してはならない。この規則の条項の実装において，Europol は，その現在の任務及び既存の法的枠組みに沿って，支援を提供し得る。

In order to avoid duplication of effort and possible interferences with investigations and to minimise

the burden to the hosting service providers affected, the competent authorities should exchange information, coordinate and cooperate with each other and, where appropriate, with Europol, before issuing removal orders. When deciding whether to issue a removal order, the competent authority should give due consideration to any notification of an interference with an investigative interest (deconfliction). Where a competent authority is informed by a competent authority of another Member State of an existing removal order, it should not issue a removal order concerning the same subject matter. In implementing the provisions of this Regulation, Europol could provide support in line with its current mandate and existing legal framework.

(37) ホスティングサービスプロバイダによって行われる特別の措置の実効的かつ十分に一貫性のある実装を確保するため，職務権限のある機関は，削除命令並びに特別の措置の識別，実装及び評価に関するホスティングサービスプロバイダとの間の情報交換に関し，相互に調整及び協力すべきである。制裁に関する規定の採択及び制裁を科すことと関連するものを含め，この規則の実装のための他の措置との関係においても，調整及び協力が必要である。欧州委員会は，そのような調整及び協力を容易にすべきである。

In order to ensure the effective and sufficiently coherent implementation of specific measures taken by hosting service providers, competent authorities should coordinate and cooperate with each other with regard to the exchanges with hosting service providers as to removal orders and the identification, implementation and assessment of specific measures. Coordination and cooperation are also needed in relation to other measures to implement this Regulation, including with respect to the adoption of rules on penalties and the imposition of penalties. The Commission should facilitate such coordination and cooperation.

(38) 制裁を科すことに関して職責を負う構成国の職務権限のある機関が，削除命令の発令について，及び，その後におけるホスティングサービスプロバイダと別の構成国の職務権限のある機関との間の情報交換について完全に情報提供を受けることは，必須である。その目的のために，構成国は，適時の態様で関連情報を共有できる適切かつ安全な通信経路と仕組みを確保すべきである。

It is essential that the competent authority of the Member State responsible for imposing penalties is fully informed of the issuing of removal orders and of the subsequent exchanges between the hosting service provider and the competent authorities in other Member States. For that purpose, Member States should ensure appropriate and secure communication channels and mechanisms allowing the sharing of relevant information in a timely manner.

(39) 職務権限のある機関の間及びホスティングサービスプロバイダとの間の迅速な情報交換を容易にするため，そして，仕事の重複を避けるため，構成国は，現行のインターネット照会管理アプリケーションまたはその後継アプリケーションのような，Europol によって開発された専

用ツールの活用を推奨されるべきである。

To facilitate the swift exchanges between competent authorities as well as with hosting service providers, and to avoid duplication of effort, Member States should be encouraged to make use of the dedicated tools developed by Europol, such as the current internet Referral Management application or its successors.

(40) 構成国及び Europol による照会は，そのプロバイダのサービスを介して利用できるようにされている特定のコンテントをホスティングサービスプロバイダによる覚知を向上させ，そのプロバイダが迅速な行動をとることを実現可能にする実効的かつ迅速な手段の 1 つであることが証明されている。そのような照会は，当該コンテントがそのプロバイダ自身の利用約款に適合することをそのプロバイダによる任意の判断のために，テロリストコンテントと判断され得るという情報をホスティングサービスプロバイダに警告するための仕組みであり，削除命令に加えて利用可能なままとされるべきである。そのコンテントがそのプロバイダの利用約款に適合していないことを理由としてそのコンテントを削除すべきかどうかの最終判断は，そのホスティングサービスプロバイダに任される。この規則は，欧州議会及び理事会の規則(EU) 2016/794[11]に定める Europol の任務を害してはならない。それゆえ，この規則のいかなる条項も，オンラインのテロリストコンテントに対処するための道具として構成国及び Europol が照会を利用することを排除するものとして理解されてはならない。

Referrals by Member States and Europol have proven to be an effective and swift means of increasing hosting service providers' awareness of specific content available through their services and enabling them to take swift action. Such referrals, which are a mechanism for alerting hosting service providers of information that could be considered to be terrorist content for the provider's voluntary consideration of the compatibility of that content with its own terms and conditions, should remain available in addition to removal orders. The final decision on whether to remove the content because it is incompatible with its terms and conditions remains with the hosting service provider. This Regulation should not affect the mandate of Europol as laid down in Regulation (EU) 2016/794 of the European Parliament and of the Council(11). Therefore, nothing in this Regulation should be understood as precluding the Member States and Europol from using referrals as an instrument to address terrorist content online.

(41) 一定のオンラインのテロリストコンテントの特別に重大な結果に鑑み，ホスティングサービスプロバイダは，関係する構成国の関連機関に対し，または，そのプロバイダが拠点をもち，も

11 法執行協力のための欧州連合局（Europol）に関する，並びに，理事会決定 2009/371/JHA，理事会決定 2009/934/JHA，理事会決定 2009/935/JHA，理事会決定 2009/936/JHA 及び理事会決定 2009/968/JHA を置き換えて廃止す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).

しくは，法律上の代理者をもつ構成国の職務権限のある機関に対し，直ちに，生命に対する差し迫った脅威またはテロリスト行為の疑いを含むテロリストコンテントを連絡すべきである。比例性を確保するため，その義務は，指令(EU) 2017/541 の第 3 条第 1 項に定義するテロリスト行為に限定されるべきである。その連絡すべき義務は，そのような生命に対する差し迫った脅威またはテロリスト行為の疑いの証拠を積極的に探索すべきホスティングサービスプロバイダの義務を意味するものとしてはならない。関係する構成国は，加害者の国籍，潜在的な犯罪被害者の国籍またはテロリスト行為の標的である場所を基礎として，それらのテロリスト行為の捜査及び訴追に関する裁判管轄権をもつ構成国であると判断されるべきである。疑義がある場合，ホスティングサービスプロバイダは，Europol に対して情報を提出すべきであり，Europol は，関連国内機関に対して当該情報を転送することによる場合を含め，Europol の任務に従って関連する事後的な活動を提供すべきである。構成国の職務権限のある機関は，欧州連合法または国内法に基づいて利用可能な捜査措置を講ずるため，そのような情報を利用できるべきである。

Given the particular serious consequences of certain terrorist content online, hosting service providers should promptly inform the relevant authorities in the Member State concerned or the competent authorities of the Member State where they are established or have a legal representative of terrorist content involving an imminent threat to life or a suspected terrorist offence. In order to ensure proportionality, that obligation should be limited to terrorist offences as defined in Article 3(1) of Directive (EU) 2017/541. That obligation to inform should not imply an obligation on hosting service providers to actively seek any evidence of such imminent threat to life or a suspected terrorist offence. The Member State concerned should be understood to be the Member State with jurisdiction over the investigation and prosecution of those terrorist offences based on the nationality of the offender or of the potential victim of the offence or the target location of the terrorist act. In the case of doubt, hosting service providers should submit the information to Europol, which should provide the relevant follow-up action in accordance with its mandate, including by forwarding that information to the relevant national authorities. The competent authorities of the Member States should be allowed to use such information to take investigatory measures available under Union or national law.

(42) ホスティングサービスプロバイダは，削除命令の迅速な取扱いを容易にするための連絡場所を指定または設置すべきである。その連絡場所は，業務遂行の目的のためにのみ奉仕すべきである。連絡場所は，削除命令の電子的な送付を可能とするインハウスまたはアウトソースされた専用の手段，及び，その削除命令の迅速な処理を可能とする技術的な手段もしくは人的な手段によって構成されるべきである。その連絡場所が欧州連合内に所在していることは必要ではない。ホスティングサービスプロバイダは，その連絡場所がこの規則に定める機能を満たすことができることを条件として，この規則の目的のために既存の連絡場所を活用することが自由とすべきである。削除命令の受領後 1 時間以内にテロリストコンテントが削除またはアクセス不能化されることを確保するため，テロリストコンテントの危険に晒されて

いるホスティングサービスプロバイダの連絡場所は，いつでもアクセス可能とすべきである。連絡場所に関する情報は，その連絡場所が対処可能な言語に関する情報を含めるべきである。ホスティングサービスプロバイダと職務権限のある機関との間の通信を容易にするため，ホスティングサービスプロバイダは，そのプロバイダの利用約款において利用可能であり，通信のために利用可能な欧州連合の機関の公用語中の 1 つが利用可能とされることを推奨される。

Hosting service providers should designate or establish contact points to facilitate the expeditious handling of removal orders. The contact point should serve only for operational purposes. The contact point should consist of any dedicated means, in-house or outsourced, allowing for the electronic submission of removal orders and of technical or personal means allowing for the expeditious processing thereof. It is not necessary that the contact point be located in the Union. The hosting service provider should be free to make use of an existing contact point for the purpose of this Regulation, provided that the contact point is able to fulfil the functions provided for in this Regulation. With a view to ensuring that terrorist content is removed or that access thereto is disabled within one hour of receipt of a removal order, the contact points of hosting service providers exposed to terrorist content should be accessible at any time. The information on the contact point should include information about the language in which it can be addressed. In order to facilitate the communication between the hosting service providers and the competent authorities, hosting service providers are encouraged to allow for communication in one of the official languages of the Union institutions in which their terms and conditions are available.

(43) 欧州連合の領土内における物理的な存在を確保するというホスティングサービスプロバイダの一般的な要件が存在しない以上，欧州連合内でサービスを提供するホスティングサービスプロバイダがどの構成国の裁判管轄権の下にあるかを明確にすることを確保する必要性がある。一般原則として，ホスティングサービスプロバイダは，そのプロバイダが主たる拠点をもつ構成国またはその法律上の代理者の居住地もしくは拠点がある構成国の裁判管轄権の下にある。そのことは，削除命令及びこの規則に基づく削除命令の精査から生ずる決定の目的のために定められた職務権限に関する規定を妨げてはならない。欧州連合内に拠点をもたないが，法律上の代理者を指定していないホスティングサービスプロバイダに関しては，一事不再理の原則を尊重することを条件として，構成国は，それにも拘らず，裁判管轄権をもち，かつ，それゆえ，制裁を科し得る。

In the absence of a general requirement for hosting service providers to ensure a physical presence within the territory of the Union, there is a need to ensure clarity under which Member State's jurisdiction the hosting service provider offering services within the Union falls. As a general rule, the hosting service provider falls under the jurisdiction of the Member State in which it has its main establishment or in which its legal representative resides or is established. That should be without prejudice to the rules on competence established for the purpose of removal orders and decisions

resulting from the scrutiny of removal orders under this Regulation. With regard to a hosting service provider which has no establishment in the Union and does not designate a legal representative, any Member State should, nevertheless, have jurisdiction and therefore be able to impose penalties, provided that the principle of *ne bis in idem* is respected.

(44) 欧州連合内に拠点をもたないホスティングサービスプロバイダは，この規則に基づく義務の遵守及び執行を確保する目的のために，書面により，法律上の代理者を指定すべきである。ホスティングサービスプロバイダは，当該法律上の代理者がこの規則に定める機能を満たし得ることを条件として，別の目的のために既に指定されている法律上の代理者を，この規則の目的のために指定できるべきである。法律上の代理者は，そのホスティングサービスプロバイダの代わりに行動する権限を与えられるべきである。

Hosting service providers that are not established in the Union should designate in writing a legal representative in order to ensure compliance with and the enforcement of the obligations under this Regulation. It should be possible for hosting service providers to designate, for the purposes of this Regulation, a legal representative already designated for other purposes, provided that that legal representative is able to fulfil the functions provided for in this Regulation. The legal representative should be empowered to act on behalf of the hosting service provider.

(45) ホスティングサービスプロバイダによるこの規則の実効的な実装を確保するため，制裁が必要である。構成国は，制裁に関する規定，及び，それが適切なときは，制裁運用指針を採択すべきである。その制裁は，行政上または刑事上の性質のものであり得る。個々の案件における不遵守は，一事不再理の原則及び比例性の原則を尊重し，かつ，そのような制裁が組織的な不遵守を考慮に入れることを確保しつつ，制裁に服し得る。制裁は，軽微な違反の場合における注意処分，または，より重大な違反行為または組織的な違反行為との関係における制裁金を含め，異なる形態をとり得る。ホスティングサービスプロバイダが，組織的または恒常的に，削除命令の受領後 1 時間以内にテロリストコンテントを削除またはアクセス不能化しない場合においては，特別に厳しい制裁が科されるべきである。法的安定性を確保するため，この規則は，どのような違反行為が制裁に服するか，及び，どのような状況がそのような制裁のタイプ及びレベルの評価と関連性をもつかを定めるべきである。制裁金を科すかどうかを判断する際，そのホスティングサービスプロバイダの資金が適正に考慮に入れられるべきである。更に，職務権限のある機関は，そのホスティングサービスプロバイダがスタートアップまたは委員会勧告 2003/361/EC[12]に定義するマイクロ企業，小規模企業もしくは中規模企業であるかどうかを考慮に入れるべきである。そのホスティングサービスプロバイダの行動が客観的に軽率または非難に値するものであったかどうか，または，その違反行為が過失により実行されたか，意図的に実行されたかといったような付加的な状況は，考慮に入れ

[12] マイクロ企業，小規模企業及び中規模企業の定義に関する 2003 年 5 月 6 日の委員会勧告 2003/361/EC (OJ L 124, 20.5.2003, p. 36).

られるべきである。構成国は，この規則の違反行為に対して科される制裁が，テロリストコンテントではない対象物の削除を推進しないことを確保すべきである。

Penalties are necessary to ensure the effective implementation of this Regulation by hosting service providers. Member States should adopt rules on penalties, which can be of an administrative or criminal nature, as well as, where appropriate, fining guidelines. Non-compliance in individual cases could be subject to penalties while respecting the principles of *ne bis in idem* and of proportionality and ensuring that such penalties take account of systematic failure. Penalties could take different forms, including formal warnings in the case of minor infringements or financial penalties in relation to more severe or systematic infringements. Particularly severe penalties should be imposed in the event that the hosting service provider systematically or persistently fails to remove or disable access to terrorist content within one hour of receipt of a removal order. In order to ensure legal certainty, this Regulation should set out which infringements are subject to penalties and which circumstances are relevant for assessing the type and level of such penalties. When determining whether to impose financial penalties, due account should be taken of the financial resources of the hosting service provider. Moreover, the competent authority should take into account whether the hosting service provider is a start-up or a micro, small or medium-sized enterprise as defined in Commission Recommendation 2003/361/EC[12]. Additional circumstances, such as whether the conduct of the hosting service provider was objectively imprudent or reprehensible or whether the infringement has been committed negligently or intentionally, should be taken into account. Member States should ensure that penalties imposed for the infringement of this Regulation do not encourage the removal of material which is not terrorist content.

(46) 標準化されたテンプレートの利用は，職務権限のたる機関とホスティングサービスプロバイダとの間の協力と情報交換を容易にし，それらの者がより迅速かつ実効的に通信できるようにする。削除命令を受領した後の迅速な行動を確保することは，とりわけ重要である。テンプレートは，やりとりの費用を削減し，かつ，より高度な処理基準に貢献する。フィードバックテンプレートは，標準化された情報の交換を可能とし，かつ，ホスティングサービスプロバイダが削除命令を遵守できない場合には特に重要である。認証された送付経路は，その命令の送受信の日時の正確性を含め，削除命令の真正性を保証し得る。

The use of standardised templates facilitates cooperation and the exchange of information between competent authorities and hosting service providers, allowing them to communicate more quickly and effectively. It is particularly important to ensure expeditious action following the receipt of a removal order. Templates reduce translation costs and contribute to a higher standard of the process. Feedback templates allow for a standardised exchange of information and are particularly important where hosting service providers are unable to comply with removal orders. Authenticated submission channels can guarantee the authenticity of the removal order, including the accuracy of the date and the time of sending and receipt of the order.

(47) それが必要なときは，この規則の目的のために使用されるテンプレートの内容を迅速に改訂できるようにするため，この規則の別紙の改訂に関して，欧州連合の機能に関する条約の第 290 条に従って行為を採択する権限は，欧州委員会に対して委任されるべきである。技術の発展及び関連する法的枠組みの発展を考慮に入れることを可能とするため，欧州委員会は，削除命令の送信のために職務権限のある機関によって使用される電子的な手段に関する技術要件によってこの規則を補遺するため，委任される行為を採択する権限も与えられる。その準備作業の間，専門家レベルのものを含め，欧州委員会が適切なコンサルテーションを実施すること，及び，より良い立法に関する 2016 年 4 月 13 日の機関間合意[13]に定める基本原則に従ってそれらのコンサルテーションが行われることが特に重要である。とりわけ，委任される行為の準備への平等な参加を確保するため，欧州議会及び理事会は，構成国の専門家と同時に全ての文書を受領し，かつ，それらの専門家は，自動的に，委任される行為の準備を取り扱う欧州委員会の専門家グループの会合へのアクセスをもつ。

In order to allow for a swift amendment, where necessary, of the content of the templates to be used for the purposes of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of amending the annexes to this Regulation. In order to be able to take into account the development of technology and of the related legal framework, the Commission should also be empowered to adopt delegated acts to supplement this Regulation with technical requirements for the electronic means to be used by competent authorities for the transmission of removal orders. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making(13). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(48) 構成国は，この規則の実装に関する情報を収集すべきである。構成国は，それが必要なときは，この規則によるその構成国自身の透明性報告書のような，より詳細な情報と共に，ホスティングサービスプロバイダの透明性報告書及びその実装を活用できるべきである。この規則の実装の評価の情報提供のため，この規則の出力，結果及び影響の監視のための詳細な計画が定められるべきである。

Member States should collect information on the implementation of this Regulation. It should be possible for Member States to make use of the hosting service providers' transparency reports and complement them, where necessary, with more detailed information, such as their own transparency

[13] OJ L 123, 12.5.2016, p. 1.

reports pursuant to this Regulation. A detailed programme for monitoring the outputs, results and impacts of this Regulation should be established in order to inform an evaluation of the implementation of this Regulation.

(49) 実装報告書の判断及び結論，並びに，監視の実行結果を基礎として，欧州委員会は，この規則の発効から 3 年以内に，この規則の評価を遂行すべきである。その評価は，効率性，必要性，実効性，比例性，関連性，一貫性及び欧州連合の付加価値を基礎とすべきである。欧州委員会は，オンラインのテロリストコンテントの検知，識別同定及び削除を拡大するための措置，安全確保の仕組みの実効性，並びに，メディアの自由と多元主義を含め，表現及び情報伝達の自由，事業活動を営む自由，私生活の権利及び個人データの保護のような，潜在的に影響を受ける基本的な権利に対する影響を含め，この規則によって定められる異なる業務遂行上の措置及び技術上の措置の稼働を評価すべきである。欧州委員会は，潜在的に影響を受ける第三者の権利に対する影響も評価する。

Based on the findings and conclusions in the implementation report and the outcome of the monitoring exercise, the Commission should carry out an evaluation of this Regulation within three years of the date of its entry into force. The evaluation should be based on the criteria of efficiency, necessity, effectiveness, proportionality, relevance, coherence and Union added value. It should assess the functioning of the different operational and technical measures provided for by this Regulation, including the effectiveness of measures to enhance the detection, identification and removal of terrorist content online, the effectiveness of safeguard mechanisms as well as the impacts on potentially affected fundamental rights, such as the freedom of expression and information, including the freedom and pluralism of the media, the freedom to conduct a business, the right to private life and the protection of personal data. The Commission should also assess the impact on potentially affected interests of third parties.

(50) この規則の目的，すなわち，オンラインのテロリストコンテントの伝達に対処することによりデジタル単一市場の円滑な稼働を確保することは，構成国によっては十分に達成され得ず，その規模及び影響のゆえに，欧州連合レベルでより良く達成され得るので，欧州連合は，TEU の第 5 条に定める補完性の原則に従い，措置を採択できる。同条に定める比例性の原則に従い，この規則は，その目的を達成するために必要となるところを超えることがない，

Since the objective of this Regulation, namely ensuring the smooth functioning of the digital single market by addressing the dissemination of terrorist content online, cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective,

以上のとおりであるので, この規則を採択する:

HAVE ADOPTED THIS REGULATION:

第 I 節 総則的な規定
Section I General Provisions

第 1 条 対象事項及び適用範囲
Article 1 Subject matter and scope

1. この規則は，オンラインのテロリストコンテントの公衆に対する伝達のためのホスティングサービスの濫用に対処するための統一的な規定，とりわけ，以下に関して，定める：
   (a) そのプロバイダのサービスを介するテロリストコンテントの公衆に対する伝達に対処するため，及び，それが必要なときは，そのようなコンテントを削除し，もしくは，そのコンテントへのアクセスを不能にすることを確保するため，ホスティングサービスプロバイダによって適用されるべき合理的かつ比例的な取扱い；
   (b) 以下のために，欧州連合法に従って，かつ，基本的な権利，とりわけ，開かれた民主主義社会における表現及び情報伝達の自由を保護するための適切な安全確保に服して，構成国によって設けられる措置：
      (i) ホスティングサービスにより，テロリストコンテントを識別同定すること及び迅速な削除を確保すること；並びに，
      (ii) 構成国の職務権限のある機関，ホスティングサービスプロバイダ，及び，それが適切なときは，Europol の間の協力を容易にすること。

   This Regulation lays down uniform rules to address the misuse of hosting services for the dissemination to the public of terrorist content online, in particular on:
   (a) reasonable and proportionate duties of care to be applied by hosting service providers in order to address the dissemination to the public of terrorist content through their services and ensure, where necessary, the expeditious removal of or disabling of access to such content;
   (b) the measures to be put in place by Member States, in accordance with Union law and subject to suitable safeguards to protect fundamental rights, in particular the freedom of expression and information in an open and democratic society, in order to:
      (i) identify and ensure the expeditious removal of terrorist content by hosting service providers; and
      (ii) facilitate cooperation among the competent authorities of Member States, hosting service providers and, where appropriate, Europol.

2. この規則は，そのプロバイダの主達拠点の所在地に拘りなく，そのプロバイダが公衆に対して情報を伝達する限り，欧州連合内においてサービスを提供するホスティングサービスプロバイダに対して適用される。

   This Regulation applies to hosting service providers offering services in the Union, irrespective of their place of main establishment, insofar as they disseminate information to the public.

3. 教育，報道，芸術または調査研究の目的のために，または，公衆の討議における極端な見解，論争となる見解または特異な見解の表現を含め，テロリズムの防止またはそれへの対抗の目的のために，公衆に対して伝達される対象物は，テロリストコンテントと判断されてはならない。評価は，当該伝達の真の目的，及び，それらの目的のために対象物が公衆に対して伝達されるかどうかを決定する。

Material disseminated to the public for educational, journalistic, artistic or research purposes or for the purposes of preventing or countering terrorism, including material which represents an expression of polemic or controversial views in the course of public debate, shall not be considered to be terrorist content. An assessment shall determine the true purpose of that dissemination and whether material is disseminated to the public for those purposes.

4. この規則は，TEU の第 6 条に示す権利，自由及び基本原則を尊重すべき義務を修正する効果をもってはならず，かつ，メディアの自由と多元主義を含め，表現及び情報伝達の自由と関連する基本原則を妨げることなく，適用される。

This Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles referred to in Article 6 TEU and shall apply without prejudice to fundamental principles relating to freedom of expression and information, including freedom and pluralism of the media.

5. この規則は，指令 2000/31/EC を妨げない。指令 2010/13/EU の第 1 条第 1 項(a)に定義する視聴覚メディアサービスに関しては，指令 2010/13/EU が優先する。

This Regulation shall be without prejudice to Directives 2000/31/EC and 2010/13/EU. For audiovisual media services as defined in point (a) of Article 1(1) of Directive 2010/13/EU, Directive 2010/13/EU shall prevail.

第 2 条 定義

Article 2 Definitions

この規則の目的のために，以下の定義が適用される：

(1) 「ホスティングサービスプロバイダ」とは，欧州議会及び理事会の指令(EU) 2015/1535[14]の第 1 条(b)に定義する，コンテント提供者から，その要求により提供された情報の記録保存を組成するサービスのプロバイダのことを意味し；

(2) 「コンテント提供者」とは，ホスティングサービスプロバイダによって記録保存及び公衆

[14] 技術規則の分野及び情報社会サービス関連法の分野における情報提供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).

に対して伝達されている情報，または，記録保存及び公衆に対して伝達された情報を提供した利用者のことを意味し；

(3) 「公衆に対して伝達」とは，潜在的に不特定数の者に対して，コンテント提供者の要求により，情報を利用できるようにすることを意味し；

(4) 「欧州連合内においてサービスを提供する」とは，1 または複数の構成国の自然人または法人に対し，構成国または複数の構成国と実質的な接続をもつホスティングサービスプロバイダのサービスを利用できるようにすることを意味し；

(5) 「実質的な接続」とは，欧州連合内の拠点から生ずる，または，以下のような特別の事実の判断基準から生ずる 1 または複数の構成国との間のホスティングサービスプロバイダの接続のことを意味し；

(a) 1 もしくは複数の構成国においてそのプロバイダのサービスの多数の利用者をもつこと；または

(b) 1 もしくは複数の構成国に対してそのプロバイダの活動の的を絞っていること；

(6) 「テロリスト行為」とは，指令(EU) 2017/541 の第 3 条に定義する侵害行為のことを意味し；

(7) 「テロリストコンテント」とは，1 または複数の以下のタイプの対象物，すなわち，以下の対象物のことを意味し：

(a) そのような対象物が，テロリスト行為の美化による場合のように，直接または間接に，テロリスト行為の実行を鼓舞し，それによって，そのような 1 または複数の侵害行為が実行され得る危険を生じさせている場合，指令(EU) 2017/541 の第 3 条第 1 項の(a)ないし(i)に示す侵害行為のいずれかの実行を扇動する；

(b) 個人または個人のグループに対し，指令(EU) 2017/541 の第 3 条第 1 項の(a)ないし(i)に示す侵害行為のいずれかを実行することを勧誘し，または，その実行に寄与することを勧誘する；

(c) 個人または個人のグループに対し，指令(EU) 2017/541 の第 4 条(b)の意味におけるテロリストグループの活動への参加を勧誘する；

(d) 指令(EU) 2017/541 の第 3 条第 1 項の(a)ないし(i)に示すテロリスト行為のいずれかを実行する目的またはその実行に寄与する目的のために，爆発物，銃器もしくはそれ以外の武器，有害もしくは危険な物質の製造もしくは使用に関する指示，または，それら以外の特別の手法もしくは技法に関する指示を提供する；

(e) 指令(EU) 2017/541 の第 3 条第 1 項の(a)ないし(i)に示す侵害行為のいずれかの実行の脅威を組成する；

(8) 「利用約款」とは，その名称または形態の別に拘らず，ホスティングサービスプロバイダとそのサービスの利用者との間の契約関係を規律する全ての約款，条件及び契約条項のことを意味し；

(9) 「主たる拠点」とは，そのホスティングサービスプロバイダの，最上位の資金決済機能及び業務遂行管理権限のある本店または登録された事務所のことを意味する。

For the purposes of this Regulation, the following definitions apply:

(1) ‘hosting service provider’ means a provider of services as defined in point (b) of Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council [(14)], consisting of the storage of information provided by and at the request of a content provider;

(2) ‘content provider’ means a user that has provided information that is, or that has been, stored and disseminated to the public by a hosting service provider;

(3) ‘dissemination to the public’ means the making available of information, at the request of a content provider, to a potentially unlimited number of persons;

(4) ‘offering services in the Union’ means enabling natural or legal persons in one or more Member States to use the services of a hosting service provider which has a substantial connection to that Member State or those Member States;

(5) ‘substantial connection’ means the connection of a hosting service provider with one or more Member States resulting either from its establishment in the Union or from specific factual criteria, such as:
   (a) having a significant number of users of its services in one or more Member States; or
   (b) the targeting of its activities to one or more Member States;

(6) ‘terrorist offences’ means offences as defined in Article 3 of Directive (EU) 2017/541;

(7) ‘terrorist content’ means one or more of the following types of material, namely material that:
   (a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;
   (b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;
   (c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541;
   (d) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;
   (e) constitutes a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

(8) ‘terms and conditions’ means all terms, conditions and clauses, irrespective of their name or form, which govern the contractual relationship between a hosting service provider and its users;

(9) ‘main establishment’ means the head office or registered office of the hosting service provider within which the principal financial functions and operational control are exercised.

第Ⅱ節 オンラインのテロリストコンテントの伝達に対処するための措置
SECTION II Measures to Address the Dissemination of Terrorist Content Online

第 3 条 削除命令
Article 3 Removal orders

1. 各構成国の職務権限のある機関は，ホスティングサービスプロバイダに対し，テロリストコンテントを削除すること，または，全ての構成国においてテロリストコンテントへのアクセスを不能化することを要求する削除命令を発令する権限をもつ。

   The competent authority of each Member State shall have the power to issue a removal order requiring hosting service providers to remove terrorist content or to disable access to terrorist content in all Member States.

2. 職務権限のある機関がホスティングサービスプロバイダに対して削除命令を発令したことがない場合，その職務権限のある機関は，当該ホスティングサービスプロバイダに対し，その削除命令を発令する少なくとも 12 時間前に，適用可能な手続及び期限に関する情報を提供する。

   Where a competent authority has not previously issued a removal order to a hosting service provider, it shall provide that hosting service provider with information on the applicable procedures and deadlines, at least 12 hours before issuing the removal order.

   第 1 副項は，適正に正当化される緊急の場合においては，適用してはならない。

   The first subparagraph shall not apply in duly justified cases of emergency.

3. ホスティングサービスプロバイダは，可能な限り速やかに，かつ，いかなる場合においてもその削除命令を受領した後 1 時間以内に，テロリストコンテントを削除し，または，全ての構成国においてテロリストコンテントをアクセス不能化する。

   Hosting service providers shall remove terrorist content or disable access to terrorist content in all Member States as soon as possible and in any event within one hour of receipt of the removal order.

4. 職務権限のある機関は，別紙 I に定めるテンプレートを用いて削除命令を発令する。削除命令は，以下の要素を含める：
   (a) 削除命令を発令する職務権限のある機関の識別名の詳細及び当該職務権限のある機関によるその削除命令の認証；
   (b) そのコンテントがテロリストコンテントであると判断されることを説明する十分に詳細な理

由の説明，及び，第 2 条第 7 号に示す対象物の関連タイプの参照；
(c) 正確な統一資源位置指定子（URL），及び，それが必要なときは，テロリストコンテントの識別同定のための付加的な情報；
(d) 削除命令の法的根拠としてのこの規則の参照；
(e) 日付，タイムスタンプ，及び，削除命令を発する職務権限のある機関の電子署名；
(f) その職務権限のある機関に対する救済申立て，裁判所によること，並びに，不服申立の期限に関する情報を含め，ホスティングサービスプロバイダ及びコンテント提供者にとって利用可能な救済に関する容易に理解できる情報；
(g) それが必要かつ適切なときは，第 11 条第 3 項に従い，テロリストコンテントの削除またはアクセス不能化に関する情報を開示しない決定。

Competent authorities shall issue removal orders using the template set out in Annex I. Removal orders shall contain the following elements:
(a) identification details of the competent authority issuing the removal order and authentication of the removal order by that competent authority;
(b) a sufficiently detailed statement of reasons explaining why the content is considered to be terrorist content, and a reference to the relevant type of material referred to in point (7) of Article 2;
(c) an exact uniform resource locator (URL) and, where necessary, additional information for the identification of the terrorist content;
(d) a reference to this Regulation as the legal basis for the removal order;
(e) the date, time stamp and electronic signature of the competent authority issuing the removal order;
(f) easily understandable information about the redress available to the hosting service provider and to the content provider, including information about redress to the competent authority, recourse to a court, as well as the deadlines for appeal;
(g) where necessary and proportionate, the decision not to disclose information about the removal of or disabling of access to terrorist content in accordance with Article 11(3).

5. 職務権限のある機関は，そのホスティングサービスプロバイダの主たる拠点，または，第 17 条に従って指定されたそのプロバイダの法律上の代理者に宛てて削除命令を発する。

The competent authority shall address the removal order to the main establishment of the hosting service provider or to its legal representative designated in accordance with Article 17.

当該職務権限のある機関は，その命令の送受信の日時の正確性を含め，送信者の真正性を確認できる条件の下で，書面による記録を生成可能な電子的手段により，第 15 条第 1 項に示す連絡場所に対してその削除命令を送信する。

That competent authority shall transmit the removal order to the contact point referred to in Article 15(1) by electronic means capable of producing a written record under conditions that allow to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order.

6. ホスティングサービスプロバイダは，不適正な遅滞なく，職務権限のある機関に対し，別紙 II に定めるテンプレートを用いて，とりわけ，当該削除またはアクセス不能化の時を含め，そのテロリストコンテントの削除またはそのテロリストコンテントへの全ての構成国におけるアクセスの不能化を連絡する。

The hosting service provider shall, without undue delay, inform the competent authority, using the template set out in Annex II, of the removal of the terrorist content or the disabling of access to the terrorist content in all Member States, indicating, in particular, the time of that removal or disabling.

7. ホスティングサービスプロバイダが，客観的に正当化し得る技術上の理由または業務遂行上の理由を含め，そのホスティングサービスプロバイダの責に帰さない不可抗力または事実上不可能であることを根拠として，その削除命令を遵守できない場合，そのプロバイダは，不適正な遅滞なく，その削除命令を発令した職務権限のある機関に対し，別紙 III に定めるテンプレートを用いて，それらの根拠を連絡する。

If the hosting service provider cannot comply with the removal order on grounds of *force majeure* or *de facto* impossibility not attributable to the hosting service provider, including for objectively justifiable technical or operational reasons, it shall, without undue delay, inform the competent authority that issued the removal order of those grounds, using the template set out in Annex III.

第 3 項に定める期限は，本項第 1 副項に示す根拠が存在しなくなり次第，その進行を開始させる。

The deadline set out in paragraph 3 shall start to run as soon as the grounds referred to in the first subparagraph of this paragraph have ceased to exist.

8. その命令書が明白な誤りを含んでいるため，または，その命令を執行するための十分な情報を含めていないため，ホスティングサービスプロバイダがその削除命令を遵守できない場合，そのホスティングサービスプロバイダは，不適正な遅滞なく，その削除命令を発令した職務権限のある機関に対して連絡し，かつ，別紙 III に定めるテンプレートを用いて，必要な説明を要求する。

If the hosting service provider cannot comply with the removal order because it contains manifest errors or does not contain sufficient information for its execution, it shall, without undue delay,

inform the competent authority that issued the removal order and request the necessary clarification, using the template set out in Annex III.

第 3 項に定める期限は，そのホスティングサービスプロバイダが必要な説明を受領し次第，その進行を開始させる。

The deadline set out in paragraph 3 shall start to run as soon as the hosting service provider has received the necessary clarification.

9. 削除命令は，国内法に従って不服が申立てられなかった場合，その不服申立期間の満了により，または，不服申立後の有効性確認により確定する。

A removal order shall become final upon the expiry of the deadline for appeal where no appeal has been lodged in accordance with national law or upon confirmation following an appeal.

削除命令が確定する場合，その削除命令を発令した職務権限のある機関は，そのホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者の居住地もしくは拠点がある構成国の第 12 条第 1 項(c)に示す職務権限のある機関に対し，そのことを連絡する。

When the removal order becomes final, the competent authority that issued the removal order shall inform the competent authority referred to in point (c) of Article 12(1) of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established of that fact.

第 4 条　国境を越える削除命令に関する手続

Article 4 Procedure for cross-border removal orders

1. 第 3 条に服して，ホスティングサービスプロバイダが，その削除命令を発令した職務権限のある機関の構成国内にその主たる拠点または法律上の代理者をもたない場合，当該機関は，同時に，そのホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者の居住地もしくは拠点がある構成国の職務権限のある機関に対し，その削除命令の副本を送付する。

Subject to Article 3, where the hosting service provider does not have its main establishment or legal representative in the Member State of the competent authority that issued the removal order, that authority shall, simultaneously, submit a copy of the removal order to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established.

2. ホスティングサービスプロバイダが本条に示す削除命令を受領したときは，そのプロバイダは，第 3 条に示す措置を講じ，かつ，本条第 7 条に従い，そのコンテントまたはそれへのアクセスを回復できるようにするために必要となる措置を講ずる。

Where a hosting service provider receives a removal order as referred to in this Article, it shall take the measures provided for in Article 3 and take the necessary measures to be able to reinstate the content or access thereto, in accordance with paragraph 7 of this Article.

3. そのホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者の居住地もしくは拠点がある構成国の職務権限のある機関は，その機関自身の発意により，第 1 項に従った削除命令の副本の受領後 72 時間以内に，その削除命令がこの規則または憲章によって保障されている基本的な権利及び自由に重大に違反または明白に違反しているかどうかを判断するため，その削除命令を精査する。

The competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established may, on its own initiative, within 72 hours of receiving the copy of the removal order in accordance with paragraph 1, scrutinise the removal order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter.

その機関が，違反していると判断するときは，その機関は，同一の期間内に，その旨の理由を付した決定を採択する。

Where it finds an infringement, it shall, within the same period, adopt a reasoned decision to that effect.

4. ホスティングサービスプロバイダ及びコンテント提供者は，削除命令または第 11 条第 2 項による情報のいずれかの受領から 48 時間以内に，そのホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者の居住地もしくは拠点がある構成国の職務権限のある機関に対し，本条第 3 項第 1 副項に示す削除命令の精査を求める理由を付した要請書を提出する権利をもつ。

Hosting service providers and content providers shall have the right to submit, within 48 hours of receiving either a removal order or information pursuant to Article 11(2), a reasoned request to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established to scrutinise the removal order as referred to in the first subparagraph of paragraph 3 of this Article.

職務権限のある機関は，その要請書の受領から 72 時間以内に，違反が存在するか否かに

関するその機関の判断を示し，その機関によるその削除命令の精査後の理由を付した決定を採択する。

The competent authority shall, within 72 hours of receiving the request, adopt a reasoned decision following its scrutiny of the removal order, setting out its findings as to whether there is an infringement.

5. 職務権限のある機関は，第 3 項第 2 副項による決定または第 4 項第 2 副項による違反と判断する決定を採択する前に，その削除命令を発令した職務権限のある機関に対し，その決定を採択する予定であること及びその機関がそのようにする理由を連絡する。

The competent authority shall, before adopting a decision pursuant to the second subparagraph of paragraph 3 or a decision finding an infringement pursuant to the second subparagraph of paragraph 4, inform the competent authority that issued the removal order of its intention to adopt the decision and of its reasons for doing so.

6. そのホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者の居住地もしくは拠点がある構成国の職務権限のある機関が，本条の第 3 項または第 4 項に従って理由を付した決定を採択する場合，その機関は，遅滞なく，その削除命令を発令した職務権限のある機関，ホスティングサービスプロバイダ，本条の第 4 項により精査を要請したコンテント提供者，及び，第 14 条に従い，Europol に対し，当該決定を通知する。その決定が，本条の第 3 項または第 4 項により違反があると判断する場合，その削除命令は，その法的効果をもつことを終える。

Where the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established adopts a reasoned decision in accordance with paragraph 3 or 4 of this Article, it shall, without delay, communicate that decision to the competent authority that issued the removal order, the hosting service provider, the content provider who requested the scrutiny pursuant to paragraph 4 of this Article and, in accordance with Article 14, Europol. Where the decision finds an infringement pursuant to paragraph 3 or 4 of this Article, the removal order shall cease to have legal effects.

7. 第 6 項に従って通知された違反があると判断する決定の受領の後，関係するホスティングサービスプロバイダは，欧州連合法及び国内法に従ってそのプロバイダの利用約款を執行できることを妨げず，直ちに，そのコンテントまたはそのコンテントへのアクセスを回復する。

Upon receiving a decision finding an infringement communicated in accordance with paragraph 6, the hosting service provider concerned shall immediately reinstate the content or access thereto, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and

national law.

第 5 条 特別の措置
Article 5 Specific measures

1. 第 4 項に示すテロリストコンテントの危険に晒されているホスティングサービスプロバイダは，それが可能なときは，テロリストコンテントの公衆に対する伝達のためのそのプロバイダのサービスの濫用に対処するための条項を，そのプロバイダの利用約款の中に含め，かつ，その条項を適用する。

A hosting service provider exposed to terrorist content as referred to in paragraph 4 shall, where applicable, include in its terms and conditions and apply provisions to address the misuse of its services for the dissemination to the public of terrorist content.

そのホスティングサービスプロバイダは，テロリストコンテントではない対象物の削除を避けるため，全ての状況において，利用者の基本的な権利を適正に考慮し，かつ，とりわけ，開かれた民主主義社会における表現及び情報伝達の自由の基本的な重要性を考慮に入れた上で，勤勉であり，比例的であり，かつ，非差別の態様で，そのようにする。

It shall do so in a diligent, proportionate and non-discriminatory manner, with due regard, in all circumstances, to the fundamental rights of the users and taking into account, in particular, the fundamental importance of the freedom of expression and information in an open and democratic society, with a view to avoiding the removal of material which is not terrorist content.

2. 第 4 項に示すテロリストコンテントの危険に晒されているホスティングサービスプロバイダは，テロリストコンテントの公衆に対する伝達に抗してそのプロバイダのサービスを防護するための特別の措置を講ずる。

A hosting service provider exposed to terrorist content as referred to in paragraph 4 shall take specific measures to protect its services against the dissemination to the public of terrorist content.

特別の措置の選択に関する判断は，そのホスティングサービスプロバイダに任される。そのような措置は，以下の 1 または複数のものを含め得る：

(a) テロリストコンテントを識別同定し，迅速に削除またはアクセス不能化するための適切な職員配置または技術的措置のような，適切な技術上及び運用上の措置または能力；
(b) テロリストコンテントであると主張するコンテントをそのホスティングサービスプロバイダに対して通報または警報するための容易にアクセス可能かつユーザフレンドリな仕組み；
(c) 利用者の節度監視のための仕組みのような，そのプロバイダのサービス上にあるテロリ

ストコンテントの覚知を増加させるための上記以外の仕組み；
(d) そのプロバイダのサービス上にあるテロリストコンテントの可用性に対処するために適切であるとそのホスティングサービスプロバイダが判断する上記以外の措置。

The decision as to the choice of specific measures shall remain with the hosting service provider. Such measures may include one or more of the following:
(a) appropriate technical and operational measures or capacities, such as appropriate staffing or technical means to identify and expeditiously remove or disable access to terrorist content;
(b) easily accessible and user-friendly mechanisms for users to report or flag to the hosting service provider alleged terrorist content;
(c) any other mechanisms to increase the awareness of terrorist content on its services, such as mechanisms for user moderation;
(d) any other measure that the hosting service provider considers to be appropriate to address the availability of terrorist content on its services.

3. 特別の措置は，以下の要件の全てに適合するものとする：
(a) それらの措置が，そのホスティングサービスプロバイダのサービスがテロリストコンテントの危険に晒されているレベルの緩和において実効的であること；
(b) それらの措置が，とりわけ，そのホスティングサービスプロバイダのサービスがテロリストコンテントの危険に晒されているレベルの重大性，並びに，技術上及び運用上の能力，資金力，ホスティングサービスプロバイダのサービスの利用者数，及び，そのプロバイダが提供するコンテントの分量を考慮に入れた上で，的を絞ったものであり，かつ，比例的なものであること；
(c) それらの措置が，利用者の権利及び正当な利益，とりわけ，表現及び情報提供の自由，私生活の尊重，及び，個人データの保護と関係する利用者の基本的な権利を考慮に入れた態様で適用されること；
(d) それらの措置が，勤勉かつ非差別の態様で適用されること。

Specific measures shall meet all of the following requirements:
(a) they shall be effective in mitigating the level of exposure of the services of the hosting service provider to terrorist content;
(b) they shall be targeted and proportionate, taking into account, in particular, the seriousness of the level of exposure of the services of the hosting service provider to terrorist content as well as the technical and operational capabilities, financial strength, the number of users of the services of the hosting service provider and the amount of content they provide;
(c) they shall be applied in a manner that takes full account of the rights and legitimate interest of the users, in particular users' fundamental rights concerning freedom of expression and information, respect for private life and protection of personal data;
(d) they shall be applied in a diligent and non-discriminatory manner.

特別の措置が技術手段の利用を含むものである場合，正確性を確保するため，及び，テロリストコンテントではない対象物の削除を避けるため，とりわけ，人間による監視及び憲章による，適切かつ実効的な安全確保が提供されるものとする。

Where specific measures involve the use of technical measures, appropriate and effective safeguards, in particular through human oversight and verification, shall be provided to ensure accuracy and to avoid the removal of material that is not terrorist content.

4. そのホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者の居住地もしくは拠点がある構成国の職務権限のある機関が，以下のことを実施した場合，そのホスティングサービスプロバイダは，テロリストコンテントの危険に晒されているものとする：
   (a) そのホスティングサービスプロバイダが過去 12 か月間に 2 以上の確定削除命令を受けたことのような，客観的な要素を基礎として，そのホスティングサービスプロバイダがテロリストコンテントの危険に晒されていると判断する決定をし；かつ，
   (b) そのホスティングサービスプロバイダに対し，(a)に示す決定を通知した場合。

   A hosting service provider is exposed to terrorist content where the competent authority of the Member State of its main establishment or where its legal representative resides or is established has:
   (a) taken a decision, on the basis of objective factors, such as the hosting service provider having received two or more final removal orders in the previous 12 months, finding that the hosting service provider is exposed to terrorist content; and
   (b) notified the decision referred to in point (a) to the hosting service provider.

5. 第 4 項に示す決定，または，それが関連するときは，第 6 項に示す決定を受けた後，ホスティングサービスプロバイダは，職務権限のある機関に対し，第 2 項及び第 3 項を遵守するためにそのプロバイダが講じた特別の措置及びそのプロバイダが講ずる予定の特別の措置を報告する。そのプロバイダは，その決定の受領から 3 か月以内に，及び，その後は年次で，そのようにする。当該義務は，第 7 条による要請に応じて，そのホスティングサービスプロバイダがテロリストコンテントの危険に晒されなくなった旨をその職務権限のある機関が決定した時に終了する。

   After having received a decision as referred to in paragraph 4 or, where relevant, paragraph 6, a hosting service provider shall report to the competent authority on the specific measures that it has taken and that it intends to take in order to comply with paragraphs 2 and 3. It shall do so within three months of receipt of the decision and on an annual basis thereafter. That obligation shall cease once the competent authority has decided, upon request pursuant to paragraph 7, that the hosting service provider is no longer exposed to terrorist content.

6. 第 5 項に示す報告を基礎として，及び，それが関連するときは，その他の客観的な要素を基礎として，その特別の措置が第 2 項及び第 3 項を遵守していないと職務権限のある機関が判断する場合，当該職務権限のある機関は，そのホスティングサービスプロバイダに対し，第 2 項及び第 3 項が遵守されることを確保するために必要となる措置をそのプロバイダが講じることを要求する決定を発する。

Where, based on the reports referred to in paragraph 5 and, where relevant, any other objective factors, the competent authority considers that the specific measures taken do not comply with paragraphs 2 and 3, that competent authority shall address a decision to the hosting service provider requiring it to take the necessary measures so as to ensure that paragraphs 2 and 3 are complied with.

ホスティングサービスプロバイダは，講じられる特別の措置のタイプを選択できる。

The hosting service provider may choose the type of specific measures to take.

7. ホスティングサービスプロバイダは，いつでも，職務権限のある機関に対し，第 4 項または第 6 項による決定の見直し，及び，それが適切なときは，変更または取消しを要求できる。

A hosting service provider may, at any time, request the competent authority to review and, where appropriate, amend or revoke a decision as referred to in paragraph 4 or 6.

職務権限のある機関は，その要求の受領から 3 か月以内に，客観的な要素を基礎として，その要求に関する理由を付した決定を採択し，かつ，そのホスティングサービスプロバイダに対し，その決定を通知する。

The competent authority shall, within three months of receipt of the request, adopt a reasoned decision on the request based on objective factors and notify the hosting service provider of that decision.

8. 特別の措置を講ずることを求める要件は，指令 2000/31/EC の第 15 条第 1 項を妨げず，かつ，そのプロバイダが送信または記録保存する情報を監視すべきホスティングサービスプロバイダの一般的義務，及び，違法な活動を示す事実または情報を積極的に探索すべき一般的な義務を伴うものとしてはならない。

Any requirement to take specific measures shall be without prejudice to Article 15(1) of Directive 2000/31/EC and shall entail neither a general obligation for hosting services providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

特別の措置を講ずることを求める要件は，ホスティングサービスプロバイダによる自動化されたツールの利用の義務を含めてはならない。

Any requirement to take specific measures shall not include an obligation to use automated tools by the hosting service provider.

第 6 条 コンテント及び関連データの保全

Article 6 Preservation of content and related data

1. ホスティングサービスプロバイダは，削除命令の結果として，または，第 3 条もしくは第 5 条による特別の措置の結果として，削除されまたはそのアクセスが不能化されたテロリストコンテント，並びに，そのようなテロリストコンテントの削除の結果として削除された関連データであって，以下のために必要なものを保全する：
   (a) テロリストデータ及び関連データの削除もしくはアクセス不能化の決定を不服とする行政上もしくは法務上の見直し手続，または，第 10 条に基づく不服申立ての取扱い；または
   (b) テロリスト行為の防止，検知，捜査及び訴追。

   Hosting service providers shall preserve terrorist content which has been removed or access to which has been disabled as a result of a removal order, or of specific measures pursuant to Article 3 or 5, as well as any related data removed as a consequence of the removal of such terrorist content, which are necessary for:
   (a) administrative or judicial review proceedings or complaint-handling under Article 10 against a decision to remove or disable access to terrorist content and related data; or
   (b) the prevention, detection, investigation and prosecution of terrorist offences.

2. 第 1 項に示すテロリストコンテント及び関連データは，その削除またはアクセス不能化から 6 か月間保全される。テロリストコンテントは，第 1 項(a)に示す現在進行中の行政上または法務上の見直し手続のために必要となる長さの期間に限り，職務権限のある機関または裁判所からの要求に応じて，指定された期間，更に保全される。

   The terrorist content and related data, as referred to in paragraph 1, shall be preserved for six months from the removal or disabling. The terrorist content shall, upon request from the competent authority or court, be preserved for a further specified period only if and for as long as necessary for ongoing administrative or judicial review proceedings, as referred to in point (a) of paragraph 1.

3. ホスティングサービスプロバイダは，第 1 項により保全されたテロリストコンテント及び関連データが，技術上及び組織上の適切な安全確保に服することを確保する。

Hosting service providers shall ensure that the terrorist content and related data preserved pursuant to paragraph 1 are subject to appropriate technical and organisational safeguards.

それらの技術上及び組織上の安全確保は，保全されたテロリストコンテント及び関連データが，第 1 項に示す目的に限りアクセス及び処理されることを確保し，かつ，関係する個人データの高いレベルの安全性を確保する。ホスティングサービスプロバイダは，それが必要なときは，それらの安全確保を見直し，アップデートする。

Those technical and organisational safeguards shall ensure that the terrorist content and related data preserved are accessed and processed only for the purposes referred to in paragraph 1, and ensure a high level of security of the personal data concerned. Hosting service providers shall review and update those safeguards where necessary.

第Ⅲ節　安全確保及び説明責任

Section III Safeguards and Accountability

第 7 条　ホスティングサービスプロバイダの透明性義務

Article 7 Transparency obligations for hosting service providers

1. ホスティングサービスプロバイダは，そのプロバイダの利用約款の中で，それが適用可能なときは，自動化されたツールを含め，それが適切なときは，特別の措置の機能に関する意味のある説明を含め，テロリストコンテントの伝達に対処するためのそのプロバイダの基本方針を明確に定める。

   Hosting service providers shall set out clearly in their terms and conditions their policy for addressing the dissemination of terrorist content, including, where appropriate, a meaningful explanation of the functioning of specific measures, including, where applicable, the use of automated tools.

2. 当の暦年内において，テロリストコンテントの伝達に対処するための行動を行ったホスティングサービスプロバイダ，または，この規則による行動を行うことを要求されたホスティングサービスプロバイダは，当該年におけるそれらの行動に関する透明性報告書を公表する。そのプロバイダは，翌年の 3 月 1 日よりも前に，その報告書を刊行する。

   A hosting service provider that has taken action to address the dissemination of terrorist content or has been required to take action pursuant to this Regulation in a given calendar year, shall make publicly available a transparency report on those actions for that year. It shall publish that report before 1 March of the following year.

3. 透明性報告書は，少なくとも，以下の情報を含める：

(a) テロリストコンテントの識別同定及び削除またはアクセス不能化と関係するそのホスティングサービスプロバイダの措置に関する情報；
(b) とりわけ，自動化されたツールが使用された場合において，そのコンテントがテロリストコンテントであると判断されたことにより以前に削除されまたはそのアクセスが不能化された対象物のオンラインの再出現に対処するためのそのホスティングサービスプロバイダの措置に関する情報；
(c) 削除命令または特別の措置に従って削除されまたはそのアクセスが不能化されたテロリストコンテントの数，並びに，その根拠と共に，第 3 条第 7 項第 1 副項及び第 3 条第 8 項第 1 副項により，そのコンテントが削除またはそのアクセスが不能化されなかった削除命令の数；
(d) 第 10 条に従ってそのホスティングサービスプロバイダによって取り扱われた不服申立の数及びその結果；
(e) そのホスティングサービスプロバイダによって申立てられた行政上または法務上の見直しの数及びその結果；
(f) 行政上または法務上の見直し手続の結果として，そのホスティングサービスプロバイダがコンテントまたはそのアクセスの回復を要求された案件の数；
(g) コンテント提供者による不服申立てに従って，そのホスティングサービスプロバイダがコンテントまたは曾のアクセスを回復した案件の数。

Transparency reports shall include at least the following information:
(a) information about the hosting service provider's measures in relation to the identification and removal of or disabling of access to terrorist content;
(b) information about the hosting service provider's measures to address the reappearance online of material which has previously been removed or to which access has been disabled because it was considered to be terrorist content, in particular where automated tools have been used;
(c) the number of items of terrorist content removed or to which access has been disabled following removal orders or specific measures, and the number of removal orders where the content has not been removed or access to which has not been disabled pursuant to the first subparagraph of Article 3(7) and the first subparagraph of Article 3(8), together with the grounds therefor;
(d) the number and the outcome of complaints handled by the hosting service provider in accordance with Article 10;
(e) the number and the outcome of administrative or judicial review proceedings brought by the hosting service provider;
(f) the number of cases in which the hosting service provider was required to reinstate content or access thereto as a result of administrative or judicial review proceedings;
(g) the number of cases in which the hosting service provider reinstated content or access thereto following a complaint by the content provider.

第 8 条 職務権限のある機関の透明性報告書

Article 8 Competent authorities' transparency reports

1. 職務権限のある機関は，この規則に基づくその機関の活動に関する年次透明性報告書を刊行する。それらの報告書は，少なくとも，当暦年との関係における以下の情報を含める：
   (a) 第 4 条第 1 項に服する削除命令の数，第 4 条に基づいて精査された削除命令の数，並びに，テロリストコンテントが削除されまたはそのアクセスが不能化された案件の数及びテロリストコンテントが削除されまたはそのアクセスが不能化されなかった案件の数を含め，関係するホスティングサービスプロバイダによるそれらの削除命令の実装に関する情報を示して，第 3 条に基づいて発令された削除命令の数；
   (b) 第 5 条第 4 項，第 6 項または第 7 項に従って行われた決定の数，及び，特別の措置の記述を含め，ホスティングサービスプロバイダによるそれらの決定の実装に関する情報；
   (c) 削除命令並びに第 5 条第 4 項及び第 6 項に従って行われた決定が行政上または法務上の見直し手続に服した案件の数，並びに，それぞれの手続の結果に関する情報；
   (d) 第 18 条による制裁を科す決定の数，及び，科された制裁のタイプの記述。

   Competent authorities shall publish annual transparency reports on their activities under this Regulation. Those reports shall include at least the following information in relation to the given calendar year:
   (a) the number of removal orders issued under Article 3, specifying the number of removal orders subject to Article 4(1), the number of removal orders scrutinised under Article 4, and information on the implementation of those removal orders by the hosting service providers concerned, including the number of cases in which terrorist content was removed or access thereto was disabled and the number of cases in which terrorist content was not removed or access thereto was not disabled;
   (b) the number of decisions taken in accordance with Article 5(4), (6) or (7), and information on the implementation of those decisions by hosting service providers, including a description of the specific measures;
   (c) the number of cases in which removal orders and decisions taken in accordance with Article 5(4) and (6) were subject to administrative or judicial review proceedings and information on the outcome of the relevant proceedings;
   (d) the number of decisions imposing penalties pursuant to Article 18, and a description of the type of penalty imposed.

2. 第 1 項に示す年次透明性報告書は，テロリスト行為の防止，検知，捜査または訴追のために現在進行中の活動または国家安全保障上の利益を妨げ得る情報を含めてはならない。

   The annual transparency reports referred to in paragraph 1 shall not include information that may

prejudice ongoing activities for the prevention, detection, investigation or prosecution of terrorist offences or interests of national security.

第 9 条 救済

Article 9 Remedies

1. 第 3 条第 1 項により発令された削除命令，または，第 4 条第 4 項または第 5 条第 4 項，第 6 項もしくは第 7 項による決定を受領したホスティングサービスプロバイダは，実効的な救済の権利をもつ。その権利は，その削除命令を発令した職務権限のある機関の構成国の裁判所においてそのような削除命令に対して不服を申立てる権利，及び，その決定を行った職務権限のある機関の構成国の裁判所において第 4 条第 4 項または第 5 条第 4 項，第 6 項もしくは第 7 項による決定に対して不服を申立てる権利を含む。

   Hosting service providers that have received a removal order issued pursuant to Article 3(1) or a decision pursuant to Article 4(4) or to Article 5(4), (6) or (7), shall have a right to an effective remedy. That right shall include the right to challenge such a removal order before the courts of the Member State of the competent authority that issued the removal order and the right to challenge the decision pursuant to Article 4(4) or to Article 5(4), (6) or (7), before the courts of the Member State of the competent authority that took the decision.

2. 削除命令に従ってそのコンテントが削除またはそのアクセスが不能化されたコンテント提供者は，実効的な救済の権利をもつ。その権利は，その削除命令を発令した職務権限のある機関の構成国の裁判所において第 3 条第 1 項により発令された削除命令に対して不服を申立てる権利，及び，その決定を行った職務権限のある機関の構成国の裁判所において第 4 条第 4 項による決定に対して不服を申立てる権利を含む。

   Content providers whose content has been removed or access to which has been disabled following a removal order shall have the right to an effective remedy. That right shall include the right to challenge a removal order issued pursuant to Article 3(1) before the courts of the Member State of the competent authority that issued the removal order and the right to challenge a decision pursuant to Article 4(4) before the courts of the Member State of the competent authority that took the decision.

3. 構成国は，本条に示す権利の行使のための実効的な手続を設ける。

   Member States shall put in place effective procedures for exercising the rights referred to in this Article.

第 10 条　不服申立の仕組み

Article 10 Complaint mechanisms

1. 各ホスティングサービスプロバイダは，そのコンテントが第 5 条による特別の措置の結果として削除またはそのアクセスが不能化されたコンテント提供者が，そのコンテントまたはそのアクセスの回復を要求して，当該削除またはアクセス不能化に関する不服を申立てることができるようにする実効的かつアクセス可能な仕組みを設ける。

   Each hosting service provider shall establish an effective and accessible mechanism allowing content providers where their content has been removed or access thereto has been disabled as a result of specific measures pursuant to Article 5 to submit a complaint concerning that removal or disabling, requesting the reinstatement of the content or of access thereto.

2. 各ホスティングサービスプロバイダは，第 1 項に示す仕組みを介してそのプロバイダが受けた全ての不服申立てを迅速に吟味し，かつ，そのコンテントの削除またはそのアクセス不能化が正当化されない場合，不適切な遅滞なく，そのコンテントまたはそのアクセスを回復する。そのホスティングサービスプロバイダは，その不服申立者に対し，その不服申立てを受けた時から 2 週間以内に，その不服申立ての結果を連絡する。

   Each hosting service provider shall expeditiously examine all complaints that it receives through the mechanism referred to in paragraph 1 and reinstate the content or access thereto, without undue delay, where its removal or disabling of access thereto was unjustified. It shall inform the complainant of the outcome of the complaint within two weeks of the receipt thereof.

   その不服申立てが排斥される場合，そのホスティングサービスプロバイダは，その不服申立者に対し，その判断の理由を提供する。

   Where the complaint is rejected, the hosting service provider shall provide the complainant with the reasons for its decision.

   コンテントまたはそのアクセスの回復は，そのホスティングサービスプロバイダまたは職務権限のある機関の決定に対して不服申立てする行政上または法務上の見直し手続を排除してはならない。

   A reinstatement of content or of access thereto shall not preclude administrative or judicial review proceedings challenging the decision of the hosting service provider or of the competent authority.

第 11 条 コンテント提供者に対する情報提供

Article 11 Information to content providers

1. ホスティングサービスプロバイダがテロリストコンテントを削除またはアクセス不能化する場合，そのホスティングサービスプロバイダは，そのコンテント提供者に対し，そのような削除またはアクセス不能化に関する情報を利用できるようにする。

   Where a hosting service provider removes or disables access to terrorist content, it shall make available to the content provider information on such removal or disabling.

2. そのコンテント提供者の要求に応じて，そのホスティングサービスプロバイダは，そのコンテント提供者に対し，削除もしくはアクセス不能化の理由及びその削除命令に対してそのコンテント提供者が不服を申立てる権利を連絡し，または，そのコンテント提供者に対し，その削除命令の写しを提供する。

   Upon request of the content provider, the hosting service provider shall either inform the content provider of the reasons for the removal or disabling and its rights to challenge the removal order or provide the content provider with a copy of the removal order.

3. その削除命令を発令した職務権限のある機関が，テロリスト行為の防止，捜査，検知及び訴追のような，公共の保安を理由として不開示とすることが必要かつ適切であると判断する場合，それが必要な長さの期間，ただし，当該決定から 6 週間を超えない間，第 1 項及び第 2 項による義務を適用してはならない。そのような場合，そのホスティングサービスプロバイダは，テロリストコンテントの削除またはアクセス不能化に関する情報を開示してはならない。

   The obligation pursuant to paragraphs 1 and 2 shall not apply where the competent authority issuing the removal order decides that it is necessary and proportionate that there be no disclosure for reasons of public security, such as the prevention, investigation, detection and prosecution of terrorist offences, for as long as necessary, but not exceeding six weeks from that decision. In such a case, the hosting service provider shall not disclose any information on the removal or disabling of access to terrorist content.

   職務権限のある機関は，そのような不開示が正当化され続けている場合，更に 6 週間までその期間を延長できる。

   That competent authority may extend that period by a further six weeks, where such non-disclosure continues to be justified.

第IV節　職務権限のある機関及び協力
Section IV Competent Authorities and Cooperation

第 12 条　職務権限のある機関の指定
Article 12 Designation of competent authorities

1. 各構成国は，以下のための職務権限のある機関を指定する：
   (a) 第 3 条により削除命令を発令すること；
   (b) 第 4 条により削除命令を精査すること；
   (c) 第 5 条により特別の措置の実装を監督すること；
   (d) 第 18 条により制裁を科すこと。

   Each Member State shall designate the authority or authorities competent to:
   (a) issue removal orders pursuant to Article 3;
   (b) scrutinise removal orders pursuant to Article 4;
   (c) oversee the implementation of specific measures pursuant to Article 5;
   (d) impose penalties pursuant to Article 18.

2. 各構成国は，当該職務権限のある機関によって発令された削除命令との家系において説明及びフィードバックを求める要求を取り扱うため，第 1 項(a)に示す職務権限のある機関の中に，連絡部局が指定または設置されることを確保する。

   Each Member State shall ensure that a contact point is designated or established within the competent authority referred to in point (a) of paragraph 1 to handle requests for clarification and feedback in relation to removal orders issued by that competent authority.

   構成国は，連絡部局に関する情報が公表されることを確保する。

   Member States shall ensure that the information on the contact point is made publicly available.

3. 2022 年 6 月 7 日までに，構成国は，欧州委員会に対し，第 1 項に示す職務権限のある機関及びその変更を通知する。欧州委員会は，EU 官報上において，その通知及びその変更を公表する。

   By 7 June 2022, Member States shall notify the Commission of the competent authority or authorities referred to in paragraph 1 and any modification thereof. The Commission shall publish the notification and any modification thereto in the *Official Journal of the European Union*.

4. 2022 年 6 月 7 日までに，欧州委員会は，第 1 項に示す職務権限のある機関及び各職務権

限のある機関のための第 2 項により指定または設置される連絡部局を列挙するオンラインの登録簿を設置する。欧州委員会は，その登録簿の変更を定期的に公表する。

By 7 June 2022, the Commission shall set up an online register listing the competent authorities referred to in paragraph 1 and the contact point designated or established pursuant to paragraph 2 for each competent authority. The Commission shall publish any modification thereto regularly.

第 13 条 職務権限のある機関

Article 13 Competent authorities

1. 構成国は，その構成国の職務権限のある機関が，この規則の狙いを達成し，この規則に基づくその機関の義務を履行するために必要となる権限及び十分な資源をもつことを確保する。

Member States shall ensure that their competent authorities have the necessary powers and sufficient resources to achieve the aims of and fulfil their obligations under this Regulation.

2. 構成国は，その構成国の職務権限のある機関が，基本的な権利を完全に尊重しつつ，客観的かつ非差別の態様でこの規則に基づくその機関の職務を遂行することを確保する。職務権限のある機関は，第 12 条第 1 項に基づくその機関の職務の遂行との関係において，他の組織に指示を求めてはならず，かつ，他の組織から指示を受けてはならない。

Member States shall ensure that their competent authorities carry out their tasks under this Regulation in an objective and non-discriminatory manner while fully respecting fundamental rights. Competent authorities shall not seek or take instructions from any other body in relation to the carrying out of their tasks under Article 12(1).

第 1 副項は，国内憲法に従った監督を排除してはならない。

The first subparagraph shall not prevent supervision in accordance with national constitutional law.

第 14 条 ホスティングサービスプロバイダ，職務権限のある機関及び Europol の間の協力

Article 14 Cooperation between hosting service providers, competent authorities and Europol

1. 職務権限のある機関は，削除命令に関し，とりわけ，仕事の重複を避け，調整を拡大し，かつ，異なる構成国内の捜査への干渉を避けるため，相互に，及び，それが適切なときは，Europol との間で，情報を交換し，調整及び協力する。

Competent authorities shall exchange information, coordinate and cooperate with each other and,

where appropriate, with Europol, with regard to removal orders, in particular to avoid duplication of effort, enhance coordination and avoid interference with investigations in different Member States.

2. 構成国の職務権限のある機関は，第 5 条により講じられる特別の措置及び第 18 条により科される制裁に関し，第 12 条第 1 項の(c)及び(d)に示す職務権限のある機関との間で情報を交換し，調整及び協力する。構成国は，第 12 条第 1 項の(c)及び(d)に示す職務権限のある機関が，全ての関連情報を保有することを確保する。

Competent authorities of Member States shall exchange information, coordinate and cooperate with the competent authorities referred to in points (c) and (d) of Article 12(1) with regard to specific measures taken pursuant to Article 5 and penalties imposed pursuant to Article 18. Member States shall ensure that the competent authorities referred to in points (c) and (d) of Article 12(1) are in possession of all the relevant information.

3. 第 1 項の目的のために，構成国は，適時の態様で関連情報が交換されることを確保するための適切かつ安全な通信経路または仕組みを定める。

For the purposes of paragraph 1, Member States shall provide for the appropriate and secure communication channels or mechanisms to ensure that the relevant information is exchanged in a timely manner.

4. この規則の実効的な実装のため，及び，仕事の重複を避けるため，構成国及びホスティングサービスプロバイダは，とりわけ，以下のことを容易にするため，Europol によって作成されたツールを含め，専用のツールを活用できる：
   (a) 第 3 条による削除命令と関連する処理及びフィードバック；並びに
   (b) 第 5 条による特別の措置を識別及び実装するための協力。

For the effective implementation of this Regulation as well as to avoid duplication of effort, Member States and hosting service providers may make use of dedicated tools, including those established by Europol, to facilitate in particular:
   (a) the processing and feedback relating to removal orders pursuant to Article 3; and
   (b) cooperation with a view to identifying and implementing specific measures pursuant to Article 5.

5. ホスティングサービスプロバイダが，生命に対する差し迫った危険を含め，テロリストコンテントに気づいたときは，そのプロバイダは，直ちに，関係する構成国の犯罪行為の捜査及び訴追に関して職責を負う機関に対し，連絡する。そのホスティングサービスプロバイダが，関係する構成国を識別できない場合，そのホスティングサービスプロバイダは，そのホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理

者の居住地もしくは拠点がある構成国の第 12 条第 2 項による連絡部局に対して通知し，かつ，適切な事後対応のために，Europol に対し，当該テロリストコンテントに関する情報を送信する。

Where hosting service providers become aware of terrorist content involving an imminent threat to life, they shall promptly inform authorities competent for the investigation and prosecution of criminal offences in the Member States concerned. Where it is impossible to identify the Member States concerned, the hosting service providers shall notify the contact point pursuant to Article 12(2) in the Member State where they have their main establishment or where their legal representative resides or is established, and transmit information concerning that terrorist content to Europol for appropriate follow-up.

6. 職務権限のある機関は，この規則によるテロリストコンテントの削除またはそのアクセス不能化の命令に服するテロリストコンテントのタイプの分析を含む年次報告書を Europol が提供できるようにするため，Europol に対し，削除命令の副本を送付することが推奨される。

The competent authorities are encouraged to send copies of the removal orders to Europol to allow it to provide an annual report that includes an analysis of the types of terrorist content subject to an order to remove it or to disable access thereto pursuant to this Regulation.

第 15 条 ホスティングサービスプロバイダの連絡場所

Article 15 Hosting service providers' contact points

1. 各ホスティングサービスプロバイダは，第 3 条及び第 4 条により，電子的な手段により削除命令を受領し，その命令を迅速に処理するための連絡場所を指定または設置する。そのホスティングサービスプロバイダは，その連絡場所に関する情報が公表されることを確保する。

Each hosting service provider shall designate or establish a contact point for the receipt of removal orders by electronic means and their expeditious processing pursuant to Articles 3 and 4. The hosting service provider shall ensure that information about the contact point is made publicly available.

2. 本条第 1 項に示す情報は，連絡場所がその言語に対処でき，かつ，第 3 条による削除命令と関連してその言語で更に意見交換が行われる，規則 1/58[15]に示す欧州連合の機関の公用語を指定する。それらの言語は，そのホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者の居住地もしくは拠点がある構成国の公用語中の少なくとも 1 つを含める。

[15] 欧州経済共同体によって使用される言語を定める規則第 1 号 (OJ 17, 6.10.1958, p. 385).

The information referred to in paragraph 1 of this Article shall specify the official languages of the Union institutions referred to in Regulation 1/58 [15] in which the contact point can be addressed and in which further exchanges in relation to removal orders pursuant to Article 3 are to take place. Those languages shall include at least one of the official languages of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established.

第Ⅴ節 実装及び執行
Section V Implementation and Enforcement

第 16 条 裁判管轄権
Article 16 Jurisdiction

1. ホスティングサービスプロバイダの主たる拠点の構成国は，第 5 条，第 18 条及び第 21 条による裁判管轄権をもつ。欧州連合内においてその主たる拠点をもたないホスティングサービスプロバイダは，そのプロバイダの法律上の代理者の居住地または拠点がある構成国の裁判管轄権の下にあるものと推定される。

   The Member State of the main establishment of the hosting service provider shall have jurisdiction for the purposes of Articles 5, 18 and 21. A hosting service provider which does not have its main establishment within the Union shall be deemed to be under the jurisdiction of the Member State where its legal representative resides or is established.

2. 欧州連合内においてその主たる拠点をもたないホスティングサービスプロバイダが法律上の代理者を指定しない場合，全ての構成国が裁判管轄権をもつ。

   Where a hosting service provider which does not have its main establishment in the Union fails to designate a legal representative, all Member States shall have jurisdiction.

3. 構成国の職務権限のある機関が第 2 項による裁判管轄権を行使する場合，その職務権限のある機関は，他の全ての構成国の職務権限のある機関に対し，連絡する。

   Where a competent authority of a Member State exercises jurisdiction pursuant to paragraph 2, it shall inform the competent authorities of all other Member States.

第 17 条 法律の代理者
Article 17 Legal representative

1. 欧州連合内にその主たる拠点をもたないホスティングサービスプロバイダは，書面により，職務権限のある機関から発された削除命令及び決定の受領，遵守及び執行の目的のための

欧州連合内におけるそのプロバイダの法律上の代理者として，自然人または法人を指定する。

A hosting service provider which does not have its main establishment in the Union shall designate, in writing, a natural or legal person as its legal representative in the Union for the purpose of the receipt of, compliance with and the enforcement of removal orders and decisions issued by the competent authorities.

2. ホスティングサービスプロバイダは，そのプロバイダの法律上の代理者に対し，それらの削除命令及び決定を遵守し，職務権限のある機関との間で調整するために必要となる権限及び資源を提供する。

The hosting service provider shall provide its legal representative with the necessary powers and resources to comply with those removal orders and decisions and to cooperate with the competent authorities.

法律上の代理者は，そのホスティングサービスプロバイダがそのサービスを提供する構成国中の 1 つに居住し，または，拠点をもつ。

The legal representative shall reside or be established in one of the Member States where the hosting service provider offers its services.

3. 法律上の代理者は，そのホスティングサービスプロバイダの法的責任またはそのプロバイダを相手方とする訴訟を妨げることなく，この規則の違反行為に関して法的責任を負い得る。

The legal representative may be held liable for infringements of this Regulation, without prejudice to any liability of or legal actions against the hosting service provider.

4. ホスティングサービスプロバイダは，そのプロバイダの法律上の代理者の居住地または拠点がある構成国の第 12 条第 1 項の(d)に示す職務権限のある機関に対し，その指定を通知する。

The hosting service provider shall notify the competent authority referred to in point (d) of Article 12(1) of the Member State where its legal representative resides or is established of the designation.

ホスティングサービスプロバイダは，その法律上の代理者に関する情報を公表する。

The hosting service provider shall make the information about the legal representative publicly available.

第VI節 最終規定
Section VI Final Provisions

第 18 条 制裁
Article 18 Penalties

1. 構成国は，ホスティングサービスプロバイダによるこの規則の違反行為に適用可能な制裁に関する規定を定め，かつ，それらの規定が実装されることを確保するために必要となる全ての措置を講ずる。そのような制裁は，第 3 条第 3 項及び第 6 項，第 4 条第 2 項及び第 7 項，第 5 条第 1 項，第 2 項，第 3 項，第 5 項及び第 6 項，第 6 条，第 7 条，第 10 条及び第 11 条，第 14 条第 5 項，第 15 条第 1 項及び第 17 条の違反行為に対処するために限定される。

   Member States shall lay down the rules on penalties applicable to infringements of this Regulation by hosting service providers and shall take all measures necessary to ensure that they are implemented. Such penalties shall be limited to addressing infringements of Article 3(3) and (6), Article 4(2) and (7), Article 5(1), (2), (3), (5) and (6), Articles 6, 7, 10 and 11, Article 14(5), Article 15(1) and Article 17.

   第 1 副項に示す制裁は，実効的であり，比例的であり，かつ，抑止力のあるものとする。構成国は，2022 年 6 月 7 日までに，欧州委員会に対し，それらの規定及びそれらの措置を通知し，かつ，欧州委員会に対し，遅滞なく，それらの影響のあるその後の改正を通知する。

   The penalties referred to in the first subparagraph shall be effective, proportionate and dissuasive. Member States shall, by 7 June 2022, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

2. 構成国は，制裁を科すかどうか判断する際，及び，制裁のタイプ及びレベルを決定する際，職務権限のある機関が，以下の事項を含め，関連する全ての状況を考慮に入れることを確保する：
   (a) 違反行為の性質，重大性及び持続期間；
   (b) その違反行為が意図的なものであるか，過失によるものであるか；
   (c) そのホスティングサービスプロバイダによる既往の違反行為；
   (d) そのホスティングサービスプロバイダの資金力；
   (e) そのホスティングサービスプロバイダの職務権限のある機関との間の協力のレベル；
   (f) そのホスティングサービスプロバイダの性質及び規模，とりわけ，そのプロバイダが，マイクロ企業，小規模企業または中規模企業であるかどうか；
   (g) この規則を遵守するためにそのホスティングサービスプロバイダによって講じられた技術上及び組織上の措置を考慮に入れた上で，そのホスティングサービスプロバイダの不履行の程度。

Member States shall ensure that the competent authorities, when deciding whether to impose a penalty and when determining the type and level of penalty, take into account all relevant circumstances, including:

(a) the nature, gravity and duration of the infringement;
(b) whether the infringement was intentional or negligent;
(c) previous infringements by the hosting service provider;
(d) the financial strength of the hosting service provider;
(e) the level of cooperation of the hosting service provider with the competent authorities;
(f) the nature and size of the hosting service provider, in particular whether it is a micro, small or medium-sized enterprise;
(g) the degree of fault of the hosting service provider, taking into account the technical and organisational measures taken by the hosting service provider to comply with this Regulation.

3. 構成国は，第 3 条第 3 項による義務の組織的または恒常的な不遵守が，そのホスティングサービスプロバイダの前事業年の全世界の売上の 4%を上限とする制裁金に服することを確保する。

Member States shall ensure that a systematic or persistent failure to comply with obligations pursuant to Article 3(3) is subject to financial penalties of up to 4 % of the hosting service provider's global turnover of the preceding business year.

第 19 条　技術上の要件及び別紙の改訂

Article 19 Technical requirements and amendments to the annexes

1. 欧州委員会は，削除命令の送信のために職務権限のある機関によって使用される電子的な手段のために必要となる技術上の要件によってこの規則を補遺するため，第 20 条に従って委任される行為を採択する権限を与えられる。

The Commission shall be empowered to adopt delegated acts in accordance with Article 20 in order to supplement this Regulation with the necessary technical requirements for the electronic means to be used by competent authorities for the transmission of removal orders.

2. 欧州委員会は，削除命令のためのテンプレートの内容に関してあり得る改善の必要性に実効的に対処するため，及び，削除命令を執行することが不可能であることに関する情報を提供するために別紙を改訂するため，第 20 条に従って委任される行為を採択する権限を与えられる。

The Commission shall be empowered to adopt delegated acts in accordance with Article 20 to amend the annexes in order to effectively address a possible need for improvements regarding the

content of templates for removal orders and to provide information on the impossibility to execute removal orders.

第 20 条 委任の実行

Article 20 Exercise of the delegation

1. 委任される行為を採択する権限は，本条に定める条件に服して，欧州委員会に対して与えられる。

   The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. 第 19 条に示す権限の委任は，2022 年 6 月 7 日から不定期間で，欧州委員会に対して与えられる。

   The power to adopt delegated acts referred to in Article 19 shall be conferred on the Commission for an indeterminate period of time from 7 June 2022.

3. 第 19 条に示す権限の委任は，いつでも，欧州議会または理事会によって取消され得る。取消しの決定は，同決定の中で指示される権限の委任を終了させる。その決定は，EU 官報上で公示された翌日に発効し，または，その決定の中で指示された後の日に発効する。その決定は，既に発効している委任される行為の有効性を害してはならない。

   The delegation of power referred to in Article 19 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day after the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. 委任される行為を採択する前に，欧州委員会は，より良い立法に関する 2016 年 4 月 13 日の機関間合意に定める基本原則に従い，各構成国から指名された専門家と協議する。

   Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. 委任される行為を欧州委員会が採択した後直ちに，欧州委員会は，欧州議会及び理事会に対し，同時に，そのことを通知する。

As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. 第19条により採択された委任される行為は，欧州議会及び理事会に対する当該行為の通知から 3 か月以内に欧州議会もしくは理事会のいずれからも異議が表明されないとき，または，その期間が満了する前に，欧州議会及び理事会の両者から欧州委員会に対して異議を述べない旨が連絡されたときに限り発効する。その期間は，欧州議会または理事会の発意により，3か月まで延長される。

A delegated act adopted pursuant to Article 19 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

第 21 条 監視

Article 21 Monitoring

1. 構成国は，その構成国の職務権限のある機関及びその構成国の裁判管轄権の下にあるホスティングサービスプロバイダから，前暦年においてこの規則に従って行われた活動に関する情報を収集し，かつ，欧州委員会に対し，毎年 3 月 31 日までに，その情報を送付する。その情報は，以下の情報を含める：
   (a) 発令された削除命令の数及び削除されまたはそれへのアクセスが不能化されたテロリストコンテントの項目の数並びにその削除またはアクセス不能化の速度；
   (b) 削除されまたはそれへのアクセスが不能化されたテロリストコンテントの項目の数並びにその削除またはアクセス不能化の速度を含め，第 5 条により講じられた特別の措置；
   (c) 第 6 条によりホスティングサービスプロバイダによって保全されたコンテントに関して，職務権限のある機関から発されたアクセス要求の数；
   (d) 第 10 条により開始された不服申立て手続及びホスティングサービスプロバイダによって行われた活動の数；
   (e) 開始された行政上または法務上の見直し手続及び国内法に従って職務権限のある機関によって行われた決定の数。

Member States shall collect from their competent authorities and the hosting service providers under their jurisdiction and send to the Commission by 31 March of every year information about the actions they have taken in accordance with this Regulation in the previous calendar year. That information shall include:

(a) the number of removal orders issued and the number of items of terrorist content which have

been removed or access to which has been disabled and the speed of the removal or disabling;

(b) the specific measures taken pursuant to Article 5, including the number of items of terrorist content which have been removed or access to which has been disabled and the speed of the removal or disabling;

(c) the number of access requests issued by competent authorities regarding content preserved by hosting service providers pursuant to Article 6;

(d) the number of complaint procedures initiated and actions taken by the hosting service providers pursuant to Article 10;

(e) the number of administrative or judicial review proceedings initiated and decisions taken by the competent authority in accordance with national law.

2. 2023 年 6 月 7 日までに, 欧州委員会は, この規則の出力, 結果及び影響を監視するための詳細な計画を策定する。その監視計画は, 指標, 並びに, データ及びそれ以外の証拠が収集される手段及びその収集の間隔を定める。その監視契約は, 進捗状況の監視と第 23 条によるこの規則の評価のためのデータ及びそれ以外の証拠の収集及び分析において, 欧州委員会によって行われる活動と構成国によって行われる活動を指定する。

By 7 June 2023, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the indicators and the means by which and the intervals at which the data and other necessary evidence are to be collected. It shall specify the actions to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence to monitor the progress and evaluate this Regulation pursuant to Article 23.

第 22 条 実装報告書

Article 22 Implementation report

2023 年 6 月 7 日までに, 欧州委員会は, 欧州議会及び理事会に対し, この規則の適用に関する報告書を提出する。その報告書は, 第 21 条に基づく監視に関する情報及び第 8 条に基づく透明性義務から生ずる情報を含める。構成国は, 欧州委員会に対し, その報告書の作成のために必要となる情報を提供する。

By 7 June 2023, the Commission shall submit a report on the application of this Regulation to the European Parliament and to the Council. That report shall include information on monitoring under Article 21 and information resulting from the transparency obligations under Article 8. Member States shall provide the Commission with the information necessary for the drafting of the report.

第 23 条 評価
Article 23 Evaluation

2024 年 6 月 7 日までに, 欧州委員会は, この規則の評価を遂行し, かつ, 欧州議会及び理事会に対し, 以下の事項を含め, この規則の適用に関する報告書を提出する:
(a) 安全確保の仕組み, とりわけ, 第 4 条第 4 項, 第 6 条第 3 項及び第 7 条ないし第 11 条に定める安全確保の仕組みの稼働及び実効性;
(b) 基本的な権利, とりわけ, 表現及び情報伝達の自由, 私生活の尊重並びに個人データの保護に対するこの規則の適用の影響; 並びに,
(c) 公共の保安に対するこの規則の貢献。

By 7 June 2024, the Commission shall carry out an evaluation of this Regulation and submit a report to the European Parliament and to the Council on its application including:
(a) the functioning and effectiveness of the safeguard mechanisms, in particular those provided for in Article 4(4), Article 6(3) and Articles 7 to 11;
(b) the impact of the application of this Regulation on fundamental rights, in particular the freedom of expression and information, the respect for private life and the protection of personal data; and
(c) the contribution of this Regulation to the protection of public security.

それが適切なときは, その報告書は, 立法提案を添付する。

Where appropriate, the report shall be accompanied by legislative proposals.

構成国は, 欧州委員会に対し, その報告書の作成のために必要となる情報を提供する。

Member States shall provide the Commission with the information necessary for the drafting of the report.

欧州委員会は, この規則に基づく通信及び協力を容易にするための, オンラインのテロリストコンテントに関する欧州プラットフォームの構築の必要性及び実現可能性も評価する。

The Commission shall also assess the necessity and feasibility of establishing a European platform on terrorist content online for facilitating communication and cooperation under this Regulation.

第 24 条 発効及び適用
Article 24 Entry into force and application

この規則は, EU 官報上で公示された 20 日後に発効する。

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

この規則は，2022 年 6 月 7 日から適用される。

It shall apply from 7 June 2022.

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

This Regulation shall be binding in its entirety and directly applicable in all Member States.

ブリュッセルにおいて，2021 年 4 月 29 日に行われた。

Done at Brussels, 29 April 2021.

欧州議会として	理事会として
議長 D. M. SASSOLI	A.P. ZACARIAS

別紙 I

削除命令
Removal Order

（欧州議会及び理事会の規則(EU) 2021/784 の第 3 条）
(Article 3 of Regulation (EU) 2021/784 of the European Parliament and of the Council)

規則(EU) 2017/784（「規則」）の第 3 条により，この削除命令の名宛人は，この削除命令の受領後直ちに，かつ，いかなる場合においても， 受領後 1 時間以内に，テロリストコンテントを削除し，または，全ての構成国においてテロリストコンテントへのアクセスを不能化する。

Pursuant to Article 3 of Regulation (EU) 2021/784 (the 'Regulation') the addressee of this removal order shall remove terrorist content or disable access to terrorist content in all Member States as soon as possible and in any event within one hour of receipt of the removal order.

規則の第 6 条により，その名宛人は，6 か月間，または，職務権限のある機関もしくは裁判所からの要求により，それよりも長い期間，削除またはアクセス不能化されたコンテント及び関連データを保全する。

Pursuant to Article 6 of the Regulation the addressee shall preserve content and related data, which has been removed or access to which as been disabled, for six months or longer upon request from the competent authorities or courts.

規則の第 15 条第 2 項により，この削除命令は，名宛人によって指定された言語中の 1 つにより送付される。

Pursuant to Article 15(2) of the Regulation, this removal order shall be sent in one of the languages designated by the addressee.

セクション A
Section A

発令元である職務権限のある機関の構成国:
Member State of the issuing competent authority:

注記:発令元である職務権限のある機関の詳細は，E 節及び F 節の中で与えられる
NB: details of the issuing competent authority to be provided in Sections E and F

名宛人，及び，関連するときは，法律上の代理者：
Addressee and, where relevant, legal representative:

連絡部局：
Contact point:

ホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者が居住地またはその拠点をもつ構成国：
Member State where the hosting service provider has its main establishment or where its legal representative resides or is established:

削除命令の発令日時：
Time and date of issuing of the removal order:

削除命令の参照番号：
Reference number of the removal order:

セクション B：削除命令の受領後直ちに，かつ，いかなる場合においても，受領後 1 時間以内に，削除され，または，全ての構成国においてそれへのアクセスが不能化されるべきテロリストコンテント
Section B: Terrorist content to be removed or access to which is to be disabled in all Member States as soon as possible and in any event within one hour of receipt of the removal order

テロリストコンテントの URL 及びその識別同定と正確な所在場所特定を可能にする付加的な情報：
URL and any additional information enabling the identification and exact location of the terrorist content:

規則の第 2 条第 7 号に従い，その対象物がテロリストコンテントであると判断する理由。
Reasons for considering the material to be terrorist content, in accordance with point (7) of Article 2 of the Regulation.

対象物（関連するボックスをチェックしてください）：

The material (please tick the relevant box(es)):

☐ テロリスト行為を美化することのような，そのような犯罪行為の実行を鼓舞することによる，他者に対してテロリスト行為を扇動する（規則第 2 条第 7 項(a)）

incites others to commit terrorist offences, such as by glorifying terrorist acts, by advocating the commission of such offences (point (7)(a) of Article 2 of the Regulation)

☐ 他者に対してテロリスト行為を勧誘する，または，テロリスト行為の実行に寄与することを勧誘する（規則第 2 条第 7 項(b)）

solicits others to commit or to contribute to the commission of terrorist offences (point (7)(b) of Article 2 of the Regulation)

☐ 他者に対してテロリストグループの活動への参加を勧誘する（規則第 2 条第 7 項(c)）

solicits others to participate in the activities of a terrorist group (point (7)(c) of Article 2 of the Regulation)

☐ テロリスト行為を実行する目的またはその実行に寄与する目的のために，爆発物，銃器もしくはそれ以外の武器，有害もしくは危険な物質の製造もしくは使用に関する指示，または，それら以外の特別の手法もしくは技法に関する指示を提供する（規則第 2 条第 7 項(d)）

provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of terrorist offences (point (7)(d) of Article 2 of the Regulation)

☐ テロリスト行為のいずれかの実行の脅威を組成する（規則第 2 条第 7 項(e)）

constitutes a threat to commit one of the terrorist offences (point (7)(e) of Article 2 of the Regulation)

その対象物をテロリストコンテントであるとする判断と関連する付加的な情報：
Additional information for considering the material to be terrorist content:

セクション C：コンテント提供者に対する情報提供
Section C: Information to the content provider

以下の点に留意してください（適用可能な場合，ボックスをチェックしてください）：
Please note that (please tick the box, if applicable):

□公共の保安上の理由により，名宛人は，テロリストコンテントの削除またはそのアクセス不能化について，コンテント提供者に対して情報提供することを控えなければならない

□for reasons of public security, the addressee must refrain from informing the content provider of the removal of or disabling of access to the terrorist content

ボックスが適用可能ではないときは，国内法に基づく発令元である職務権限のある機関の構成国において削除命令に不服申立てできることの詳細（要求があるときは，コンテント提供者に対し，削除命令の写しが送付されなければならない）に関しては，G 節を参照してください

If the box is not applicable, please see Section G for details of possibilities to challenge the removal order in the Member State of the issuing competent authority under national law (a copy of the removal order must be sent to the content provider, if requested)

セクション D：ホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者が居住地またはその拠点をもつ構成国の職務権限のある機関に対する情報提供
Section D: Information to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established

関連するボックスをチェックしてください：
Please tick the relevant box(es):

□ ホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者が居住地またはその拠点をもつ構成国は，発令元である職務権限のある機関の構成国とは別の構成国

The Member State where the hosting service provider has its main establishment or where its legal representative resides or is established is other than the Member State of the issuing competent authority

☐	ホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者が居住地またはその拠点をもつ構成国の職務権限のある機関に対して，削除命令の副本が送付される A copy of the removal order is sent to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established

セクション E：発令元である職務権限のある機関の詳細

Section E: Details of the issuing competent authority

タイプ（関連するボックスをチェックしてください）：

Type (please tick the relevant box):

☐ 判事，裁判所または捜査判事
judge, court or investigating judge

☐ 法執行機関
law enforcement authority

☐ 上記以外の職務権限のある機関→セクション F も埋めてください
other competent authority → please complete also Section F

発令元である職務権限のある機関または削除命令が正確かつ真正であることを証明するその機関の代表者：

Details of the issuing competent authority or its representative certifying the removal order as accurate and correct:

発令元である職務権限のある機関の名称：

Name of the issuing competent authority:

その機関の代表者の姓名及び保有している地位（職格及び職位）：

Name of its representative and post held (title and grade):

記録番号：

File No:

住所：

Address:

電話番号（国別コード）（区域コード／都市コード）：

Tel. No (country code) (area/city code):

……

ファックス番号（国別コード）（区域コード／都市コード）：
Fax No (country code) (area/city code):

……

電子メールアドレス：……
Email address:…
日付：……
Date:…
公印（利用可能な場合）及び署名[1]
Official stamp (if available) and signature [1]:

セクション F：事後対応のための連絡先
Section F: Contact details for follow-up

削除またはアクセス不能化の時に関するフィードバックのため，または，更に説明を提供するための，発令元である職務権限のある機関の連絡先：
Contact details of the issuing competent authority for feedback on the time of removal or the disabling of access, or to provide further clarification:

……

ホスティングサービスプロバイダがその主たる拠点をもつ構成国またはそのプロバイダの法律上の代理者が居住地またはその拠点をもつ構成国の職務権限のある機関の連絡先：
Contact details of the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established:

……

セクション G：救済の可能性に関する情報
Section G: Information about redress possibilities

削除命令に対して不服申立てするための職務権限のある組織または裁判所，期限及び手続に関する情報：
Information about competent body or court, deadlines and procedures for challenging the removal order:

削除命令に対して不服を申立て得る職務権限のある組織または裁判所：
Competent body or court before which the removal order can be challenged:

……

[1] 削除命令の真正性を保証し得る認証された送信経路を介して削除命令が送信される場合，署名は不要。

削除命令に対して不服申立てをする期限(開始後の日数／月数):
Deadline for challenging the removal order (days/months starting from):

.....

国内立法の条項へのリンク:
Link to provisions in national legislation:

.....

別紙Ⅱ

テロリストコンテントの削除またはアクセス不能化後のフィードバック
Feedback following Removal of or Disabling of Access to Terrorist Content

（欧州議会及び理事会の規則(EU) 2021/784 の第 3 条第 6 項）
(Article 3(6) of Regulation (EU) 2021/784 of the European Parliament and of the Council)

セクション A: Section A: 削除命令の名宛人: Addressee of the removal order: ---------- 削除命令を発令した職務権限のある機関: Competent authority that issued the removal order: ---------- 削除命令を発令した職務権限のある機関の記録参照: File reference of the competent authority that issued the removal order: ---------- 名宛人の記録参照: File reference of the addressee: ---------- 削除命令の受領日時: Time and date of receipt of removal order: ----------
セクション B:削除命令を遵守して講じられた措置 Section B: Measures taken in compliance with the removal order （関連するボックスをチェックしてください）: (please tick the relevant box): ☐ テロリストコンテントは，削除された the terrorist content has been removed

□	テロリストコンテントは，全ての構成国においてアクセス不能化された access to the terrorist content has been disabled in all Member States

措置が講じられた日時:
Time and date of the measure taken:

.....

セクション C：名宛人の詳細
Section C: Details of the addressee

ホスティングサービスプロバイダの名称:
Name of the hosting service provider:

.....
または
ホスティングサービスプロバイダの法律上の代理者の名称:
Name of the legal representative of the hosting service provider:

.....

ホスティングサービスプロバイダの主たる拠点の構成国:
Member State of main establishment of the hosting service provider:

.....
または
ホスティングサービスプロバイダの代理者の居住地または拠点の構成国:
Member State of residence or establishment of the legal representative of the hosting service provider:

.....

権限を与えられた者の姓名：
Name of the authorised person:

.....

連絡場所の電子メールアドレス：
Email address of the contact point:

.....

日付:
Date:

.....

別紙Ⅲ

削除命令の執行が不可能であることに関する情報提供
Information about the Impossibility to Execute the Removal Order

（欧州議会及び理事会の規則(EU) 2021/784 の第 3 条第 7 項及び第 8 項）
(Article 3(7) and (8) of Regulation (EU) 2021/784 of the European Parliament and of the Council)

セクション A:
Section A:

削除命令の名宛人:
Addressee of the removal order:

削除命令を発令した職務権限のある機関:
Competent authority that issued the removal order:

削除命令を発令した職務権限のある機関の記録参照:
File reference of the competent authority that issued the removal order:

名宛人の記録参照:
File reference of the addressee:

削除命令の受領日時:
Time and date of receipt of removal order:

セクション B:不執行
Section B: Non-execution

(1) 以下の理由により，期限内に削除命令を執行できない（関連するボックスをチェックしてください）:
The removal order cannot be executed within the deadline for the following reasons (please tick the relevant box(es)):

☐ 客観的に正当化し得る技術上の理由または業務遂行上の理由を含め，ホスティングサービスプロバイダの責に帰さない不可抗力または事実上不可能
force majeure or *de facto* impossibility not attributable to the hosting service provider, including for objectively justifiable technical or operational reasons

☐ 削除命令が明白な誤りを含んでいる
the removal order contains manifest errors

☐ 削除命令が十分な情報を含んでいない
the removal order does not contain sufficient information

(2) 不執行の理由と関連する情報を更に提供してください
Please provide further information as to the reasons for non-execution:

.....

(3) 削除命令が明白な誤りを含んでいる場合，及びまたは，十分な情報を含んでいない場合，その誤り，及び，更に必要な情報または必要な説明を指示してください。
If the removal order contains manifest errors and/or does not contain sufficient information, please specify the errors and the further information or clarification necessary:

.....

セクション C：ホスティングサービスプロバイダまたはその法律上の代理者の詳細
Section C: Details of the hosting service provider or its legal representative

ホスティングサービスプロバイダの名称:
Name of the hosting service provider:

.....

または
ホスティングサービスプロバイダの法律上の代理者の名称:
Name of the legal representative of the hosting service provider:

.....

権限を与えられた者の姓名：
Name of the authorised person:

.....

連絡場所（電子メールアドレス）：
Email address of the contact point:

.....

署名:
Signature:

日付:
Date:

指令(EU) 2016/680
［参考訳・改訂版］

2021 年 12 月 5 日
明治大学法学部教授
夏 井 高 人

＊＊＊

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA（OJ L 119, 4.5.2016, p. 89-131）のテキスト（英語版）に基づいて和訳を試み，2017 年 1 月，法と情報雑誌 2 巻 1 号 41～140 頁にその参考訳を掲載して公表した。

その後，指令 (EU) 2016/680 の原文の第 51 条第 1 項(f)は，EU 官報（OJ L, L 127/6, 23.5.2018）によって訂正されている。

その後の研究成果及び関連法令の改正等を踏まえ，指令 (EU) 2016/680 の参考訳・初版の中で後に発見された誤訳部分及び誤記等を訂正し，また，その後における研究成果の進展に伴う訳語の統一等も併せ，指令(EU) 2016/680 の参考訳の改訂版を作成することにした。

指令(EU) 2016/680 の原文のテキストを入手できるサイトの URL は，下記のとおりである。

http://data.europa.eu/eli/dir/2016/680/oj
[2021 年 12 月 1 日確認]

指令(EU) 2016/680 は，EU の現行法である。

－解　説－

1．指令(EU) 2016/680

指令(EU) 2016/680 は，各構成国の裁判所（court），法執行機関（law enforcement authorities），関連行政機関等による犯罪捜査及び刑事公判のための個人データの処理，各構成国の捜査機関相互の協力等における個人データの処理の特殊性（特に捜査の秘密）に鑑み，規則(EU) 2016/679（GDPR）の特別法として，構成国の法執行機関（警察等）に適用される。

指令(EU) 2016/680 は，構成国の関連機関による個人データ処理に対してのみ適用される法令であり，欧州連合の機関等による個人データの処理には適用されない。

これらの刑事手続と関連する個人データの処理において指令(EU) 2016/680 が適用されることに関しては，e-CODEX 規則案（COM/2020/712 final）等の中でも明確に示されている。

指令(EU) 2016/680 が適用される場合，個人データのデータ主体の権利が大幅に制限される。

一般に，個人データ処理におけるデータ主体の事前の同意（consent）は，規則(EU) 2016/679（GDPR）が明定する個人データ保護の基本原則の 1 つである。しかし，指令(EU) 2016/680 が適用される分野においては異なる。例えば，各構成国の関連刑事法令に基づく強制捜査の際の個人データの処理に関しては，各構成国の関連刑事法令によって，データ主体が法執行機関等の命令に服さなければならない場合，その命令を法律上の根拠とし，その命令の法律上の効果として個人データの収集が行われることになるので，そのデータ主体の同意は，個人データ処理のための法律上の根拠ではない（前文(35)及び前文(37)参照）。この点に関し，規則(EU) 2016/679（GDPR）は，その第 2 条第 2 項(d)により，適用除外となっている。

なお，犯罪捜査の過程において，危難に遭遇している自然人の人命救助が必要となるような事態の発生は，あり得ることである。そのような際における自然人の生存の利益（vital interests）の確保のために行われる個人識別（個人データ処理）のためにデータ主体の同意を要しないことは，規則(EU) 2016/679（GDPR）の第 6 条第 1 項(d)に定めているとおり緊急避難の一種であり，指令(EU) 2016/680 が適用される場合に特有のことではない。

構成国の法執行機関等は，被疑者（容疑者）に関する情報，有罪判決（犯歴）に関する情報，犯罪被害者等に関する情報，及び，証人や参考人等に関する情報を区分して管理することが求められる（第 6 条参照）。

データ主体の権利の行使に関しては，各構成国の法律により，一般的な一定の制限が加えられることがある（第 13 条第 3 項，第 15 条及び第 16 条参照）。これは，権利が存在することの否定ではなく，権利の行使に対する制限の一種である。

データ主体の個別の権利の行使に関しても，直接に行使されることがなく，監督機関を介した間接的な権利の行使のみが認められる場合がある。

そのような場合，例えば，各構成国の監督機関がデータ主体に代わって検査及び見直しを実施し，「点検した」等の回答をするのみである（第 17 条，第 46 条第 1 項(g)参照）。また，不正確な個人データに関する削除の権利に関しても，データ主体が直接にその権利を行使できず，各構成国の監督機関が検査した上で，当該機関がその削除の必要があると判断したときは削除されるだけである（第 16 条参照）。

管理者である各構成国の法務当局及び法執行機関等による個人データの処理の適法性を監督するため，各構成国内に独立の監督機関が設置される。この監督機関は，例えば，規則(EU) 2016/679（GDPR）の遵守を監督するための各構成国の国内監督機関と兼務とすることができる。指令(EU) 2016/680 に基づく監督機関の権限は広範な範囲に及ぶものであるが，法務当局の独立性を保障しなければならない場合（例：裁判所による個々の裁判事件にお

ける審理及び判断等）における個人データの処理（例：訴訟関係記録の中にある個人データの処理）に対しては，監督機関の権限が及ばない。ただし，法務当局であっても，例えば，（官庁としての法務機関の）人事管理，（調達を含め）財務管理及び施設管理等のような一般業務における個人データの処理に対しては，監督機関の監督権限が及ぶ。この点は，法の欠缺が明確に存在する日本国の個人情報保護法制とはかなり大きな相違点である。

各構成国の監督機関の共同活動のための EU レベルの組織は，規則(EU) 2016/679（GDPR）によって設けられた欧州データ保護委員会（European Data Protection Board）である。その職務と権限等は，GDPR の第 68 条の第 76 条に定められている。この欧州データ保護委員会は，委員会（Board）と略称される。指令(EU) 2016/680 は，委員会の職務に関し，特別条項を定めている（第 51 条参照）。

刑事における国際的な相互補助（international mutual assistance）の場合を含め，犯罪捜査及び刑罰の執行等と関連して個人データの第三国移転が行われる場合，規則(EU) 2016/679（GDPR）の関連条項ではなく，指令(EU) 2016/680 の関連条項が適用される。国際的な犯罪捜査の協力における特殊事情等を考慮し，指令(EU) 2016/680 は，個人データの第三国移転に関する特例を定めている（前文(72)，前文(73)参照）。

規則(EU) 2016/679（GDPR）が適用される民間企業等においては，行動準則や標準約款等による対応が可能であるが，構成国の裁判所または関連行政機関に対して適用される指令(EU) 2016/680 にあっては，行動準則や標準約款等によることがそもそもあり得ない。

規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1-22）は，規則(EU) 2018/1725（OJ L 295, 21.11.2018, p.39-98）の第 99 条により，2018 年 12 月 10 日の経過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。

理事会決定 2007/533/JHA（OJ L 205, 7.8.2007, p. 63-84）は，規則(EU) 2018/1862（OJ L 312, 7.12.2018, p.56-106）によって全面的に改正された。同規則は，関連条文毎に段階的に適用（施行）され，2020 年 12 月 28 日から全面的に適用（施行）される。

指令(EU) 2016/680 の前文(94)の中で示されているテロリズムとの闘いに関する EU の最新法令は，規則(EU) 2021/784（OJ L 172, 17.5.2021, p. 79-109）である。

指令(EU) 2016/680 の前文(97)の中で示されている児童の性的虐待及び性的搾取並びに児童ポルノとの闘いに関する EU の最新の法令は，規則(EU) 2021/1232（OJ L 274, 30.7.2021, p. 41-51）である。

2. 参考訳作成における基本方針

この参考訳においては，EU 官報（OJ L, L 127/6, 23.5.2018）による第 51 条第 1 項(f)の修正

後の指令(EU) 2016/680 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対訳方式を採用することにした。ただし，原文を表示することが無意味な部分（特に脚注内）に関しては，原文または訳文の表示を省略した。

この参考訳は，あくまでも指令(EU) 2016/680 の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。

読みやすさを重視し，条文中の号(point)の表記を一部省略した。例えば，「point(a)」は「第(a)号」であるが，「第」と「号」を省略し，「(a)」と表記することにした。

この参考訳は，Eur-lex のデータ二次利用条件を遵守して作成した。

3. 参考訳作成において留意した事項

前文(51)の中にある「loss of confidentiality of data protected by professional secrecy」との箇所は，「loss of confidentiality of personal data protected by professional secrecy」の誤記である可能性がある（前文(61)参照）。しかし，この参考訳においては，原文のまま訳出することにした。

前文(61)の中にある「as soon as」との箇所は，同一の文の中にある「without undue delay」及び「not later than 72 hours」と論理的な整合性がとれていないので，誤記の一種である可能性がある。しかし，この参考訳においては，原文のまま訳出することにした。

前文(93)の末尾には「ピリオド（.）」がない。立法上のミスによるものと思われる。この参考訳においては，末尾に「ピリオド（.）」が存在するものとして訳出することにした。

第 36 条第 2 項は，非常に長い一文であるため，普通に日本語文に訳出した場合，「including」でくくられている句の部分とそれ以外の部分との区別がつきにくいという問題がある。そこで，この参考訳においては，便宜的なものとして，第 36 条第 2 項に限り，「including」でくくられている句の部分を括弧の中に入れ，他の部分と識別できるように訳出することにし

た。原文にはそのような括弧が存在しない。

4. 訳語に関する補足的説明

Controller

EU の個人データ保護法令においては，「controller」は，「管理者」であり，「取扱者」または「取扱事業者」ではない。特に，指令(EU) 2016/680 が適用される場合，「controller」の大部分が各構成国の行政機関となるので，「取扱者」または「取扱事業者」であることは，あり得ない。規則(EU) 2016/679（GDPR）においても，その適用対象が民間事業者だけではなく構成国のほぼ全ての行政機関も含まれることから，「controller」は，「管理者」であり，「取扱者」または「取扱事業者」ではない。

一般に，EU 法を理解しようとする場合，マネジメントシステムの基本理論を基礎として考察すると，理解しやすい。EU 法は，欧州理事会（European Council）によって宣言された一般的な要求仕様に相当する基本政策を実施するために欧州連合の理事会の承認を得て欧州委員会が策定する基本的な政策（policies）を詳細仕様とし，その詳細仕様を実装・運営するための管理策（control）の一種として，法令という方式による管理策を制定する。その管理策の方式に関する要件と制限は，構成国間の基本合意である欧州連合の機能に関する条約（TFEU）によって定められている。それゆえ，それぞれの法令の適用分野及び特性に応じて，当該管理策を実施するための管理者が定められることは，論理必然的なものと考えられる。また，法令というものが国家統治のためのマネジメントシステムの一種である以上，その管理策の運用を監視し，評価し，見直しを行うための仕組みが最初から当該法令の中に明示で組み込まれることも論理必然的なことである。このような明確な構造をもっていることは，合理的な国家統治のための手段の構築・運用・再設計のために資するところが大きい。手段としての有用性が高いことは，例えば，独裁主義の国家においてもこのような方式が導入可能であることを意味している。このことは，マネジメントシステムにおける管理策というものが本来的にもつ「手段」としての本質に起因するものである。また，一般に，法令を管理策（手段）として実現されるべき目的（政策）の基本理念または基本政策が明確ではない国または管理者としての職責を担う者の責任分担が明確ではない国においては，どのような管理策も合理的かつ十分に機能（稼働）することがない。

そのような国家体制の相違は，EU の基本条約に掲げられた自由主義及び民主主義並びに人権尊重という基本理念，または，国連憲章（第 1 条，第 13 条，第 55 条，第 62 条）に掲げられた自由主義及び国連人権宣言第 29 条に掲げられた民主主義という基本理念を最大限尊重すべきことを必須の制約条件として当該法令の中に内包させるか否かの相違という点にも現れている。逆から言うと，EU の法令においては，単なる手段として濫用されないための歯止めとして，自由主義及び民主主義並びに人権尊重という基本理念の尊重が制約条件として明示されているとも言い得る。EU モデルの正常な導入であるか，形骸化した濫用であるかの相違は，このような制約条件（自由主義及び民主主義並びに人権尊重という基本理念）の明示の有無によっても判定し得ることになる（GDPR の第 5 章参照）。

「controller」という語は，ここで述べたような意味での大きな構造把握の一部としても認識・理解されるべきである。

なお，EU 法においては，個人データの「取扱い」に相当する語として，「treatment」または「handling」または「deal with」等が使用されるのが一般的である。

Recipients

EU の個人データ保護法令において，「recipients」は，個人データの「取得者」である。この取得者は，当の個人データのデータ主体からの取得者も含まれる。それゆえ，例えば，日本国の行政機関個人情報保護法における行政機関及び日本国の個人情報保護法における個人情報取扱事業者は，EU 法においては全て取得者の一種である。同様に，そのようなデータ主体から個人データを取得した取得者から更に当該個人データの提供（開示）を受けた第三者もまた，取得者である。取得者として個人データを取得した者は，法定の除外事由がない限り，全て，管理者（controller）として当該個人データを管理すべき法律上の義務を負う。

この点に関し，令和 2 年の一部改正後においてもなお，日本国の個人情報保護法制の設計構造には，一貫性の欠如及び保護の欠缺が存在していることは，極めて遺憾なことである。このことは，日本国憲法に定められた基本的人権の保護を含め，日本国の極めて重要な国益を損なう原因ともなり得る。

Data protection officer

「data protection officer」は，「データ保護責任者」と訳すのが通例であり，この参考訳においてもそれに従うことにした。

このような場合の「officer」は，例えば，日本国の消防法に基づく防火担当責任者の場合の「責任者」と同じ語感をもつものである。消防法に定める防火担当責任者は，防火管理者を補佐する立場にある。それゆえ，「data protection officer」の訳語として，「データ保護担当責任者」はあり得る訳語である。

ただし，EU の個人データ保護法に定める「data protection officer」は，EU 及び構成国の個人データ保護法に関する特別の訓練を受けた者であることを要する。日本国の官庁の中においても，既に「個人情報保護責任者」またはこれと類似の責任者が指定されているところがある。この場合の「個人情報保護責任者」は，日本国の個人情報保護法制に関する専門知識をもつ者とされている。

Cross-border

「cross-border」は，原則として，EU の構成国間の域内国境を越えることを指す。EU の域外国境を越える場合は，「cross-border」ではなく，原則として，「international」と表現される。

それゆえ，構成国の法執行機関（警察等）の「cross-border」の協力とは，ある構成国の法執行機関と別の構成国の法執行機関との間の協力のことを指し，EU の構成国ではない第三国

の法執行機関との間の協力を含まない。

この参考訳においては，以上のように解した上で，関連する語句を訳出した。

Judicial redress, judicial review

「judicial redress」は，通常は，裁判所における（訴訟等による）救済のことを指す。しかし，EU の構成国の多くでは，（裁判官の人事を含め）裁判所が各国の法務省の所管する国家機関であり，また，裁判所ではない行政機関による法務上の救済（行政不服審査等）もあり得ることから，この参考訳においては，「judicial redress」を「司法救済」または「裁判所における救済」ではなく，「法務上の救済」と訳すことにした。司法権の独立を定める日本国憲法の下における日本国の国家体制及び法制度だけを前提として EU 法における基本的な法概念を理解しようとすると，必ず失敗する。EU に限らず，米国の場合を含め，一般に，（訴訟法上の意味での）裁判及び裁判官の独立と（国家機関という意味での）官庁としての裁判所の独立とを混同してはならない。

同様の理由により，「judicial review」は，「司法審査」または「裁判所による見直し」ではなく，「法務上の見直し」と訳すことにした。実際には，裁判所における行政訴訟（取消訴訟等）及び関連行政機関による不服審査が主たるものとなると考えられる。

これらの点に関し，従前の参考訳及び論考における訳語を一律に改める。

Jurisdiction

前文(86)における「jurisdiction」は，訴訟法上の意味での裁判所の事物管轄及び土地管轄の権限を含め，訴訟上の意味での裁判所が個々の訴訟事件において行使可能な全ての法律上の権限を総称するものとして用いられている。各構成国の国家主権という意味で使用されているわけではない。

この参考訳においては，そのような解釈を踏まえた上で，「jurisdiction」を「裁判管轄権」と訳すことにした。

このような文脈における「jurisdiction」を「裁判所の権限」と訳すことは可能な範囲内にある。しかし，これを「裁判権」と訳すことは，明らかに誤訳である。

一般に，「jurisdiction」は，文脈によって多義性をもつ。これを「裁判管轄権」以外の日本語で訳出しようとする場合，相当に経験を積んだ者が完全に正確な法解釈に基づいて行うのでなければ，誤訳となるリスクが大きいと言える。「jurisdiction」は，AI 技術による解析が困難なものの 1 つであり，少なくとも，印欧語と日本語のような，言語体系及び語彙に相当の隔たりのある言語間の翻訳に関する限り，人間による何十年もの期間にわたる法学上の網羅的な学識を踏まえた見識と均等な機能を具備しない限り，この語の自動翻訳（機械翻訳）は，無理である。このことは，法令や判例の「翻訳」という知的作業が単なる語の置き換え処理ではなく，まさに，かなりレベルの高い熟達者によるべき法解釈そのものであることを意味している。EU における自動翻訳（機械翻訳）が一定程度の成果をあげているのは，同じ印欧語の系統に属する言語間の翻訳だからである。

それゆえ，印欧語と日本語のような，言語体系及び語彙に相当の隔たりのある言語間の隔たりを完全に理解しないまま，法解釈の機能を安易に組み込んだ AI システムは，隠れた大きなバイアスをもつシステムであり，社会に対する危険性が極めて高いにも拘らず，（出典または典拠等が出力結果の中で明示されない著作権法違反となる AI システムにおいては特に）そのことに法的責任を負うべき者が不明確なことが普通である。単語帳レベルまたは辞書レベルのもの及び国際的な定型文または定型的な表現が既に確立している分野のものを除き，何らかの法的対応が必要である（人工知能規則案（COM/2021/206 final）参照）。

Right to have inaccurate personal data concerning him or her rectified

通常の文法上の理解に従って訳す場合，「right to have inaccurate personal data concerning him or her rectified」は，「彼または彼女に関する不正確なデータを訂正させる権利」と訳し得る。この文は，前文(47)の中にある。しかし，EU のいかなる構成国においても，私人であるデータ主体が公権力主体である管理者（行政機関）に対して法的強制力または実力をもって当該データの訂正を直接に強制するための法定の執行方法をもっていないし，そのような執行方法は法理論上存在し得ないものであるので，そもそも「訂正させる」ことがあり得ない。つまり，EU 法の法解釈の観点からすると，論理的に不可能なことであるので，「訂正させる」というような訳は成立しない。他方において，前文(47)に相当する第 16 条第 1 項第 1 文は，「Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her」と定めており，この部分は，「彼または彼女に関する不正確な個人データの訂正を得るデータ主体の権利を定める」と訳すことができる。つまり，前文(47)の該当部分と第16条第1項第1文の該当部分は，完全に同義の文でありながら表現方法が異なっている文である。そして，第 16 条第 1 項第 1 文において表現されているような権利に関しては，EU の各構成国において，代替執行等を含め，適法な執行方法が存在する。代替執行は，特定の管理者に対して特定の行為を「させる」執行方法ではなく，当の管理者とは別の適法な機関・組織等によって所期の目的を実現させ，それによる目的の実現が法的には当該管理者から得たのと均等なものとして評価され，そして，それにかかった費用を（通常の強制執行の方法により）当の管理者から弁償させる制度である。以上のことから，前文(47)の「right to have inaccurate personal data concerning him or her rectified」との箇所は，「彼または彼女に関する不正確なデータの訂正を得る権利」と訳されるべきである。従前は，同じ文及び類似の文に関し，慣例を尊重し，「させる」と訳してみたことがある。しかし，論理的にあり得ないような意味をもつ訳文を維持することは正しいことではないので，猛省した上で，自分の信念に従い，全て改めることにした。なお，第 16 条第 1 項第 2 文の中にある「right to have incomplete personal data completed」も同じである。

以上のほかは，後掲規則(EU) 2020/ 1783 の参考訳，後掲規則(EU) 2020/1784 の参考訳，後掲規則(EU) 2021/693 の参考訳，後掲規則(EU) 2021/694 の参考訳，後掲理事会決議(2020/C 342 I/01)の参考訳，後掲 e-Justice 決議 2008/2125 の参考訳，後掲電子識別規則(EU) No 910/2014 の参考訳，後掲人工知能規則案（COM/2021/206 final）の参考訳，後掲デジタル

サービス規則案（COM/2020/825 final）の参考訳及び後掲 e-CODEX 規則案の参考訳の各冒頭部分で述べたとおりである。

5. 関連参考訳及び参考文献

規則(EU) 2018/1725 の参考訳は，法と情報雑誌 4 巻 1 号 1～81 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。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。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。指令 97/66/EC の参考訳・改訂版は，法と情報雑誌 3 巻 7 号 109～123 頁にある。個人データ保護指令 95/46/EC の参考訳・改訂版は，法と情報雑誌 2 巻 5 号 332～365 頁にある。規則(EU) 2016/679（一般データ保護規則）の参考訳・再訂版は，法と情報雑誌 3 巻 5 号 1～114 頁にある。理事会枠組み決定 2008/977/JHA の参考訳は，法と情報雑誌 2 巻 1 号 141～169 頁にある。e-Justice 個人データ保護決定 2014/333/EU の参考訳は，法と情報雑誌 2 巻 10 号 197～206 頁にある。

理事会決定 2008/615/JHA の参考訳は，法と情報雑誌 2 巻 2 号 155～181 頁にある。規則(EU) 2021/1232 の参考訳は，法と情報雑誌 6 巻 6 号 219～255 頁にある。規則(EU) 2021/784 の参考訳は，法と情報雑誌 6 巻 6 号 256～338 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(EU) 2020/1783 の参考訳は，法と情報雑誌 6 巻 5 号 1～81 頁にある。規則(EU) 2020/1784 の参考訳は，法と情報雑誌 6 巻 5 号 82～159 頁にある。規則(EU) 2021/693 の参考訳は，法と情報雑誌 6 巻 4 号 440～486 頁にある。規則(EU) 2021/694 の参考訳は，法と情報雑誌 6 巻 1 号 1～104 頁にある。理事会決議(2020/C 342 I/01)の参考訳は，法と情報雑誌 6 巻 4 号 513～537 頁にある。e-Justice 決議 2008/2125 の参考訳は，法と情報雑誌 6 巻 4 号 487～512 頁にある。人工知能規則案（COM/2021/206 final）の参考訳は，法と情報雑誌 6 巻 5 号 320～562 頁にある。e-CODEX 規則案の参考訳は，法と情報雑誌 6 巻 5 号 233～319 頁にある。デジタルサービス規則案（COM/2020/825 final）の参考訳は，法と情報雑誌 6 巻 6 号 1～128 頁にある。電子識別規則(EU) No 910/2014 の参考訳は，法と情報雑誌 2 巻 10 号 147～196 頁にある。

この参考訳は，科学研究費補助金基盤研究(A)（15H01928）による研究成果の一部である。

＊＊＊

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ための職務権限のあ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に関する，並びに，理事会枠組み決定 2008/977/JHA の廃止に関する欧州議会及び理事会の 2016 年 4 月 27 日の指令 (EU) 2016/680

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

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，
立法案を国内議会に送付した後，
地域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]，

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the Committee of the Regions [(1)],
Acting in accordance with the ordinary legislative procedure [(2)],

Whereas:

(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。欧州連合の基本権憲章（「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。

The protection of natural persons in relation to the processing of personal data is a fundamental right.

[1] OJ C 391, 18.12.2012, p. 127.
[2] 欧州議会の 2014 年 3 月 12 日付け意見書（官報未搭載）及び理事会の第一読会における 2016 年 4 月 8 日付け意見書（官報未搭載）。欧州議会の 2016 年 4 月 14 日付け意見書.

Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) 自然人の個人データの処理と関連する自然人の保護に関する基本原則及び規定は，それらの者の国籍及び居住地を問わず，それらの者の基本的な権利及び自由，とりわけ，それらの者の個人データの保護の権利を尊重すべきである。この指令は，自由，保安及び法務の領域の達成のために貢献することを意図している。

The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.

(3) 急速な技術発展及びグローバリゼーションは，個人データの保護に関し，新たな検討課題をもたらした。個人データの収集及び共有の規模は，次第に大きなものとなってきている。技術は，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ような活動を遂行するために，かつてない規模で個人データが処理されることを許容している。

Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) 欧州連合内における公共の保安に対する脅威に抗する防護及び防止を含め，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の職務権限を有する機関の間における個人データの支障のない流れ並びにそのような個人データの第三国及び国際組織への移転は，高いレベルの個人データの保護を確保しつつ促進されるべきである。それらの発展は，強力な執行によって支えられた，欧州連合内における個人データの保護のためのより強力かつより一貫性のある枠組みの構築を必要としている。

The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.

(5) 欧州議会及び理事会の指令 95/46/EC[3]は，公的部門及び民間部門の両者において，構成国内の全ての個人データ処理に適用される。ただし，この指令は，刑事における法務上の協力及び警察の協力の分野における活動のような欧州共同体法の適用範囲外にある活動の過程における個人データの処理には適用されない。

Directive 95/46/EC of the European Parliament and of the Council(3) applies to all processing of personal data in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities in the areas of judicial cooperation in criminal matters and police cooperation.

(6) 理事会枠組み決定 2008/977/JHA[4]は，刑事における法務上の協力及び警察の協力の分野に適用される。同枠組み決定の適用範囲は，構成国の間で送付され，または，利用できるようにされる個人データの処理に限定される。

Council Framework Decision 2008/977/JHA(4) applies in the areas of judicial cooperation in criminal matters and police cooperation. The scope of application of that Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) 自然人の個人データの一貫性のある高いレベルの保護を確保すること，及び，構成国の職務権限のある機関の間の個人データの交換を容易にすることは，刑事における実効的な法務上の協力及び警察の協力を確保するために必須である。その目的のために，公共の保安に対する脅威に抗する防護及び防止を含め，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の職務権限のある機関による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のレベルは，全ての構成国の間において均等なものとすべきである。欧州連合全域における個人データの実効的な保護は，データ主体の権利を強化すること，個人データを処理する者の義務を強化すること，並びに，構成国内における個人データの保護のための規定の遵守を監視及び確保するための均等な権限を必要とする。

Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that end, the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation,

[3] 個人データの処理と関連する個人の保護及びそのデータの支障のない移動に関する欧州議会及び理事会の 1995 年 10 月 24 日の指令 95/46/EC（OJ L 281, 23.11.1995, p. 31）.
[4] 刑事における警察及び法務上の協力の枠組み内において処理される個人データの保護に関する理事会の 2008 年 11 月 27 日の枠組み決定 2008/977/JHA（OJ L 350, 30.12.2008, p.60）.

detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should be equivalent in all Member States. Effective protection of personal data throughout the Union requires the strengthening of the rights of data subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

(8) TFEU の第 16 条第 2 項は，欧州議会及び理事会に対し，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及び個人データの支障のない移動に関する規定を定めることを委任している。

Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural person s with regard to the processing of personal data and the rules relating to the free movement of personal data.

(9) そのことを基礎として，欧州議会及び理事会の規則(EU) 2016/679[5]は，個人データの処理との関係において自然人を保護し，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定を定めている。

On that basis, Regulation (EU) 2016/679 of the European Parliament and of the Council[(5)] lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

(10) リスボン条約を採択した政府間会合の最終合意書に附属する刑事における法務上の協力及び警察の協力の分野における個人データの保護に関する第 21 号宣言において，同政府間会合は，これらの分野の特殊な性質のゆえに，TFEU の第 16 条を基礎とする刑事における法務上の協力及び警察の協力の分野における個人データ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必要となり得ることを確認した。

In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.

[5] 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規則(EU) 2016/679（一般データ保護規則）（この官報の 1 頁参照）

(11) それゆえ，これらの分野に関しては，それらの活動の特殊な性質を尊重し，公共の保安に対する脅威に抗する防護及び防止を含め，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の職務権限のあ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に関する特別の規定を定める指令によって対処することが適切である。そのような職務権限のある機関は，法務当局，警察またはそれ以外の法執行機関のような行政機関だけではなく，この指令の目的のために公的権限または公権力を行使することを構成国法によって委ねられている他の組織または法主体をも含み得る。そのような組織または法主体がこの指令の目的以外の目的のために個人データを処理する場合，規則(EU) 2016/679 が適用される。それゆえ，その機関が服する法律上の義務を遵守するため，別の目的のために個人データを収集し，それらの個人データを別の目的のために処理する場合，規則(EU) 2016/679 が適用される。例えば，犯罪行為の捜査，検知または訴追の目的のために，金融機関は，それらの機関によって処理される一定の個人データを保持し，そして，個別の案件において，かつ，構成国法律に従い，職務権限のある国内機関に対してのみ，それらの個人データを提供する。この指令の適用範囲内においてそのような職務権限のある機関の代わりに個人データを処理する組織または法主体は，契約その他の法行為よって，及び，この指令による処理に適用される条項によって拘束されるべきであるが，この指令の適用範囲外にある処理者による個人データの処理に関しては，なお規則(EU) 2016/679 の適用が影響を受けることはない。

It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies. Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive.

(12) 警察またはそれ以外の法執行機関によって遂行される活動は，ある出来事が犯罪行為であるか否かを事前に覚知せずに実施される警察活動を含め，主として，犯罪行為の防止，捜査，検知または訴追に焦点を当てている。そのような活動は，デモ，大規模なスポーツ競技会及び暴動の際の警察活動のように，強制手段を行使することによる権限の行使も含み得る。それらの活動は，公衆の保安に対する脅威及び法律によって保護される社会の基本的な利益に対する脅威であって，犯罪行為を導き得るものとなり得るものに抗する防護とその防止のために必要となる場合において，警察またはそれ以外の法執行機関に与えられた職務として，法と秩序を維持することも含む。構成国は，職務権限のある機関に対し，それが欧州連合法の適用範囲内にある限り，規則(EU) 2016/679 の適用範囲内にあるそれら別の目的のために個人データを処理するため，公共の保管に対する脅威に抗する防護及び防止を含め，犯罪行為の防止，捜査，検知及び訴追並びに刑罰の執行の目的のために遂行する必要性のない別の職務を委任できる。

The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation (EU) 2016/679.

(13) この指令の意味における犯罪行為は，欧州連合の司法裁判所（「司法裁判所」）によって解釈されるものとしての欧州連合法上の自律的な概念とすべきである。

A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union (the ‘Court of Justice’).

(14) 欧州連合法の適用範囲外にある活動の過程における個人データ処理に対してはこの指令を適用してはならないので，国家安全保障と関係する活動，国家安全保障上の問題を取り扱う部局またはユニットの活動，及び，欧州連合条約（TEU）の第 V 款第 2 章の適用範囲内にある活動を遂行する際における構成国による個人データ処理は，この指令の適用範囲内の活動であると判断してはならない。

Since this Directive should not apply to the processing of personal data in the course of an activity

which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive.

(15) 欧州連合全域において法律上執行可能な権利により，自然人の同一のレベルの保護を確保するため，及び，職務権限のある機関の間における個人データの交換を妨げる相違を防止するため，この指令は，公共の保安に対する脅威に抗する防護及び防止を含め，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とその支障のない移動に関する整合化させた規定を定めるべきである。構成国法を近似化させることは，その構成国が与える個人データの保護の低下という結果をもたらしてはならず，それとは逆に，欧州連合内における高いレベルの保護の確保を求めるべきである。構成国は，職務権限のある機関による個人データの処理と関連するデータ主体の権利及び自由の保護に関し，この指令の中で定められるものよりも高度な安全確保を定めることを妨げられてはならない。

In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, this Directive should provide for harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The approximation of Member States' laws should not result in any lessening of the personal data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

(16) この指令は，公文書に対する公衆のアクセスの原則を妨げない。規則(EU) 2016/679 に基づき，公共の利益において実施される職務の遂行のために公的機関または公的組織もしくは民間組織によって保有される公文書中の個人データは，公文書に対する公衆のアクセスと個人データの保護の権利とを均衡させるため，行政機関または組織が服すべき欧州連合法または構成国法に従い，当該行政機関または組織によって開示され得る。

This Directive is without prejudice to the principle of public access to official documents. Under Regulation (EU) 2016/679 personal data in official documents held by a public authority or a public or private body for the performance of a task carried out in the public interest may be disclosed by that authority or body in accordance with Union or Member State law to which the public authority

or body is subject in order to reconcile public access to official documents with the right to the protection of personal data.

(17) この指令によって与えられる保護は，その国籍または居住地の別を問わず，それらの者の個人データの処理との関係において，自然人に対して適用されるべきである。

The protection afforded by this Directive should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

(18) 回避という重大なリスクがつくられる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とすべきであり，かつ，使用される技術に依存してはならない。自然人の保護は，自動化された手段による個人データの処理に適用されるべきであり，かつ，その個人データがファイリングシステムの中に含まれる場合，または，含まれることを予定する場合，手作業による処理に適用されるべきである。特定の基準に従って編成されていないファイルもしくはファイルのセット及びその表紙は，この指令の適用範囲内にあるものとしてはならない。

In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Directive.

(19) 欧州議会及び理事会の規則(EC) No 45/2001[6]は，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に適用される。規則(EC) No 45/2001 及びそのような個人データの処理に適用される欧州連合のその他の法行為は，規則(EU) 2016/679 に定める基本原則及び規定に合わせて調整されるべきである。

Regulation (EC) No 45/2001 of the European Parliament and of the Council(6) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in Regulation (EU) 2016/679.

(20) この指令は，裁判所及びそれ以外の法務当局による個人データの処理との関係において，とりわけ，法務上の判断の中または刑事手続と関連する記録の中に含まれている個人デー

[6] 欧州共同体の機関及び組織による個人データの処理と関連する個人の保護及びそのデータの支障のない移動に関する欧州議会及び理事会の 2000 年 12 月 18 日の規則(EC) No 45/2001（OJ L 8, 12.1. 2001, p.1）.

タに関し，構成国が，刑事手続に関する国内規定の中で処理業務及び処理手続の細目を定めることを妨げない。

This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings.

(21) 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と関係する全ての情報に適用されるべきである。ある自然人が識別可能であるか否かを判断するために，選別のような，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るべきである。自然人を識別するためにどのような手段が用いられる合理的な可能性があるかを確かめるため，処理の時点で利用可能な技術及び技術の発展を考慮に入れた上で，識別同定のために要する費用及び時間量のような全ての客観的要素を判断に入れるべきである。それゆえ，匿名化された情報，すなわち，識別された自然人もしくは識別可能な自然人と関連しない情報またはデータ主体が識別されないような態様で匿名化された個人データに対しては，データ保護の基本原則を適用してはならない。

The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable.

(22) 税務当局及び税関当局，金融情報ユニット，独立行政機関，または，証券市場の規制及び監視の職責を負う金融市場監視機関のような，その機関の公的な任務の遂行のために法律上の義務に従って個人データの開示を受ける行政機関は，欧州連合法または構成国法に従い，一般的な利益における特別の調査を実施するために必要となる個人データをそれらの機関が受領する場合，取得者であると判断されてはならない。行政機関から送付される開示要請は，常に，書面により，理由を付した個別的なものとすべきであり，かつ，ファイリングシステム全体に関するものであってはならず，ファイリングシステムへの相互接続を導くものであってもならない。それらの行政機関による個人データ処理は，その処理の目的に従って適用されるデータ保護の規定を遵守すべきである。

Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data protection rules according to the purposes of the processing.

(23) 遺伝子データは，自然人の，受け継がれまたは獲得された遺伝的な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唯一無二の情報を与えるものであり，かつ，当の自然人から得られた生化学資料の分析，とりわけ，染色体，デオキシリボ核酸（DNA）またはリボ核酸（RNA）の分析から得られ，または，均等な情報を得ることを可能とする他の要素の分析から得られるものとして定義されるべきである。遺伝子情報の複雑性及び機微性を考慮すると，管理者による様々な目的のための濫用または二次利用の大きなリスクが存在する。遺伝上の特性を基礎とするいかなる差別も，原則として，禁止されるべきである。

Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of that natural person and which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained. Considering the complexity and sensitivity of genetic information, there is a great risk of misuse and re-use for various purposes by the controller. Any discrimination based on genetic features should in principle be prohibited.

(24) 健康と関係する個人データは，あるデータ主体の健康状態と関係し，そのデータ主体の過去，現在及び未来の身体の状態または精神の状態と関連する情報を明らかにする全てのデータを含めるべきである。このデータは，欧州議会及び理事会の指令 2011/24/EU[7]に示す当該自然人に対する医療サービスのための登録過程で，または，そのサービスの提供過程で収集される自然人に関する情報；医療上の目的で自然人を唯一無二に識別するために自然人に対して特に割り当てられた番号，シンボルまたは個別項目；遺伝子データ及び生化学資料を含め，身体の一部または身体構成物質の試験もしくは検査から得られる情報；並びに，例えば，医師またはそれ以外の医療専門職，病院，医療機器または試験管内での診療検査のような，当該情報の情報源の別を問わず，例えば，データ主体の疾病，障害，疾病リスク，

[7] 国境を越える医療における患者の権利の適用に関する欧州議会及び理事会の 2011 年 3 月 9 日の指令 2011/24/EU（OJ L 88, 4.4.2011, p. 45）.

病歴，診療または精神状態もしくは生体医療上の状態を示す全ての情報を含む。

Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council(7) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(25) 全ての構成国は，国際刑事警察機構（Interpol）と連携している。その任務を果たすため，Interpol は，国際的な犯罪の防止及びそれとの闘いにおいて職務権限のある機関を支援するために個人データを取得し，記録保存し，及び，回覧に供する。それゆえ，個人データの自動的な処理と関連する基本的な権利及び自由に対する尊重を確保しつつ，個人データの効率的な交換を促進することにより，欧州連合と Interpol との間の協力関係を強化することが適切である。欧州連合から Interpol に対して個人データが移転される場合，及び，Interpol に参加している国々に対して移転される場合，この指令，とりわけ，国際的な移転に関する条項が適用されるべきである。この指令は，理事会共通見解 2005/69/JHA[8]及び理事会決定 2007/533/JHA[9]に定める特別の規定を妨げてはならない。

All Member States are affiliated to the International Criminal Police Organisation (Interpol). To fulfil its mission, Interpol receives, stores and circulates personal data to assist competent authorities in preventing and combating international crime. It is therefore appropriate to strengthen cooperation between the Union and Interpol by promoting an efficient exchange of personal data whilst ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. Where personal data are transferred from the Union to Interpol, and to countries which have delegated members to Interpol, this Directive, in particular the provisions on international transfers, should apply. This Directive should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA(8) and Council Decision 2007/533/JHA(9).

---

[8] 一定のデータの Interpol との交換に関する 2005 年 1 月 24 日の理事会共通見解 2005/69/JHA（OJ L 27, 29.1.2005, p.61）.

[9] 第 2 世代シェンゲン情報システム（SIS II）の設置，運用及び利用に関する 2007 年 6 月 12 日の理事会決定 2007/533/JHA（OJ L 205, 7.8.2007, p.63）.

(26) いかなる個人データ処理も，適法であり，公正であり，かつ，関係する自然人との関係において透明性をもつものでなければならず，かつ，法律によって定められた特定の目的のためにのみ処理されなければならない。このことは，それ自体としては，隠密の捜査またはビデオ監視のような活動を法執行機関が行うことを妨げない。そのような活動は，それらの活動が法律によって定められており，かつ，関係する自然人の正当な利益を適正に尊重する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ものである限り，公共の保安に対する脅威に抗する防護及び防止を含め，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行われ得る。公正な処理というデータ保護の基本原則は，憲章第 47 条及び人権及び基本的な自由の保護に関する欧州条約（ECHR）第 6 条に定義する公正な法廷の権利とは異なる概念である。自然人は，その者の個人データの処理と関係するリスク，規定，安全確保及び権利について，並びに，その処理と関係するその者の権利をどのように行使するかについて知らされるべきである。とりわけ，個人データが処理される個々の目的は，その個人データの収集の時点において，明示かつ適法かつ確定的なものとすべきである。個人データは，そのデータが処理される目的にとって十分であり，かつ，関連性のあるものとすべきである。とりわけ，収集される個人データが過剰ではないこと，及び，そのデータが処理される目的のために必要な期間を超えて保存されないことが確保されるべきである。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充足され得ない場合に限り，処理されるべきである。そのデータが必要な期間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るべきである。構成国は，公共の利益におけるアーカイブ，科学，統計または歴史の利用のためにより長期間にわたって記録保存される個人データに関し，適切な安全確保を定めるべきである。

Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of

the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.

(27) 犯罪行為の防止，捜査及び訴追のため，職務権限のある機関は，特定の犯罪行為の防止，捜査，検知または訴追の過程において収集される個人データを処理する必要があり，また，その過程以外にも，犯罪活動の理解を発展させるため，そして，検知された異なる犯罪行為の間の関連づけを行うために，収集された個人データを処理する必要がある。

For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.

(28) 処理と関係する安全性を維持し，かつ，この指令に違反する処理を防止するため，個人データは，個人データ及びその処理のために使用される機器への無権限アクセスまたはその無権限利用を防止することによる場合を含め，適切なレベルの安全性及び機密性を確保し，かつ，保護されるべき個人データのリスク及び性質との関係において利用可能な最新技術並びに実装費用を考慮に入れた態様で処理されるべきである。

In order to maintain security in relation to processing and to prevent processing in infringement of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including by preventing unauthorised access to or use of personal data and the equipment used for the processing, and that takes into account available state of the art and technology, the costs of implementation in relation to the risks and the nature of the personal data to be protected.

(29) 個人データは，この指令の適用範囲内において，特定の，明示かつ正当な目的のために収集されるべきであり，かつ，公共の保安に対する脅威に抗する防護及び防止を含め，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と適合しない目的のために処理されてはならない。その個人データが収集された目的とは異なる目的のために，この指令の適用範囲内にある目的のための同一の管理者または別の管理者によって個人データが処理される場合，そのような処理は，適用可能な法令の条項に従ってそのような処理が認められること，及び，当該別の目的にとって必要かつ比例的なものであることを条件として，許容されるべきである。

Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with the purposes of the

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. If personal data are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose.

(30) データの正確性の原則は，関係する処理の性質及び目的を考慮に入れた上で適用されるべきである。とりわけ，法務上の手続において，個人データを含む文言は，自然人の主観的な知覚を基礎とするものであり，常に検証可能であるとは限らない。従って，正確性の要求は，文言の正確性に関するものではなく，単に，ある特定の文言が作成されたという事実に関するものとすべきである。

The principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(31) 刑事における法務上の協力及び警察の協力の分野における個人データの処理において，異なる類型のデータ主体に関する個人データが処理されることは，本来的なものである。それゆえ，それが適用可能なときは，かつ，可能な限り，被疑者；犯罪行為により有罪判決を受けた者；被害者や証人のような第三者；関連情報をもつ者または接触をもつ者；被疑者または有罪判決を受けた者の関係者のような，異なる類型のデータ主体の個人データの間に明確な区分が設けられるべきである。このことは，司法裁判所及び欧州人権裁判所の判例法によってそれぞれ解釈されているように，憲章及び ECHR によって保障されているものとしての無罪の推定の権利の適用を妨げてはならない。

It is inherent to the processing of personal data in the areas of judicial cooperation in criminal matters and police cooperation that personal data relating to different categories of data subjects are processed. Therefore, a clear distinction should, where applicable and as far as possible, be made between personal data of different categories of data subjects such as: suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses; persons possessing relevant information or contacts; and associates of suspects and convicted criminals. This should not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively.

(32) 職務権限のある機関は，不正確な個人データ，不完全な個人データまたは最新のものでは

ない個人データが送付されまたは利用できるようにされないことを確保すべきである。自然人の保護，送付されまたは利用できるようにされた個人データの正確性，完全性または個人データが最新のものとされる範囲並びにその個人データの信頼性を確保するため，職務権限のある機関は，可能な限り，個人データの全ての送付の際，必要な情報を付加すべきである。

The competent authorities should ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In order to ensure the protection of natural persons, the accuracy, completeness or the extent to which the personal data are up to date and the reliability of the personal data transmitted or made available, the competent authorities should, as far as possible, add necessary information in all transmissions of personal data.

(33) この指令が構成国の法律，法律上の根拠または立法措置に言及する場合，そのことは，関係する構成国の憲法秩序による要件を妨げることなく，議会によって採択される法行為であることを必ずしも要求していない。ただし，そのような構成国の法律，法律上の根拠または立法措置は，司法裁判所及び欧州人権裁判所の判例法によって要求されているように，それらに服する者にとって明確であり，詳細であり，かつ，その適用が予測可能なものとすべきである。この指令の適用範囲内にある個人データの処理を規律する構成国法は，少なくとも，適用対象，処理される個人データ，処理の目的，個人データの完全性及び機密性を保つための手続，そのデータの破壊のための手続を定めるべきであり，そして，濫用や恣意のリスクに抗する十分な保障を提供すべきである。

Where this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

(34) 公共の保安に対する脅威に抗する防護及び防止を含め，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の職務権限のある機関による個人データの処理は，自動的な手段によるかそれ以外の手段によるかの別を問わず，収集，記録，編集，構成，記録保存，修正もしくは変更，検索，照会，使用，整列もしくは結合，処理の制限，削除または破壊のような，それらの目的のために個人データまたは個人データのセットに基づいて遂行される全ての業務遂行または業務遂行のセットを包摂すべきである。とりわけ，この指令の規

定は，この指令に服さない取得者に対するこの指令の目的のための個人データの移転に適用されるべきである。そのような取得者は，職務権限のある機関によって個人データが適法に開示される自然人または法人，行政機関，部局もしくはそれら以外の組織を包含する。この指令の目的中のいずれかのために職務権限のある機関によって最初に個人データが収集された場合，そのような処理が欧州連合法または構成国法によって認められる限り，この指令の目的以外の目的のための当該データの処理に対し，規則(EU) 2016/679 が適用されるべきである。とりわけ，この指令の適用範囲外にある目的のための個人データの送付に関し，規則(EU) 2016/679 の規定が適用される。職務権限のある機関ではない取得者またはこの指令の意味の範囲内にあるような活動をする者ではない取得者，及び，職務権限のある機関から個人データが適法に開示される取得者による個人データの処理に関しては，規則(EU) 2016/679 が適用されるべきである。この指令を実装しつつ，構成国は，規則(EU) 2016/679 に定める要件に従い，同規則の規定の適用の細則を定める得るべきである。

The processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction. In particular, the rules of this Directive should apply to the transmission of personal data for the purposes of this Directive to a recipient not subject to this Directive. Such a recipient should encompass a natural or legal person, public authority, agency or any other body to which personal data are lawfully disclosed by the competent authority. Where personal data were initially collected by a competent authority for one of the purposes of this Directive, Regulation (EU) 2016/679 should apply to the processing of those data for purposes other than the purposes of this Directive where such processing is authorised by Union or Member State law. In particular, the rules of Regulation (EU) 2016/679 should apply to the transmission of personal data for purposes outside the scope of this Directive. For the processing of personal data by a recipient that is not a competent authority or that is not acting as such within the meaning of this Directive and to which personal data are lawfully disclosed by a competent authority, Regulation (EU) 2016/679 should apply. While implementing this Directive, Member States should also be able to further specify the application of the rules of Regulation (EU) 2016/679, subject to the conditions set out therein.

(35) 公共の保安に対する脅威に抗する防護及び防止を含め，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欧州連合法または構成国法に基づき職務権限のある機関によって公共の利益において実施される職務の遂行に関し，適法であるためには，この指令に基づく個人データの処理を要するものとすべきである。それらの活動は，データ主体の生存の利益の保護を包摂すべきである。法律によって職務権限のある機関に対

して組織的に与えられている犯罪行為の防止，捜査，検知または訴追の職務の遂行は，その職務権限のある機関が，自然人に対して，命ぜられたことに従うことを要求または命令することを許容する。そのような場合，規則(EU) 2016/679 に定義されているようなデータ主体の同意は，職務権限のある機関による個人データの処理のための法律上の根拠を提供するものとしてはならない。データ主体が法律上の義務を遵守すべきことを要求される場合，データ主体の反応が彼または彼女の意思の任意に与えられた表示であると判断され得ないようにするため，そのデータ主体は，真の意味での選択の自由を全くもたない。このことは，犯罪捜査の際の DNA 検査または刑罰の執行のための電子タグによる彼もしくは彼女の所在場所監視のような，この指令の目的のための彼または彼女の個人データの処理に対してデータ主体が同意できることを，法律によって，構成国が定めることを妨げてはならない。

In order to be lawful, the processing of personal data under this Directive should be necessary for the performance of a task carried out in the public interest by a competent authority based on Union or Member State law for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Those activities should cover the protection of vital interests of the data subject. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.

(36) 送付元である職務権限のある機関に対して適用可能な欧州連合法または構成国法が，取扱いコードの使用のような，特別の状況において個人データの処理に適用される特別の条件を定めている場合，構成国は，送付元である職務権限のある機関が，そのような個人データの取得者に対し，それらの条件及びそれらの条件を尊重する必要性を連絡すべきことを定めるべきである。そのような条件は，例えば，更に別の者に対して個人データを転送することの禁止，または，取得者に対してそれらの個人データが送付された目的以外の別の目的のためにそれらの個人データを利用することの禁止，または，情報提供を受ける権利の制限がある場合において，送付元である職務権限のある機関の事前の承認なしに，データ主体に対して情報提供することの禁止を含み得る。それらの義務は，送付元である職務権限のある機関から第三国または国際組織の取得者に対する送付にも適用されるべきである。構成国は，他の構成国の取得者に対し，または，TFEU の第 V 款第 4 章及び第 5 章によって設け

られた部局，事務局もしくは組織である取得者に対して，送付元である職務権限のある機関が，当該職務権限のある機関の構成国内において同様のデータの送付に適用可能な条件以外の別の条件を適用しないことを確保すべきである。

Member States should provide that where Union or Member State law applicable to the transmitting competent authority provides for specific conditions applicable in specific circumstances to the processing of personal data, such as the use of handling codes, the transmitting competent authority should inform the recipient of such personal data of those conditions and the requirement to respect them. Such conditions could, for example, include a prohibition against transmitting the personal data further to others, or using them for purposes other than those for which they were transmitted to the recipient, or informing the data subject in the case of a limitation of the right of information without the prior approval of the transmitting competent authority. Those obligations should also apply to transfers by the transmitting competent authority to recipients in third countries or international organisations. Member States should ensure that the transmitting competent authority does not apply such conditions to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar data transmissions within the Member State of that competent authority.

(37) その個人データの性質上，基本的な権利及び自由との関係において特に機微性のある個人データは，その個人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ので，特別の保護を享受する。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べきであるが，この指令中で「人種的な出自」という語を用いることは，区分された人種の存在を確定しようと試みる理論を欧州連合が承認していることを含意しない。その処理が，法律によって定められているデータ主体の権利及び自由を守るための適切な安全確保に服し，かつ，法律によって認められている場合に許容される場合；または，そのような法律によってまだ認められていないときは，その処理が，データ主体または第三者の生存の利益を保護するために必要な場合；または，データ主体によって公開されたことが明白なデータと関連する処理の場合を除き，そのような個人データは，処理されてはならない。データ主体の権利及び自由の適切な安全確保は，関係する自然人に関する他のデータとの関係においてのみそれらのデータを収集し得ること，適切に収集されたデータを防護し得ること，職務権限のある機関の職員のデータへのアクセスに関するより厳格な規則，及び，そのようなデータの移転の禁止を含め得る。そのようなデータの処理は，彼または彼女にとって格別に侵害的な処理にデータ主体が明示で同意をしている場合においても，法律によって，許容されるべきである。ただし，データ主体の同意は，それ自体としては，職務権限のある機関によるそのような機微の個人データの処理のための法律上の根拠を提供するものとしてはならない。

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to

the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Directive does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. Such personal data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.

(38) データ主体は，自動化された処理のみを基礎とし，かつ，彼もしくは彼女に関して不利な法律上の効果を発生させ，または，彼もしくは彼女に重大な影響を与える，彼または彼女の人格的側面を評価する判定に服さない権利をもつべきである。いかなる場合においても，そのような処理は，とりわけ，彼または彼女の見解を表明するため，そのような評価の後に達した判定の説明を得るため，または，その判定に対して不服を申立てるため，データ主体に対する個別の情報提供及び人間の関与を得る権利を含め，適切な安全確保に服すべきである。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性のある個人データを基礎とする自然人にとって不利益な差別をもたらすプロファイリングは，憲章の第 21 条及び第 52 条に定める条件の下で禁止されるべきである。

The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions laid down in Articles 21 and 52 of the Charter.

(39) 彼または彼女の権利を彼または彼女が行使できるようにするため，データ主体に対する情報提供は，管理者の Web サイトを含め，容易にアクセス可能であり，かつ，明解かつ平易な言語を用い，理解しやすいものとすべきである。そのような情報提供は，児童のような脆弱な

者の必要性に応じて調整されるべきである。

In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language. Such information should be adapted to the needs of vulnerable persons such as children.

(40) とりわけ，個人データに対するアクセス及びその訂正もしくは削除並びに処理の制限を求めるための仕組み，そして，それが適用可能なときは，無料でそれらを得る仕組みを含め，この指令により採択される条項に基づくデータ主体の権利の行使を容易にするための様式が定められるべきである。この指令に従って管理者がデータ主体の権利に制限を適用する場合を除き，管理者は，データ主体からの求めに対して，不適切な遅滞なく，対応することを義務付けられるべきである。更に，データ主体が，合理性なく，反復して，情報提供を求めるような場合，または，例えば，それを求める際，虚偽の情報または誤解させる情報を提供することによって，データ主体が彼または彼女の情報提供を受ける権利を濫用している場合のように，求めが明らかに根拠のないものであるかまたは過剰なものであるときは，管理者は，合理的な手数料を課金し，または，その要求にかかる行動を拒否できるべきである。

Modalities should be provided for facilitating the exercise of the data subject's rights under the provisions adopted pursuant to this Directive, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and restriction of processing. The controller should be obliged to respond to requests of the data subject without undue delay, unless the controller applies limitations to data subject rights in accordance with this Directive. Moreover, if requests are manifestly unfounded or excessive, such as where the data subject unreasonably and repetitiously requests information or where the data subject abuses his or her right to receive information, for example, by providing false or misleading information when making the request, the controller should be able to charge a reasonable fee or refuse to act on the request.

(41) 管理者が，データ主体の同一性を確認するために必要となる付加的な情報の提供を求める場合，当該情報は，当該個別の目的のためにのみ処理されるべきであり，かつ，当該目的のために必要な期間を超えて記録保存してはならない。

Where the controller requests the provision of additional information necessary to confirm the identity of the data subject, that information should be processed only for that specific purpose and should not be stored for longer than needed for that purpose.

(42) 少なくとも以下の情報は，データ主体が利用できるようにされるべきである：すなわち，管理者の識別名，処理業務の存在，処理の目的，異議を述べる権利，並びに，個人データへの

アクセス，その訂正または削除，または，その処理の制限を管理者に対して求める権利の存在である。これは，職務権限のある機関の Web サイト上で行われ得る。加えて，個別の案件において，かつ，彼または彼女の権利を行使できるようにするため，そのデータが処理される個別の状況を考慮に入れた上で，そのデータ主体との関係において公正な処理を保証するためにそのような別の情報が必要となる範囲内で，データ主体は，その処理の法律上の根拠，及び，どれだけの期間そのデータが保存されるのかについて，情報提供を受けるべきである。

At least the following information should be made available to the data subject: the identity of the controller, the existence of the processing operation, the purposes of the processing, the right to lodge a complaint and the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing. This could take place on the website of the competent authority. In addition, in specific cases and in order to enable the exercise of his or her rights, the data subject should be informed of the legal basis for the processing and of how long the data will be stored, in so far as such further information is necessary, taking into account the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

(43) 自然人は，彼または彼女に関して収集されたデータにアクセスする権利をもつべきであり，かつ，その処理を認識し，その処理の適法性を検証するため，容易かつ合理的な間隔でその権利を行使すべきである。それゆえ，全てのデータ主体は，そのデータが処理される目的，そのデータが処理される期間，及び，第三国の取得者を含め，そのデータの取得者に関して知り，かつ，その連絡を受ける権利をもつべきである。そのような連絡が個人データの入手元に関する情報を含む場合，その情報は，特に機密の情報源内の，自然人の識別名を明らかにしてはならない。この権利が充足されるようにするためには，理解しやすい方式により，換言すると，この指令によって彼または彼女に対して与えられた権利を彼または彼女が行使できるようにするため，データ主体がそれらのデータを覚知し，当該データが正確であり，かつ，この指令に従って処理されていることを検証できるような方式により，それらのデータ全部の要旨をデータ主体がもつことで十分である。そのような要旨は，現在処理されている個人データの複製物という方式で提供され得る。

A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know, and obtain communications about, the purposes for which the data are processed, the period during which the data are processed and the recipients of the data, including those in third countries. Where such communications include information as to the origin of the personal data, the information should not reveal the identity of natural persons, in particular confidential sources. For that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an

intelligible form, that is to say a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with this Directive, so that it is possible for him or her to exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing.

(44) 構成国は，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を避けるため，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妨げを避けるため，公共の保安の防護または国家安全保障のため，または，それら以外の者の権利及び自由を保護するため，関係する自然人の基本的な権利及び正当な利益を適正に尊重した上で，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ような措置の範囲内において，かつ，その限りで，データ主体に対する情報提供を遅延させ，制限し，または，省略する立法措置を採択し，または，その個人データに対するアクセスの全部または一部を制限する立法措置を採択すべきである。管理者は，個々の案件の具体的かつ個別的な検討により，アクセスの権利の全部または一部を制限すべきか否かを評価すべきである。

Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others. The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted.

(45) アクセスの拒否または制限は，原則として，データ主体宛の書面の中で定められるべきであり，かつ，その決定が基礎とする事実上の理由または法律上の理由を含めるべきである。

Any refusal or restriction of access should in principle be set out in writing to the data subject and include the factual or legal reasons on which the decision is based.

(46) データ主体の権利の制限は，司法裁判所及び欧州人権裁判所の判例法においてそれぞれ解釈されているように，憲章及び ECHR を遵守しなければならず，かつ，とりわけ，データ主体の権利及び自由の本質部分を尊重しなければならない。

Any restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.

(47) とりわけ，そのデータが事実に関するものである場合，自然人は，彼または彼女に関する不正確な個人データの訂正を得る権利をもち，かつ，そのようなデータの処理がこの指令の違反となる場合，削除の権利をもつべきである。ただし，訂正の権利は，例えば，証人の証言内容に影響を与えるべきではない。自然人は，彼または彼女が個人データの正確性について疑義を提示しており，かつ，その個人データが正確もしくは不正確が確認され得ない場合，または，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においても，処理の制限の権利をもつべきである。とりわけ，個別の案件において，削除することがデータ主体の正当な利益を害し得ると信ずる合理的な根拠が存在する場合，個人データを削除するのではなく，処理が制限されるべきである。そのような場合，制限を受けるデータは，そのデータの削除を防止する目的のために限り，処理されるべきである。個人データの処理を制限する手法は，就中，例えば，アーカイブの目的のために，選別されたデータを別の処理システムに移動させること，または，選別されたデータを利用できないようにすることを含め得る。自動化された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，技術的な手段によって確保されるべきである。個人データの処理が制限されているという事実は，その個人データの処理が制限されていることが明確となるような態様で，そのシステム内で表示されるべきである。そのような個人データの訂正もしくは削除または処理の制限は，そのデータの開示を受けた取得者に対し，及び，その不正確なデータの入手元である職務権限のある機関に対し，連絡されるべきである。また，管理者は，そのようなデータを別の者に伝達することを控えるべきである。

A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular where it relates to facts, and the right to erasure where the processing of such data infringes this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person should also have the right to restriction of processing where he or she contests the accuracy of personal data and its accuracy or inaccuracy cannot be ascertained or where the personal data have to be maintained for purpose of evidence. In particular, instead of erasing personal data, processing should be restricted if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In such a case, restricted data should be processed only for the purpose which prevented their erasure. Methods to restrict the processing of personal data could include, inter alia, moving the selected data to another processing system, for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing should in principle be ensured by technical means. The fact that the processing of personal data is restricted should be indicated in the system in such a manner that it is clear that the processing of the personal data is restricted. Such rectification or erasure of personal data or restriction of processing should be communicated to recipients to whom the data have been disclosed and to the competent authorities from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data.

(48) 管理者が，データ主体に対し，彼または彼女の情報提供を受ける権利，個人データへのアクセスの権利，個人データの訂正もしくは削除の権利または処理の制限の権利を拒否する場合，そのデータ主体は，国内監督機関に対し，その処理の適法性の確認を求める権利をもつべきである。データ主体は，その権利の情報提供を受けるべきである。監督機関がデータ主体の代わりに行動する場合，そのデータ主体は，その監督機関から，少なくとも，監督機関によって全ての必要な確認または評価が行われたことの情報提供を受けるべきである。監督機関は，データ主体に対し，法務上の救済の権利についても情報提供すべきである。

Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. The data subject should be informed of that right. Where the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place. The supervisory authority should also inform the data subject of the right to seek a judicial remedy.

(49) 犯罪捜査の過程及び刑事における裁判所の手続の過程において個人データが処理される場合，構成国は，情報提供を受ける権利，個人データへアクセスする権利，個人データの訂正もしくは削除の権利または処理の制限の権利の行使が，法務上の手続に関する国内規定に従って遂行されることを定め得るべきである。

Where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States should be able to provide that the exercise the right to information, access to and rectification or erasure of personal data and restriction of processing is carried out in accordance with national rules on judicial proceedings.

(50) 管理者によって，または，管理者の代わりの者によって遂行される個人データの処理に関し，管理者の職責と法的責任が定められるべきである。とりわけ，管理者は，適切かつ実効的な措置の実装を義務づけられるべきであり，かつ，当該処理活動がこの指令を遵守していることを説明できるべきである。そのような措置は，その処理の性質，範囲，処理過程及び目的，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べきである。管理者によって講じられる措置は，児童のような脆弱な自然人の個人データの取扱いに関する特別の安全確保の策定及び実装を含めるべきである。

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and should be able to demonstrate that processing activities are in compliance with this Directive. Such measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of

natural persons. The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children.

(51) 自然人の権利及び自由に対する様々な蓋然性と深刻度のリスクは，データの処理から生じ得る。それは，物的な損失，財産上の損失もしくは非財産的な損失を導き得るものであり，とりわけ：その処理が，差別，ID 窃盗または ID 詐欺，金銭的損失，信用の毀損，職務上の秘密によって保護されているデータの機密性の喪失，仮名の無権限復元，または，それら以外の経済的または社会的な大きな不利益を生じさせ得る場合；データ主体がその権利及び自由を奪われ，または，それらの者個人データに対する管理の実行を奪われる場合；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が実施される場合；個人を唯一無二に識別するために遺伝子データまたは生体要素データが処理される場合，または，健康と関係するデータ，または，性生活及び性的指向，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が処理される場合；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または利用するために，職場における職務遂行能力，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，所在地もしくは移動を分析または予測する場合；脆弱な自然人の個人データ，とりわけ，児童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影響を及ぼす場合がそうである。

The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed; where personal aspects are evaluated, in particular analysing and predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(52) リスクの蓋然性及びその深刻度は，その処理の性質，範囲，処理過程及び目的に照らして判断されるべきである。リスクは，データ処理業務が高度なリスクを含むものか否かが確定される客観的な評価を基礎として評定されるべきである。高度なリスクとは，データ主体の権利

及び自由を妨げる特別のリスクのことである。

The likelihood and severity of the risk should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, through which it is established whether data-processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.

(53) 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，この指令の要件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。そのような措置の実装は，経済的な配慮のみに依拠してはならない。この指令の遵守を説明できるようにするため，管理者は，内部の基本方針を採択すべきであり，かつ，とりわけ，バイデザインのデータ保護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すべきである。管理者がこの指令に従ってデータ保護影響評価を行う場合，その評価結果は，それらの措置及び手続がいつ策定されたものであるのかを考慮に入れるべきである。その措置は，就中，可能な限り早期の仮名化の利用によって構成され得る。この指令の目的のために仮名化を利用することは，とりわけ，自由，保安及び法務の領域における個人データの支障のない流れを容易にし得るようなツールを提供し得る。

The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures are taken, to ensure that the requirements of this Directive are met. The implementation of such measures should not depend solely on economic considerations. In order to be able to demonstrate compliance with this Directive, the controller should adopt internal policies and implement measures which adhere in particular to the principles of data protection by design and data protection by default. Where the controller has carried out a data protection impact assessment pursuant to this Directive, the results should be taken into account when developing those measures and procedures. The measures could consist, inter alia, of the use of pseudonymisation, as early as possible. The use of pseudonymisation for the purposes of this Directive can serve as a tool that could facilitate, in particular, the free flow of personal data within the area of freedom, security and justice.

(54) 管理者が別の管理者と共同で処理の目的及び方法を決定する場合及び処理業務が管理者の代わりの者によって実施される場合を含め，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，監督機関による監視及び監督機関の措置との関係においても，この指令に定める責任の帰属の明確な配分を要求する。

The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities set out in this Directive, including where

a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(55) 処理者による処理の遂行は，処理者と管理者との間で結ばれ，かつ，とりわけ，管理者の指示に基づいてのみ処理者が行動すべきことを定める契約を含め，法行為によって規律されるべきである。処理者は，バイデザイン及びバイデフォルトによるデータ保護の原則を考慮に入れるべきである。

The carrying-out of processing by a processor should be governed by a legal act including a contract binding the processor to the controller and stipulating, in particular, that the processor should act only on instructions from the controller. The processor should take into account the principle of data protection by design and by default.

(56) この指令の遵守を説明するため，管理者または処理者は，その職責の下において，全ての類型の処理活動に関する記録を維持管理すべきである。各管理者または処理者は，監督機関に協力する義務を負うべきであり，かつ，監督機関がそれらの処理業務の監視のために役立て得るようにするため，要求に応じてそれらの記録を利用できるようにすべきである。自動化されていない処理システム内にある個人データを処理する管理者または処理者は，履歴またはそれ以外の方式による記録のような，処理の適法性を説明し，自己監視できるようにし，そして，データの完全性及びデータの安全性を確保する実効的な方策を設けるべきである。

In order to demonstrate compliance with this Directive, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records available to it on request, so that they might serve for monitoring those processing operations. The controller or the processor processing personal data in non-automated processing systems should have in place effective methods of demonstrating the lawfulness of the processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(57) 少なくとも，収集，修正，照会，移転を含む開示，結合または削除のような自動化された処理システム内の業務遂行に関し，履歴（ログ）が保存されるべきである。個人データを参照した者または個人データの開示を受けた者の識別子は，履歴に記録されるべきであり，かつ，当該識別子から，その処理業務の正当性を確認できるべきである。履歴は，処理の適法性の検証，自己監視，データの完全性及びデータの安全性の確保，並びに，刑事手続のために限り，利用されるべきである。自己監視は，職務権限のある機関の内部的な懲戒手続も含める。

Logs should be kept at least for operations in automated processing systems such as collection,

alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged and from that identification it should be possible to establish the justification for the processing operations. The logs should solely be used for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.

(58) その処理業務の性質，範囲または目的によってデータ主体の権利及び自由に対する高度なリスクをその処理業務が発生させるおそれがある場合，管理者によってデータ保護影響評価が遂行されるべきである。その影響評価は，とりわけ，個人データの保護を確保し，かつ，この指令の遵守を説明するために準備された措置，安全確保及び仕組みを含めるべきである。影響評価は，関連システム及び処理業務の過程を包摂するが，個々の案件を包摂してはならない。

A data protection impact assessment should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes, which should include, in particular, the measures, safeguards and mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with this Directive. Impact assessments should cover relevant systems and processes of processing operations, but not individual cases.

(59) データ主体の権利及び自由の実効的な保護を確保するため，管理者または処理者は，一定の場合において，処理開始の前に，監督機関と協議すべきである。

In order to ensure effective protection of the rights and freedoms of data subjects, the controller or processor should consult the supervisory authority, in certain cases, prior to the processing.

(60) 安全性を維持し，かつ，この指令に違反する処理を防止するため，管理者または処理者は，その処理に固有のリスクを評価すべきであり，また，暗号化のような，それらのリスクを緩和するための措置を実装すべきである。そのような措置は，機密性を含め，適切なレベルの安全性を確保すべきであり，かつ，そのリスクと関係する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るべきである。データの安全性のリスクを評価する際，送付され，記録保存され，または，それ以外の処理をされる個人データの偶発的もしくは違法な破壊，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，データ処理によって示されるリスク，とりわけ，物理的な損失，財産上の損失もしくは非財産的な損失を導き得るリスクを考慮に入れるべきである。管理者及び処理者は，個人データの処理が無権限の者によって遂行されないことを確保すべきである。

In order to maintain security and to prevent processing that infringes this Directive, the controller or

processor should evaluate the risks inherent in the processing and should implement measures to mitigate those risks, such as encryption. Such measures should ensure an appropriate level of security, including confidentiality and take into account the state of the art, the costs of implementation in relation to the risk and the nature of the personal data to be protected. In assessing data security risks, consideration should be given to the risks that are presented by data processing, such as the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed, which may, in particular, lead to physical, material or non-material damage. The controller and processor should ensure that the processing of personal data is not carried out by unauthorised persons.

(61) 個人データの侵害は，適切かつ適時の態様で対処されない場合，自然人の個人データに対する管理の喪失または自然人の権利の制限，差別，ID 窃盗または ID 詐欺，金銭的な損失，仮名の無権限復元，信用の毀損，職務上の秘密によって保護された個人データの機密性の喪失，または，関係する自然人に対する上記以外の経済的もしくは社会的な大きな不利益のような，自然人に対する物理的な損失，財産上の損失もしくは非財産的な損失をもたらし得る。それゆえ，個人データの侵害が発生したことに管理者が気づいた時は直ちに，その管理者は，監督機関に対し，不適切な遅滞なく，かつ，それが実施可能であるときは，説明責任上の諸原則に従ってその個人データの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可能性がないということを管理者が説明できない限り，それに気づいた時から遅くとも 72 時間以内に，その個人データの侵害を通知すべきである。72 時間以内にそのような通知を完了できない場合，その遅延の理由をその通知に付すべきであり，そして，更なる不適切な遅延なく，同時に，情報を提供できる。

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(62) 個人データの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，その者が予め必要な警戒をできるようにするため，自然人は，不適切な遅滞なく，連絡を受けるべきである。その通知は，個人データの侵害の性質を説明すべきであり，かつ，

潜在的な負の影響を緩和するための，関係する自然人に対する勧告を含めるべきである。データ主体に対する通知は，監督機関と緊密に協力し，かつ，監督機関またはそれ以外の関係機関から提供される運用指針を尊重して，可能な限り早く，合理的に利用できるようにされるべきである。例えば，損害発生の差し迫ったリスクを緩和する必要性があることは，データ主体への連絡を急がせることになる。これに対し，持続的または類似の個人データ侵害に抗する適切な措置を実装する必要性があることは，通知のためにより多くの時間を要することを正当化し得る。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を避けること，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妨げを避けること，公共の保安を防護すること，国家安全保障を防護すること，または，それら以外の者の権利及び自由を保護することが，関係する自然人に対する個人データの侵害の連絡を遅延させ，または，制限することでは達成され得ない場合，例外的な状況において，その連絡は，省略され得る。

Natural persons should be informed without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in order to allow them to take the necessary precautions. The communication should describe the nature of the personal data breach and include recommendations for the natural person concerned to mitigate potential adverse effects. Communication to data subjects should be made as soon as reasonably feasible, in close cooperation with the supervisory authority, and respecting guidance provided by it or other relevant authorities. For example, the need to mitigate an immediate risk of damage would call for a prompt communication to data subjects, whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for the communication. Where avoiding obstruction of official or legal inquiries, investigations or procedures, avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security or protecting the rights and freedoms of others cannot be achieved by delaying or restricting the communication of a personal data breach to the natural person concerned, such communication could, in exceptional circumstances, be omitted.

(63) 裁判所及びそれ以外の独立の法務機関がその機関の法務上の権限を行使する際の適用除外を構成国が定めている場合を除き，管理者は，この指令に従って採択された条項の内部的な遵守を監視においてその管理者を補佐する者を指定すべきである。当該の者は，管理者の既存の職員の一員であって，この分野における専門知識を獲得するためのデータ保護の法律及び実務に関する特別な訓練を受けた者とし得る。専門知識として必要なレベルは，とりわけ，実施されるデータ処理，及び，管理者によって処理される個人データに求められる保護によって決定されるべきである。彼または彼女の仕事は，パートタイムベースでもフルタイムベースでも遂行され得る。データ保護責任者は，例えば，中央当局における共有された資源のように，その者の組織上の構成及び規模を考慮に入れた上で，複数の管理者によって共同で指定され得る。当該の者は，関連する管理者の組織内で異なる立場にある者も指定され得る。当該の者は，関連するデータ保護上の義務の遵守に関し，情報提供及び助

言をすることによって，管理者及び個人データを処理する従業者を支援すべきである。そのようなデータ保護責任者は，構成国法に従い，独立の態様で，その責務及び職務を遂行する地位にあるものとすべきである。

The controller should designate a person who would assist it in monitoring internal compliance with the provisions adopted pursuant to this Directive, except where a Member State decides to exempt courts and other independent judicial authorities when acting in their judicial capacity. That person could be a member of the existing staff of the controller who received special training in data protection law and practice in order to acquire expert knowledge in that field. The necessary level of expert knowledge should be determined, in particular, according to the data processing carried out and the protection required for the personal data processed by the controller. His or her task could be carried out on a part-time or full-time basis. A data protection officer may be appointed jointly by several controllers, taking into account their organisational structure and size, for example in the case of shared resources in central units. That person can also be appointed to different positions within the structure of the relevant controllers. That person should help the controller and the employees processing personal data by informing and advising them on compliance with their relevant data protection obligations. Such data protection officers should be in a position to perform their duties and tasks in an independent manner in accordance with Member State law.

(64) 構成国は，公共の保安に対する脅威に抗する防護及び防止を含め，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ために必要な場合に限り，第三国または国際組織に対する移転が起きることを確保し，かつ，第三国または国際組織内の管理者がこの指令の意味における職務権限のある機関であることを確保すべきである。管理者の代わりに処理者が移転をすることが明示で指示されている場合を除き，職務権限のある機関が管理者として行動する場合に限り，移転が遂行されるべきである。当の第三国または国際組織が十分なレベルの保護を確保していると欧州委員会が判定した場合，適切な安全確保が提供されている場合，または，特別の状況のための特例が適用される場合，そのような移転が起き得る。第三国または国際組織から同一もしくは別の第三国または国際組織の管理者または処理者に対して個人データが転送される場合を含め，欧州連合から第三国または国際組織の管理者，処理者またはそれ以外の取得者に対して個人データが移転される場合，この指令によって欧州連合内において定められている自然人の保護のレベルが損なわれてはならない。

Member States should ensure that a transfer to a third country or to an international organisation takes place only if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and that the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer should be carried out only by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. Such a transfer may take place in cases where the Commission has

decided that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply. Where personal data are transferred from the Union to controllers, to processors or to other recipients in third countries or international organisations, the level of protection of natural persons provided for in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same or in another third country or international organisation.

(65) 法執行機関の効率的な協力という利益は，個人データが構成国から第三国または国際組織に対して移転される場合，原則として，そのデータを最初に取得した構成国がそのデータの移転に承認を与えた後に限り，そのような移転が起きるべきである。構成国もしくは第三国の公共の保安に対する脅威または構成国の必須の利益に対する脅威の性質が，適時に事前の承認を得ることを不可能にするほどの緊急のものである場合において，そのような事前の承認なしに関連個人データを関係する第三国または国際組織に対して職務権限のある機関が移転できるべきことを要求する。構成国は，その移転に関する個別の条件が第三国または国際組織に対して通知されるべきことを定めるべきである。個人データの転送は，最初の移転を遂行した職務権限のある機関からの事前の承認に服するべきである。転送の承認の要請に関して判断する際，最初の移転を遂行した職務権限のある機関は，犯罪行為の重大性，データの最初の移転が服すべき個別の条件及びその移転の目的，刑罰の執行の性質及び条件，並びに，個人データが転送される第三国または国際組織における個人データの保護のレベルを含め，関連する全ての要素を適正に考慮に入れるべきである。最初に移転を遂行した職務権限のある機関は，その転送も個別の条件に服させ得るべきである。そのような個別の条件は，例えば，取扱いコードで表現され得る。

Where personal data are transferred from a Member State to third countries or international organisations, such a transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law-enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Member State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such a prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries or international organisations. Onward transfers of personal data should be subject to prior authorisation by the competent authority that carried out the original transfer. When deciding on a request for the authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all relevant factors, including the seriousness of the criminal offence, the specific conditions subject to which, and the purpose for which, the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or

an international organisation to which personal data are onward transferred. The competent authority that carried out the original transfer should also be able to subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

(66) 欧州委員会は，一定の第三国，第三国内の地域または 1 もしくは複数の特定の分野，または，国際組織が十分なレベルのデータ保護を提供しており，そして，そのような十分なレベルの保護を提供していると判断される第三国または国際組織に関して欧州全域における法的安定性及び統一性を提供している旨の，欧州連合全域において有効性をもつ判定をできるべきである。そのような場合，そのデータを最初に取得した別の構成国がその移転に承認を与えなければならない場合を除き，個別の承認を得る必要なく，それらの国に対する個人データの移転が起き得るべきである。

The Commission should be able to decide with effect for the entire Union that certain third countries, a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such a level of protection. In such cases, transfers of personal data to those countries should be able to take place without the need to obtain any specific authorisation, except where another Member State from which the data were obtained has to give its authorisation to the transfer.

(67) 欧州連合が基盤としている基本的な価値，とりわけ，人権の保護に沿って，欧州委員会は，第三国または第三国内の地域もしくは特定の分野の評価に際し，特定の第三国が，法の支配，法務へのアクセス，並びに，国際的な人権上の規範及び標準，そして，公共の保安，国防及び国家安全保障並びに公共の秩序及び刑事法に関する立法を含め，第三国の一般法及び特別法をいかに尊重しているかを考慮に入れるべきである。第三国内の地域または特定の分野に関する十分性の判定の採択は，特定の処理活動及びその第三国において有効な適用可能な法的基準及び立法の適用範囲のような，明確かつ客観的な基準を考慮に入れるべきである。とりわけ，個人データが 1 または複数の特定の分野において処理される場合においては，第三国は，欧州連合内において確保された保護と基本的に均等な十分なレベルの保護を確保していることの保証を提供すべきである。とりわけ，第三国は，実効的に独立のデータ保護監督を確保し，かつ，構成国のデータ保護機関との間の協力の仕組みを定めるべきであり，また，データ主体は，実効的かつ執行可能な権利及び実効的な行政上の救済及び法務上の救済を与えられるべきである。

In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security, as

well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(68) 第三国または国際組織が加入している国際的な合意とは別に，欧州委員会は，とりわけ，個人データの保護と関連する多国間制度または領域制度への第三国または国際組織の参加から生ずる義務，並びに，そのような義務の実装も考慮に入れるべきである。とりわけ，個人データの自動的な処理と関連する個人の保護に関する 1981 年 1 月 28 日の欧州評議会条約及びその追加議定書への第三国の加入が考慮に入れられるべきである。欧州委員会は，第三国または国際組織における保護のレベルを評価する際，規則(EU) 2016/679 によって設けられる欧州データ保護委員会（以下「委員会」という。）と協議すべきである。欧州委員会は，規則(EU) 2016/679 の第 45 条に従って採択された欧州委員会の関連十分性判定も考慮に入れるべきである。

Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult with the European Data Protection Board established by Regulation (EU) 2016/679 (the 'Board') when assessing the level of protection in third countries or international organisations. The Commission should also take into account any relevant Commission adequacy decision adopted in accordance with Article 45 of Regulation (EU) 2016/679.

(69) 欧州委員会は，第三国，第三国内の地域もしくは特定の分野または国際組織における保護のレベルに関する判定の稼働状態を監視すべきである。その十分性の判定の中で，欧州委員会は，その判定の稼働状況を定期的に見直す仕組みを定めるべきである。この定期的な見直しは，当の第三国または国際組織と協議して実施されるべきであり，かつ，その第三国または国際組織における全ての関連する発展を考慮に入れるべきである。

The Commission should monitor the functioning of decisions on the level of protection in a third

country, a territory or a specified sector within a third country, or an international organisation. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be undertaken in consultation with the third country or international organisation in question and should take into account all relevant developments in the third country or international organisation.

(70) 欧州委員会は，第三国，第三国内の地域もしくは特定の分野または国際組織が十分なレベルのデータ保護を確保しなくなったとも認識できるべきである。その場合の結果として，当該第三国または国際組織に対する個人データの移転は，適切な安全確保による移転及び特別の状況のための特例に関するこの指令の要件が満たされない限り，禁止されるべきである。欧州委員会とそのような第三国または国際組織との間の協議に関する手続のための条項が設けられるべきである。欧州委員会は，その状況を解消するため，適時の態様で，その第三国または国際組織に対し，その理由を通知し，かつ，協議に入るべきである。

The Commission should also be able to recognise that a third country, a territory or a specified sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently, the transfer of personal data to that third country or international organisation should be prohibited unless the requirements in this Directive relating to transfers subject to appropriate safeguards and derogations for specific situations are fulfilled. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(71) そのような十分性の判定を基礎としない移転は，個人データの保護を確保する適切な安全確保が法律上の拘束力のある文書の中で定められている場合，または，管理者がデータの移転と関連する全ての状況を評価した上で，その評価を基礎として，個人データの保護に関する適切な安全確保が存在していると判断する場合に限り，起きるべきである。そのような法律上の拘束力のある文書は，例えば，構成国によって締結され，構成国の法秩序の中に実装され，かつ，データ保護の要件の遵守を確保し，実効的な行政上の救済または法務上の救済を得る権利を含め，データ主体の権利を確保することをその構成国のデータ主体が執行し得る法律上の拘束力のある 2 国間協定であり得る。管理者は，データ移転と関連する全ての状況の評価を遂行する際，Europol または Eurojust と第三国との間で締結され，個人データの交換を許容している協力協定を考慮に入れ得るべきである。管理者は，その個人データの移転が，守秘義務に服し，かつ，その移転の目的とは別の目的のためにそのデータが処理されることがないという特定性の原則に服するということも考慮に入れるべきである。加えて，管理者は，死刑またはその他の残虐で非人道的な取扱いを要求し，宣告し，または，執行するためにその個人データが用いられることがないということも考慮に入れるべきである。これらの条件がデータの移転を許容する適切な安全確保として考慮され得るが，管理者

は，付加的な安全確保を要求し得るべきである。

Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. The controller should be able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, the controller should be able to require additional safeguards.

(72) 十分性の判定または適切な安全確保が存在しないときは，データ主体もしくは他の者の生存の利益を保護するため，または，個人データの移転元構成国の法律がそのように定めている場合において，データ主体の正当な利益を守るため；構成国もしくは第三国の公共の保安に対する差し迫った重大な脅威を防止するため；個別の案件において，公共の保安に対する脅威に抗する防護及び防止を含め，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；または，個別の案件において，訴訟の提起，攻撃もしくは防御のための必要な場合，特別の状況下に限り，移転またはある類型の移転が起き得る。これらの特例は，限定的に解釈されるべきであり，かつ，個人データの頻繁，大量かつ構造的な移転またはデータの大規模な移転を許容してはならず，厳格に必要なデータのみに限定されるべきである。そのような移転は，文書化されるべきであり，かつ，その移転の適法性を監視するために，要求に応じて，監督機関が利用できるべきである。

Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could take place only in specific situations, if necessary to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; for the prevention of an immediate and serious threat to the public security of a Member State or a third country; in an individual case for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or in an individual case for the establishment, exercise or defence of legal claims. Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary. Such transfers should be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.

(73) 構成国の職務権限のある機関は，それらの機関に法律上与えられた職務を遂行できるようにするための関連情報の交換に関し，刑事における法務上の協力及び警察の協力の分野において第三国との間で締結され，発効している 2 国間もしくは多国間の国際協定を適用する。原則として，これは，この指令の目的のために関係第三国内の職務権限のある機関の協力を介して，または，少なくとも，その機関との間で起き，時として，2 国間もしくは多国間の国際協定が存在しない場合にも起きる。ただし，個々の案件において，とりわけ，その移転が適時に遂行され得ないという理由により，または，第三国の機関が法の支配または国際的な人権の規範及び基準を尊重しないという理由により，その第三国内のそのような機関との連絡を定期的に求める手続が非実効的または不適切なときは，当該構成国の職務権限のある機関は，当該第三国に拠点のある取得者に対して直接に個人データを移転することを決定し得る。このことは，犯罪行為の被害者となる危険に晒されている者の生命を守るため，または，テロリズムを含め，犯罪の目前の準備を阻止する利益において，個人データを移転する差し迫った必要性がある場合がそれに該当し得る。職務権限のある機関と第三国内に拠点のある取得者との間のそのような移転が特定の個々の案件において起きるべきものではあるが，この指令は，そのような場合を規律するための条件を定めるべきである。それらの条項は，刑事における法務上の協力及び警察の協力の分野における 2 国間もしくは多国間の国際協定からの逸脱と判断されてはならない。それらの規定は，この指令の他の規定に加えて，とりわけ，処理の適法性及び第 5 章に関するものに適用されるべきである。

Competent authorities of Member States apply bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial cooperation in criminal matters and police cooperation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through, or at least with, the cooperation of the authorities competent in the third countries concerned for the purposes of this Directive, sometimes even in the absence of a bilateral or multilateral international agreement. However, in specific individual cases, the regular procedures requiring contacting such an authority in the third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, so that competent authorities of Member States could decide to transfer personal data directly to recipients established in those third countries. This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of

a crime, including terrorism. Even if such a transfer between competent authorities and recipients established in third countries should take place only in specific individual cases, this Directive should provide for conditions to regulate such cases. Those provisions should not be considered to be derogations from any existing bilateral or multilateral international agreements in the field of judicial cooperation in criminal matters and police cooperation. Those rules should apply in addition to the other rules of this Directive, in particular those on the lawfulness of processing and Chapter V.

(74) 個人データが国境を越えて移動する場合，それらの個人データの違法な利用または開示からデータ主体自身を保護するためのデータ保護の権利を行使する自然人の能力に対するリスクを増加させることとなり得る。それと同時に，監督機関は，その国境外の活動と関連して異議を唱え，または，その調査を実行できないと判断するかもしれない。国境を越える文脈における監督機関の作業を共同にする努力は，不十分な防止権限もしくは是正権限及び一貫性のない法制度によっても阻害され得る。それゆえ，監督機関の国外における相手方との間の情報交換について監督機関を支援するための，データ保護監督機関間の緊密な協力を促進する必要がある。

Where personal data move across borders it may put at increased risk the ability of natural persons to exercise data protection rights to protect themselves from the unlawful use or disclosure of those data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers and inconsistent legal regimes. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information with their foreign counterparts.

(75) 完全に独立してその権限を行使する監督機関を構成国内に設けることは，自然人の個人データの処理と関連する自然人の保護の必須の構成要素の 1 つである。監督機関は，自然人の個人データの処理と関連して自然人を保護するため，この指令によって採択された条項の適用を監視すべきであり，かつ，欧州連合全域におけるそれらの条項の一貫性のある適用に貢献すべきである。その目的のために，監督機関は，相互に及び欧州委員会との間で協力すべきである。

The establishment in Member States of supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and should contribute to their consistent application throughout the Union in order to protect natural persons with regard to the processing of their personal data. To that end, the supervisory authorities should cooperate with each other and with the Commission.

(76) 構成国は，規則(EU) 2016/679 に基づいて既に設置されている監督機関に対し，この指令に基づいて設けられるべき国内監督機関によって遂行される職務に関する職責を委任できる。

Member States may entrust a supervisory authority already established under Regulation (EU) 2016/679 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(77) 構成国は，その構成国の憲法上，国家組織上及び行政上の構造を反映させるため，複数の監督機関を設けることが認められるべきである。各監督機関は，欧州連合全域における相互補助及び他の監督機関との間の協力と関連する職務に関するものを含め，その監督機関の職務の実効的な遂行のために必要となる資金及び人的資源，施設及びインフラを提供されるべきである。各監督機関は，区分された公式の年次予算をもつべきである。それは，国全体の予算または国内予算の一部とすることができる。

Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with the financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(78) 監督機関は，そのような資金監督が監督機関の独立性に影響を与えないことを条件として，その資金の支出に関して独立の監督または監視の仕組みに服するべきである。

Supervisory authorities should be subject to independent control or monitoring mechanisms regarding their financial expenditure, provided that such financial control does not affect their independence.

(79) 監督機関の構成員に関する一般的な条件は，構成国法によって定められるべきであり，また，とりわけ，透明性のある手段により，政府もしくは政府の構成員，議会もしくはその議会の議院からの任命提案，または，構成国法によって信任された独立の組織からの任命提案を基礎として，その構成国の議会もしくは政府または州の首長のいずれかによって，その構成国の監督機関の構成員が任命されることを定めるべきである。監督機関の独立性を確保するため，その構成員は，誠実に行動すべきであり，また，その責務と適合しないいかなる行動も控えるべきであり，かつ，その在任中は，報酬の有無を問わず，その職務と適合しない仕事に従事してはならない。監督機関の独立性を確保するため，監督機関によってその職員が選任されるべきである。その職員は，構成国法によって信任された独立の組織の介入を含め得る。

The general conditions for the member or members of the supervisory authority should be laid down by Member State law and should in particular provide that those members should be either appointed by the parliament or the government or the head of State of the Member State based on a proposal from the government or a member of the government, or the parliament or its chamber, or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, should refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. In order to ensure the independence of the supervisory authority, the staff should be chosen by the supervisory authority which may include an intervention by an independent body entrusted by Member State law.

(80) この指令は，国内裁判所及びそれ以外の法務機関の活動に対しても適用されるが，裁判官の法務上の職務の遂行における裁判官の独立を防護するため，裁判所がその法務上の権能において活動する場合における個人データの処理に対しては，監督機関の職務権限を適用してはならない。この例外は，訴訟事件における法務上の活動に限定されるべきであり，それ以外の，裁判官が構成国法に従って関与し得る活動に対しては適用されない。構成国は，例えば，検察庁のような，裁判所以外の独立の法務機関がその法務上の権能において行動する際の個人データの処理に対して監督機関の職務権限が適用されないことも定めるべきである。いかなる場合においても，裁判所及びそれ以外の独立の法務機関によるこの指令の規定の遵守は，常に，憲章の第 8 条第 3 項に従い，独立の監督に服する。

While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data where courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. That exemption should be limited to judicial activities in court cases and not apply to other activities where judges might be involved in accordance with Member State law. Member States should also be able to provide that the competence of the supervisory authority does not cover the processing of personal data of other independent judicial authorities when acting in their judicial capacity, for example public prosecutor's office. In any event, the compliance with the rules of this Directive by the courts and other independent judicial authorities is always subject to independent supervision in accordance with Article 8(3) of the Charter.

(81) 各監督機関は，データ主体から申立てられた異議を取扱うべきであり，かつ，その事項を調査し，または，職務権限のある監督機関に対してその異議を移送すべきである。異議申立て後の調査は，法務上の見直しに服して，個別の案件において適切な範囲内で遂行されるべきである。その監督機関は，そのデータ主体に対し，合理的な期間内に，その異議申立の進捗状況及び結果を通知すべきである。更に調査を要する場合または他の監督機関との協力を要する場合，そのデータ主体に対し，中間的な情報が提供されるべきである。

Each supervisory authority should handle complaints lodged by any data subject and should investigate the matter or transmit it to the competent supervisory authority. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject.

(82) 司法裁判所によって解釈される TFEU により，欧州連合全域においてこの指令の遵守及び執行の実効的であり，信頼性があり，かつ，一貫性のある監視を確保するため，監督機関は，各構成国内において，その監督機関の職務を遂行するために必要となる措置を構成する調査，是正及び助言の権限を含め，同一の職務及び実効的な権限をもつべきである。ただし，監督機関の権限は，犯罪行為の捜査及び訴追を含め，刑事手続に関する特別の規定または法務当局の独立に対して干渉してはならない。構成国法に基づく検察当局の権限を妨げることなく，監督機関は，法務当局に対してこの指令の違反行為に注意を向けさせ，法律上の手続に従事させる権限をもつべきである。監督機関の権限は，欧州連合法及び構成国法に定める適切な手続上の安全確保に従って，公平，公正かつ合理的な期間内に行使されるべきである。とりわけ，個々の措置は，個々の案件の状況を考慮に入れ，関係する者に対して不利益な影響を与える個々の措置が講じられる前に全ての者が聴聞の機会をもつ権利を尊重し，かつ，関係する者に対する過剰な費用負担と過度の不便を避けることを考慮に入れた上で，この指令の遵守を確保するという観点から，適切であり，必要であり，かつ，比例的なものとすべきである。施設へのアクセスと関連する調査権限は，法務機関の事前許可の要求のような，構成国法中の個別の要件に従って行使されるべきである。法律上の拘束力のある決定の採択は，その決定を採択した監督機関の構成国において，法務上の見直しに服するべきである。

In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the TFEU as interpreted by the Court of Justice, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective, and advisory powers which constitute necessary means to perform their tasks. However, their powers should not interfere with specific rules for criminal proceedings, including investigation and prosecution of criminal offences, or the independence of the judiciary. Without prejudice to the powers of prosecutorial authorities under Member State law, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities or to engage in legal proceedings. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards laid down by Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Directive, taking into account the circumstances of each individual case, respect the right of

every person to be heard before any individual measure that would adversely affect the person concerned is taken, and avoiding superfluous costs and excessive inconvenience to the person concerned. Investigative powers as regards access to premises should be exercised in accordance with specific requirements in Member State law, such as the requirement to obtain a prior judicial authorisation. The adoption of a legally binding decision should be subject to judicial review in the Member State of the supervisory authority that adopted the decision.

(83) 監督機関は，この指令によって採択された条項の一貫性のある適用及び執行を確保するために，その職務の遂行において，相互に援助し，かつ，相互補助を提供すべきである。

The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(84) 委員会は，欧州委員会に対して助言をすること及び欧州連合全域にわたる監督機関の協力を容易にすることを含め，欧州連合全域にわたるこの指令の一貫性のある適用に貢献すべきである。

The Board should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the cooperation of the supervisory authorities throughout the Union.

(85) 全てのデータ主体は，この指令によって採択された条項に基づく彼もしく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，または，監督機関が，異議に対して何もせず，その異議の一部または全部を却下もしくは棄却する場合，または，データ主体の権利を保護するためにそのような行為が必要となる場合において何らの活動もしない場合，単一の監督機関に異議を申立てる権利及び憲章の第 47 条に従って実効的な法務上の救済の権利をもつべきである。異議申立て後の調査は，法務上の見直しに服して，個別の案件において適切な範囲内で行われるべきである。職務権限のある監督機関は，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すべきである。更に調査を要する場合または他の監督機関との協力を要する場合，そのデータ主体に対し，中間的な情報が提供されるべきである。異議申立書の提出を容易にするため，各監督機関は，他の通信手段を排除することなく，電子的にも完了され得る異議申立書の提出を提供することのような措置を講じるべきである。

Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses

a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The competent supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(86) 個々の自然人または法人は，当該の者と関係して法律上の効果を発生させる監督機関の決定を不服として，職務権限のある国内裁判所において，実効的な法務上の救済の権利をもつべきである。そのような決定は，とりわけ，監督機関による調査の権限，是正の権限及び承認の権限の行使，または，異議の却下または棄却と関係する。ただし，その権利は，監督機関が発する意見や監督機関が提供する助言のような法律上の拘束力をもたない監督機関の上記以外の措置を包含しない。監督機関を相手方とする訴訟手続は，その監督機関が設けられている構成国の裁判所において提起されるべきであり，かつ，構成国法に従って実施されるべきである。それらの裁判所は，その裁判所に提起される紛争と関連する事実上及び法律上の全ての争点を吟味するための裁判管轄権を含む完全な裁判管轄権を行使すべきである。

Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, that right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

(87) この指令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，データ主体の個人データの保護と関連するデータ主体の権利及び利益を保護することを狙いとし，かつ，構成国法に従って構成されている組織に対し，彼または彼女の代わりに監督機関に対する異議を申立てること，及び，法務上の救済の権利を行使することを委任する権利をもつべきである。このデータ主体の代理者の権利は，裁判所において，理事会決定 77/249/EEC[10]に定義する弁護士によるデータ主体の代理強制を要求できる構成

[10] 役務提供の自由の弁護士による実効的な行使の促進のための 1977 年 3 月 22 日の理事会決定

国の手続法を妨げてはならない。

Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a body which aims to protect the rights and interests of data subjects in relation to the protection of their personal data and is constituted according to Member State law to lodge a complaint on his or her behalf with a supervisory authority and to exercise the right to a judicial remedy. The right of representation of data subjects should be without prejudice to Member State procedural law which may require mandatory representation of data subjects by a lawyer, as defined in Council Directive 77/249/EEC [(10)], before national courts.

(88) この指令により採択された条項に違反する処理の結果として被害を受け得る者の損害は，構成国法に基づき，管理者またはそれ以外の職務権限のある機関からその賠償を受けるべきである。損害の概念は，この指令の目的を完全に反映する態様で，司法裁判所の判例法に照らし，広く解釈されるべきである。このことは，欧州連合法または構成国法中の他の規定の違反から生ずる損害の賠償請求を妨げない。違法な処理またはこの指令によって採択された条項に違反する処理への参照が行われるときは，その参照は，この指令によって採択された実装行為に違反する処理も包摂する。データ主体は，そのデータ主体が被った損害に関し，完全かつ実効的な賠償を受けるべきである。

Any damage which a person may suffer as a result of processing that infringes the provisions adopted pursuant to this Directive should be compensated by the controller or any other authority competent under Member State law. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Directive. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. When reference is made to processing that is unlawful or that infringes the provisions adopted pursuant to this Directive it also covers processing that infringes implementing acts adopted pursuant to this Directive. Data subjects should receive full and effective compensation for the damage that they have suffered.

(89) 公法または私法のいずれによって規律されるかを問わず，この指令に違反する自然人または法人に対しては，制裁が科されるべきである。構成国は，その制裁が実効的であり，比例的であり，かつ，抑止力をもつことを確保すべきであり，かつ，制裁を実装するための全ての措置を講ずるべきである。

Penalties should be imposed on any natural or legal person, whether governed by private or public law, who infringes this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and should take all measures to implement the penalties.

77/249/EEC（OJ L 78, 26.3.1977, p.17）.

(90) この指令の実装のための統一的な条件を確保するため，第三国，第三国内の地域もしくは特定の分野または国際組織によって与えられる十分なレベルの保護並びに監督機関の間及び監督機関と委員会との間の相互援助及び電子的な手段による情報交換のための手立ての書式と手続に関し，その実装権限は，欧州委員会に対して与えられるべきである。それらの権限は，欧州議会及び理事会の規則(EU) No 182/2011[11]に従って行使されるべきである。

In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission with regard to the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (11).

(91) それらの実装行為が一般的な適用範囲をもつ行為であることに鑑み，第三国，第三国内の地域もしくは特定の分野または国際組織によって与えられる十分なレベルの保護，監督機関の間及び監督機関と委員会の間の相互援助及び電子的な手段による情報交換のための手立ての書式と手続に関する実装行為の採択のために，審議手続が用いられるべきである。

The examination procedure should be used for the adoption of implementing acts on the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and on the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, given that those acts are of a general scope.

(92) 十分なレベルでの保護を確保しなくなった第三国，第三国内の地域もしくは特定の分野または国際組織と関連する適正に正当化される案件において，緊急性という優先的な根拠がそのように要求ときは，欧州委員会は，直ちに，適用可能な実装行為を採択すべきである。

The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country, a territory or a specified sector within a third country, or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

(93) この指令の目的，すなわち，自然人の基本的な権利及び自由，とりわけ，自然人の個人データの保護の権利を保護すること，並びに，欧州連合内における職務権限のある機関による

11 欧州委員会の実装権限の行使の構成国による管理のための仕組みに関する規定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 No 182/2011 (OJ L 55, 28.2.2011, p. 13).

個人データの支障のない交換を確保することは，構成国によっては十分に達成され得ず，その活動の規模及び影響のゆえに，欧州連合によって，より良く達成され得るので，欧州連合は，TEU の第 5 条に定める補完性の原則に従い，措置を採択できる。同条に定める比例性の原則に従い，この指令は，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。

Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the TEU. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives

(94) 例えば，理事会決定 2008/615/JHA[12]によって適用される個人データの保護に関する特別の条項または欧州連合の構成国間の刑事における相互補助に関する条約[13]の第 23 条のような，刑事における法務上の協力及び警察の協力の分野において採択された欧州連合の法行為の特別の条項であって，この指令の採択の日よりも前に採択され，構成国間の個人データの処理及び諸条約によって設けられた情報システムへの構成国の指定された機関のアクセスを規律するものは，影響を受けないままとすべきである。憲章の第 8 条及び TEFU の第16条は，個人データの保護のための基本的な権利が，欧州全域にわたり一貫性のある態様で確保されることを要求しているので，欧州委員会は，それらの特別の条項を揃える必要性の有無を評価するため，この指令の採択の日よりも前に採択され，構成国間の個人データの処理及び諸条約によって設けられた情報システムへの構成国の指定された機関のアクセスを規律する法行為とこの指令との間の関係に関する状況を評価すべきである。それが適切なときは，欧州委員会は，個人データの処理と関連する一貫性のある法規範を確保するという観点から，提案を行うべきである。

Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, such as, for example, the specific provisions concerning the protection of personal data applied pursuant to Council Decision 2008/615/JHA [(12)], or Article 23 of the

12 特にテロリズム及び国境を越える犯罪との闘いにおける国境を越える協力の増進に関する 2008 年 6 月 23 日の理事会決定 2008/615/JHA（OJ L 210, 6.8.2008, p.1）.

13 欧州連合の構成国間の刑事における共助に関する欧州連合条約の第 34 条に従って設けられる 2000 年 5 月 29 日の理事会の行為（OJ C 197, 12.7.2000, p.1）.

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union [13]. Since Article 8 of the Charter and Article 16 TFEU require that the fundamental right to the protection of personal data be ensured in a consistent manner throughout the Union, the Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of those specific provisions with this Directive. Where appropriate, the Commission should make proposals with a view to ensuring consistent legal rules relating to the processing of personal data.

(95) 欧州連合内における個人データの包括的かつ一貫性のある保護を確保するため，この指令の発効の日よりも前に構成国によって締結され，かつ，その発効日よりも前に適用可能な関連する欧州連合法を遵守する国際協定は，改正，置き換えまたは廃止までの間は，有効なままとすべきである。

In order to ensure a comprehensive and consistent protection of personal data in the Union, international agreements which were concluded by Member States prior to the date of entry into force of this Directive and which comply with the relevant Union law applicable prior to that date should remain in force until amended, replaced or revoked.

(96) 構成国は，この指令を国内法に移植するため，この指令の発効の日から 2 年を超えない期間が認められるべきである。当該発効日に既に実行中の処理は，この指令の発効後 2 年以内に，この指令に適合するようにされるべきである。ただし，そのような処理がこの指令の発効日よりも前に適用可能な欧州連合法を遵守するときは，監督機関の事前協議に関するこの指令の要件は，その本質上，処理の前にそれらの要件に適合すべきであることに鑑み，その発効日に既に実行中の処理業務に対して適用してはならない。当該発効日よりも前に設置された自動化された処理システムに関する履歴記録義務に適合するため，この指令の発効日の後 7 年間で満了となる期間よりも長期の実装期間を構成国が用いる場合，管理者または処理者は，データ処理の適法性を説明するため，自己監視のため，及び，履歴またはそれ以外の方式による記録のような，データの完全性とデータの安全性を確保するため，実効的な手法を設けるべきである。

Member States should be allowed a period of not more than two years from the date of entry into force of this Directive to transpose it. Processing already under way on that date should be brought into conformity with this Directive within the period of two years after which this Directive enters into force. However, where such processing complies with the Union law applicable prior to the date of entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way on that date given that those requirements, by their very nature, are to be met prior to the

processing. Where Member States use the longer implementation period expiring seven years after the date of entry into force of this Directive for meeting the logging obligations for automated processing systems set up prior to that date, the controller or the processor should have in place effective methods for demonstrating the lawfulness of the data processing, for enabling self-monitoring and for ensuring data integrity and data security, such as logs or other forms of records.

(97) この指令は，欧州議会及び理事会の指令 2011/93/EU[14]に定める児童の性的虐待及び性的搾取並びに児童ポルノとの闘いに関する法令を妨げない。

This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council [(14)].

(98) それゆえ，枠組み決定 2008/977/JHA は，廃止されるべきである。

Framework Decision 2008/977/JHA should therefore be repealed.

(99) TEU 及び TFEU に附属する自由，保安及び法務の領域と関連する連合王国及びアイルランドの地位に関する議定書第 21 号の第 6 条 a に従い，英国及びアイルランドは，TFEU の第 16 条を基礎として定められる条項の遵守を要求する刑事における法務上の協力及び警察の協力を形成することを規律する規定によって英国及びアイルランドが拘束されない場合において，TFEU の第 3 部の第 V 款第 4 章または第 5 章の適用範囲内にある活動を遂行する際，構成国による個人データの処理と関連するこの指令中に定める条項によって拘束されない。

In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, the United Kingdom and Ireland are not bound by the rules laid down in this Directive which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU.

(100)TEU 及び TFEU に附属するデンマークの地位に関する議定書第 22 号の第 2 条及び第 2 条 a に従い，デンマークは，この指令に定める条項によって拘束されず，または，TFEU の

[14] 児童の性的虐待及び性的搾取並びに児童ポルノとの闘い，並びに，枠組み決定 2004/68/JHA の改正に関する欧州議会及び理事会の 2011 年 12 月 13 日の指令 2011/93/EU (OJ L 335, 17.12.2011, p.1)

第 3 部の第 V 款第 4 章または第 5 章の適用範囲内にある活動を遂行する際，構成国による個人データ処理と関連するこの指令に定める条項の適用に服さない。この指令がシェンゲン協定を基礎とすることに鑑み，デンマークは，TFEU の第 3 部第 V 款に基づき，同議定書の第 4 条に従って，この指令の採択後 6 か月以内に，同指令を国内法の中に実装するか否かを決定すべきである。

In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, as annexed to the TEU and to the TFEU, Denmark is not bound by the rules laid down in this Directive or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. Given that this Directive builds upon the Schengen *acquis*, under Title V of Part Three of the TFEU, Denmark, in accordance with Article 4 of that Protocol, is to decide within six months after adoption of this Directive whether it will implement it in its national law.

(101)アイスランド及びノルウェーに関しては，この指令は，シェンゲン協定の実装，適用及び発展へのそれら 2 国の参加に関する欧州連合の理事会とアイスランド共和国及びノルウェー王国との間で締結された協定[15]に定めるシェンゲン協定の条項の発展を構成する。

As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen *acquis*, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (15).

(102)スイスに関しては，この指令は，シェンゲン協定の実装，適用及び発展へのスイス連邦の参加に関する欧州連合，欧州共同体及びスイス連邦の間の協定[16]に定めるシェンゲン協定の条項の発展を構成する。

As regards Switzerland, this Directive constitutes a development of provisions of the Schengen *acquis*, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis* (16).

(103)リヒテンシュタインに関しては，この指令は，シェンゲン協定の実装，適用及び発展へのスイス連邦の参加に関する欧州連合，欧州共同体及びスイス連邦の間の協定へのリヒテンシュタイン公国の加入に関する欧州連合，欧州共同体，スイス連邦及びリヒテンシュタイン公国の

15 OJ L 176, 10.7.1999, p.36
16 OJ L 53, 27.2.2008, p.52.

間の議定書[17]に定めるシェンゲン協定の条項の発展を構成する。

As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (17).

(104)この指令は，TFEU に掲げられている憲章の中で認められた基本的な権利，とりわけ，私生活及び家庭生活の尊重の権利，個人データの保護の権利，実効的な法務上の救済の権利及び公正な法廷の権利を尊重し，かつ，そこで認められている基本原則を尊重する。それらの権利に対する制限は，欧州連合によって認められる一般的な利益の目的にそれらの制限が適合する必要性があり，または，他の者の権利及び自由を保護するために必要であることを要するので，憲章の第 52 条第 1 項に従っている。

This Directive respects the fundamental rights and observes the principles recognised in the Charter as enshrined in the TFEU, in particular the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on those rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(105)説明文書に関する構成国及び欧州委員会の 2011 年 9 月 28 日の共同政治宣言に従い，構成国は，正当化される場合において，指令の内容とそれに対応する国内移植措置の部分との間の関係を説明する 1 もしくは複数の文書を，その構成国の移植措置の通知に添付させるべきである。この指令に関し，立法者は，そのような文書の送付が正当なものであると判断する。

In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition measures. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(106)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，2012

[17] OJ L 160, 18.6.2011, p. 21.

年 3 月 7 日にその意見書[18]を提出した。

The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 (18).

(107)この指令は，個人データの情報提供，アクセス，訂正または削除に関するデータ主体の権利の行使，刑事手続の過程における処理の制限及びそれらの権利の制限を設け得ることを，刑事手続に関する国内規定の中で構成国が実装することを妨げてはならない，

This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access to and rectification or erasure of personal data and restriction of processing in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure,

以上のとおりであるので，この指令を採択する：

HAVE ADOPTED THIS DIRECTIVE:

[18] OJ C 192, 30.6.2012, p.7.

第 I 章 総則的な規定
Chapter I General provisions

第 1 条 対象事項及び目的
Article 1 Subject-matter and objectives

1. この指令は，公共の保安に対する脅威に抗する防護及び防止を含め，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の職務権限のあ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に関する規定を定める。

This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

2. この指令に従い，構成国は:
   (a) 自然人の基本的な権利及び自由，並びに，とりわけ，自然人の個人データの保護の権利を保護し;かつ，
   (b) そのような交換が欧州連合法または構成国法によって要求される場合，欧州連合内における職務権限のある機関による個人データの交換が，個人データの処理と関連する自然人の保護と関係する理由によって制限されることがなく，かつ，禁止されることもないことを確保する。

In accordance with this Directive, Member States shall:
   (a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and
   (b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

3. この指令は，構成国が，職務権限のある機関による個人データの処理と関連するデータ主体の権利及び自由の保護に関し，この指令の中で定められる安全確保よりも高度な安全確保を定めることを妨げてはならない。

This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

第 2 条 適用範囲
Article 2 Scope

1. この指令は，第 1 条第 1 項に定める目的のための職務権限のある機関による個人データの処理に適用される。

   This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).

2. この指令は，その全部または一部が自動化された手段による個人データの処理，及び，自動化された手段以外の手段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ことが予定されているものに対して適用される。

   This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

3. この指令は，以下の個人データの処理に対しては適用されない：
   (a) 欧州連合法の適用範囲外にある活動の過程における処理;
   (b) 欧州連合の機関，組織，事務局及び部局による処理。

   This Directive does not apply to the processing of personal data:
   (a) in the course of an activity which falls outside the scope of Union law;
   (b) by the Union institutions, bodies, offices and agencies.

第 3 条 定義
Article 3 Definitions

この指令の目的のために：

(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」）と関連する全ての情報のことを意味し;識別可能な自然人とは，とりわけ，姓名，識別番号，位置データ，オンライン識別子のような識別子の参照によって，または，当該自然人の身体的，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に固有な 1 もしくは複数の要素を参照することによって，直接または間接に，識別され得る者のことであり;

(2) 「処理」とは，それが自動化された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，照会，使用，移転による開示，伝達またはそれ外に利用できるようにすること，整列もしくは結合，制限，削除または破壊のような，個人デ

ータもしくは個人データのセットに対して実施される全ての業務または業務のセットのことを意味し；

(3) 「処理の制限」とは，将来におけるその個人データの処理を限定することを狙いとして，記録保存された個人データに目印を付すことを意味し；

(4) 「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に，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，位置及び移動に関する側面を分析または予測するために，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化された処理のことを意味し；

(5) 「仮名化」とは，そのような付加的な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帰属しないことを確保するための技術上及び組織上の措置に服することを条件として，付加的な情報の利用なしにはその個人情報が特定のデータ主体に帰属し得なくなるような態様による個人データの処理のことを意味し；

(6) 「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の集中型，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できるもののことを意味し；

(7) 「職務権限のある機関」とは，以下の者のことを意味し：

(a) 公共の保安に対する脅威に抗する防護及び防止を含め，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に関する職務権限のある行政機関；または

(b) 構成国法により，公共の保安に対する脅威に抗する防護及び防止を含め，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の公的権限及び公権力の行使の委任を受けた上記以外の組織または法主体；

(8) 「管理者」とは，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手段を決定する職務権限のある機関のことを意味し；そのような処理の目的及び方法が欧州連合または構成国法によって決定される場合，管理者または管理者を指定するための個別の基準は，欧州連合または構成国法によって定められる得るものであり；

(9) 「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，部局またはそれら以外の組織のことを意味し；

(10) 「取得者」とは，第三者であるか否かを問わず，個人データを開示される自然人もしくは法人，行政機関，部局またはそれら以外の組織のことを意味する。ただし，構成国法に従って特別の照会の枠組み内で個人データを取得し得る行政機関は，取得者とはみなされず；行政機関によるそのようなデータの処理は，その処理の目的に従って適用可能なデータ保護規定を遵守すべきであり；

(11) 「個人データの侵害」とは，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を導くような，送付され，記録保存され，または，それら以外の処理がなされる個人データの安全性の侵害のことを意味し；

(12) 「遺伝子データ」とは，自然人の，受け継がれまたは獲得された遺伝的特性に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唯一無二な情報を与え，

かつ，とりわけ，当の自然人から得られた生化学資料の分析結果に由来するもののことを意味し；

(13) 「生体要素データ」とは，顔画像または指紋データのような，自然人の身体的，生理的または行動的な特徴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，当該自然人の唯一無二な識別同定をできるようにし，または，それを確認するもののことを意味し；

(14) 「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；

(15) 「監督機関」とは，第 41 条により構成国によって設けられる独立の行政機関のことを意味し；

(16) 「国際組織」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，2 以上の国家間の合意によって，もしくは，その合意を基礎として，設置されるもののことを意味する。

For the purposes of this Directive:

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

(4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) ‘competent authority’ means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(8) ‘controller’ means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(9) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(10) ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(11) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(12) ‘genetic data’ means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(13) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(14) ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(15) ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 41;

(16) ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

第Ⅱ章 基本原則
Chapter II Principles

第 4 条 個人データの処理と関連する基本原則
Article 4 Principles relating to processing of personal data

1. 構成国は，個人データが以下のとおりであることを定める:
   (a) 適法かつ公正に処理されること;
   (b) 特定の，明示かつ正当な目的のために収集され，かつ，その目的に適合しない態様で処理されないこと;
   (c) その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;
   (d) 正確であり，かつ，それが必要なときは，最新の状態に保たれること;そのデータが処理される目的を考慮した上で，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手立てが講じられなければならない;
   (e) そのデータが処理される目的のために必要な期間内に限り，データ主体の識別同定を許容する方式を保つこと;
   (f) 無権限もしくは違法な処理に抗して，並びに，事故による喪失，破壊または毀損に抗して，適切な技術上または組織上の措置を用いる防護を含め，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こと。

   Member States shall provide for personal data to be:
   (a) processed lawfully and fairly;
   (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
   (c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
   (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. その個人データが収集される目的以外の第 1 条第 1 項に定める目的のいずれかのための同一の管理者または別の管理者による処理は，以下の場合に限り，許容される：
   (a) その管理者が，欧州連合法または構成国法に従い，そのような目的のためにそのような個人データを処理することが認められており；かつ，
   (b) 処理が，欧州連合法または構成国法に従い，当該別の目的のために必要かつ適切である場合。

   Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:
   (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and
   (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

3. 同一の管理者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確保に服し，第 1 条第 1 項に定める目的のために，公共の利益におけるアーカイブ，科学，統計または歴史の利用を含め得る。

   Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.

4. 管理者は，第 1 項，第 2 項及び第 3 項の遵守に関する職責を負い，かつ，その遵守を説明できるものとする。

   The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

第 5 条 記録保存及び見直しの期限

Article 5 Time-limits for storage and review

構成国は，個人データの削除のために設けられ，及び，個人データの記録保存の必要性の定期的な見直しのために設けられる適切な期限を定める。手続上の措置は，それらの期限が尊重されることを確保する。

Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

第 6 条 異なる類型のデータ主体間の区分

Article 6 Distinction between different categories of data subject

構成国は，それが適用可能なときは，かつ，可能な限り，管理者が，以下のような異なる類型のデータ主体の個人データの間に明確な区分を設けることを定める：

(a) 当該の者が犯罪行為を実行したこと，または，犯罪行為の実行に関与したことを疑うための重大な根拠が存在する者；
(b) 犯罪行為により有罪判決を受けた者；
(c) 犯罪行為の被害者，または，その者と関連する一定の事実が，彼もしくは彼女が犯罪行為の被害者であり得ると信ずる根拠を生じさせている者；及び，
(d) 犯罪行為と関係する捜査またはその後の刑事手続において供述をするために呼び出され得る者，犯罪行為に関する情報を提供し得る者，または，(a)及び(b)に示す者の中のいずれかと連絡のある者もしくは関係をもつ者のような，犯罪行為の上記以外の関係者。

Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

第 7 条 個人データ間の区別及び個人データの品質の検査

Article 7 Distinction between personal data and verification of quality of personal data

1. 構成国は，可能な限り，事実を基礎とする個人データと個人の評価を基礎とする個人データとが区別されることを定める。

Member States shall provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments.

2. 構成国は，職務権限のある機関が，不正確な個人データ，不完全な個人データ，または，最新のものではない個人データが送付され，もしくは，これを利用できるようにされることのないことを確保するための全ての合理的な手立てを講ずることを定める。その目的のために，

各職務権限のある機関は，可能な限り，そのデータが送付され，または，利用できるようにされる前に，個人データの品質を検査する。可能な限り，個人データの全ての送付において，個人データの正確性，完全性及び信頼性の程度を送付先である職務権限のある機関が評価できるようにするために必要となる情報，並びに，それらのデータがアップデートされる範囲が付加される。

Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.

3. 不正確な個人データが送付され，または，個人データが違法に送付される事態が生じた場合，その取得者は，遅滞なく，その通知を受ける。そのような場合，その個人データは，訂正もしくは削除され，または，処理は，第 16 条に従って制限される。

If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16.

第 8 条 処理の適法性

Article 8 Lawfulness of processing

1. 構成国は，第 1 条第 1 項に定める目的のために職務権限のある監督機関によって遂行される職務の遂行のために処理が必要であり，かつ，その処理が欧州連合法または構成国法に基礎とする場合に限り，かつ，その範囲内に限り，処理が適法となることを定める。

Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.

2. この指令の適法範囲内にある処理を規律する構成国法は，少なくとも，処理の対象，処理される個人データ及び処理の目的の細目を定める。

Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

第 9 条 特別の処理の条件

Article 9 Specific processing conditions

1. 第 1 条第 1 項に定める目的のために職務権限のある機関によって収集された個人データは，欧州連合法または構成国法によって認められる処理ではない限り，第 1 条第 1 項に定める目的以外の目的のために処理してはならない。そのような別の目的のために個人データが処理される場合，欧州連合法の適用範囲外の活動においてその処理が遂行されるのではない限り，規則(EU) 2016/679 が適用される。

   Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.

2. 職務権限のある機関が，第 1 条第 1 項に定める目的のために遂行される職務以外の職務の遂行を構成国法によって委任されている場合，欧州連合法の適用範囲外の活動において処理が実施されるのではない限り，公共の利益におけるアーカイブの目的，科学もしくは歴史の調査の目的，または，統計の目的を含め，そのような目的のための処理に対し，規則(EU) 2016/679 が適用される。

   Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law.

3. 送付元である職務権限のある機関に対して適用可能な欧州連合法または構成国法が，処理のための個別の条件を定めている場合，構成国は，その送付元である職務権限のある機関が，そのような個人データの取得者に対して，それらの条件及びそれらの条件を遵守する必要性を連絡することを定める。

   Member States shall, where Union or Member State law applicable to the transmitting competent authority provides specific conditions for processing, provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and the requirement to comply with them.

4. 構成国は，他の構成国の取得者，または，TFEU の第 V 款第 4 章及び第 5 章によって設けられた部局，事務局もしくは組織である取得者に対し，送付元である職務権限のある機関の

構成国内において同様のデータ送付に適用可能な条件以外には，送付元である職務権限のある機関が第 3 項による条件を適用しないことを定める。

Member States shall provide for the transmitting competent authority not to apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.

第 10 条 特別の類型の個人データの処理

Article 10 Processing of special categories of personal data

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，労働組合の加入を明らかにする個人データの処理，及び，自然人の唯一無二な識別の目的のための遺伝子データ，生体要素データの処理，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，限界に必要性な場合に限り，そのデータ主体の権利及び自由のための適切な安全確保に服し，以下の場合に限り，認められる：

(a) 欧州連合法または構成国法によって認められている場合において；
(b) データ主体または他の自然人の生存の利益を守るため；または
(c) そのような処理が，データ主体によって公開されたことが明白なデータと関連する場合。

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State law;
(b) to protect the vital interests of the data subject or of another natural person; or
(c) where such processing relates to data which are manifestly made public by the data subject.

第 11 条 自動化された個人の判定

Article 11 Automated individual decision-making

1. 構成国は，その管理者が服する欧州連合法または構成国法によって認められており，かつ，それらの法律がデータ主体の権利及び自由のための安全確保，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，データ主体に関して不利な法律上の効果を発生させ，または，彼もしくは彼女に対して大きな影響を与える，自動化された処理のみを基礎とする判定を禁止することを定める。

Member States shall provide for a decision based solely on automated processing, including

profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. 本条第 1 項に示す判定は，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ない限り，第 10 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。

Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3. 第 10 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して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。

Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

第Ⅲ章　データ主体の権利

Chapter III Rights of the data subject

第 12 条　データ主体の権利の行使のための情報提供及び方式

Article 12 Communication and modalities for exercising the rights of the data subject

1. 構成国は，管理者が，第 13 条に示す情報を提供するため，並びに，処理に関する第 11 条，第 14 条ないし第 18 条及び第 31 条と関連するデータ主体に対する通知を，明瞭で平易な言語を用い，明解で理解しやすく，容易にアクセスし得る方式により行うための合理的な手立てを講ずることを定める。その情報は，電子的な手段を含め，適切な手段によって提供される。一般原則として，管理者は，その要求と同じ方式で情報を提供する。

Member States shall provide for the controller to take reasonable steps to provide any information referred to in Article 13 and make any communication with regard to Articles 11, 14 to 18 and 31 relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

2. 構成国は，管理者が，第 11 条及び第 14 条ないし第 18 条に基づき，データ主体の権利の

行使を容易にすることを定める。

Member States shall provide for the controller to facilitate the exercise of the rights of the data subject under Articles 11 and 14 to 18.

3. 構成国は，管理者が，不適切な遅滞なく，書面により，データ主体に対し，彼または彼女の要求への事後対応に関して連絡することを定める。

Member States shall provide for the controller to inform the data subject in writing about the follow up to his or her request without undue delay.

4. 構成国は，第 13 条に基づいて提供される情報及び第 11 条，第 14 条ないし第 18 条及び第 31 条によって行われる通知または活動が，無料で提供されることを定める。特にその反復的な性質という理由により，データ主体からの要求が，明らかに根拠のないもの，または，過剰なものである場合，管理者は，以下のようにできる：
   (a) 情報提供もしくは通知または要求された行動を行うための管理運営上の費用を考慮に入れた上で，合理的な手数料を課金すること；または
   (b) その要求にかかる行動を拒否すること。

Member States shall provide for the information provided under Article 13 and any communication made or action taken pursuant to Articles 11, 14 to 18 and 31 to be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
   (a) charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or
   (b) refuse to act on the request.

管理者は，その要求が明らかに根拠のないもの，または，過剰なものであることを説明する責任を負う。

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

5. 第 14 条または第 16 条に示す要求をしてい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付加的な情報の提供を要求できる。

Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 14 or 16, the controller may request the provision of additional

information necessary to confirm the identity of the data subject.

第 13 条　データ主体が利用できるようにされる情報またはデータ主体に対して与えられる情報
Article 13 Information to be made available or given to the data subject

1. 構成国は，管理者が，少なくとも，以下の情報をデータ主体が利用できるようにすることを定める：
   (a) 管理者の識別名及び連絡先；
   (b) それが適用可能なときは，データ保護責任者の連絡先；
   (c) その個人データについて予定されている処理の目的；
   (d) 監督機関に異議を申立てる権利及び監督機関の連絡先；
   (e) そのデータ主体と関係する個人データへのアクセス，そのデータの訂正または削除及びその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。

   Member States shall provide for the controller to make available to the data subject at least the following information:
   (a) the identity and the contact details of the controller;
   (b) the contact details of the data protection officer, where applicable;
   (c) the purposes of the processing for which the personal data are intended;
   (d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;
   (e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

2. 第 1 項に示す情報提供に加え，構成国は，個別の案件において，彼または彼女の権利を行使できるようにするため，管理者が，データ主体に対し，以下の情報を更に提供することを，法律によって定める：
   (a) その処理の法律上の根拠；
   (b) その個人データが記録保存されることになる期間，または，それが不可能な場合，当該期間を決定するために用いられる基準；
   (c) それが適用可能なときは，第三国または国際組織を含め，その個人データの取得者の類型；
   (d) それが必要なときは，とりわけ，データ主体が知覚なしに個人データが収集される場合，上記以外の情報。

   In addition to the information referred to in paragraph 1, Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:
   (a) the legal basis for the processing;

(b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;
(c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;
(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

3. 構成国は，以下の場合のために，関係する自然人の基本的な権利及び正当な利益を適正に尊重した上で，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ような措置の範囲内において，かつ，その限りで，第 2 項によるデータ主体に対する情報の提供を遅延させ，制限し，または，省略する立法措置を採択できる：
(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支障を避けるため；
(c) 公共の保安を防護するため；
(d) 国家安全保障を防護するため；
(e) 他の者の権利及び自由を保護するため。

Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:
(a) avoid obstructing official or legal inquiries, investigations or procedures;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

4. 構成国は，その全部または一部が第 3 項に列挙する各号のいずれかに該当し得る処理の類型を判定するための立法措置を採択できる。

Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.

第 14 条 データ主体によるアクセスの権利

Article 14 Right of access by the data subject

第 15 条に服して，構成国は，データ主体が，彼または彼女に関する個人データが処理されているか否かの確認を管理者から得る権利，及び，該当する場合，その個人データ及び以

下の情報にアクセスを得る権利を定める:
(a) その処理の目的及び法律上の根拠;
(b) 関係する個人データの類型;
(c) その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, 第三国または国際組織の取得者;
(d) それが可能なときは, 個人データが記録保存されることになる予定期間, 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) データ主体と関係する個人データの訂正または削除及びその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) 監督機関に異議を申立てる権利及び監督機関の連絡先;
(g) 処理実行中の個人データの通知, 及び, その個人データの入手元に関する利用可能な情報の通知。

Subject to Article 15, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
(a) the purposes of and legal basis for the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;
(f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;
(g) communication of the personal data undergoing processing and of any available information as to their origin.

第 15 条 アクセスの権利の制限
Article 15 Limitations to the right of access

1. 構成国は, 以下の場合のために, 関係する自然人の基本的な権利及び正当な利益を十分に尊重した上で, そのような部分的または全面的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ような措置の範囲内において, かつ, その限りで, データ主体のアクセスの権利の全部または一部を制限する立法措置を採択できる:
(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支障を避けるため;
(c) 公共の保安を防護するため;

(d) 国家安全保障を防護するため；
(e) 他の者の権利及び自由を保護するため。

Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:
(a) avoid obstructing official or legal inquiries, investigations or procedures;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

2. 構成国は，その全部または一部が第 1 項の(a)ないし(e)のいずれかに該当し得る処理の類型を判定するための立法措置を採択できる。

Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under points (a) to (e) of paragraph 1.

3. 第 1 項及び第 2 項に示す場合，構成国は，管理者が，データ主体に対し，不適切な遅滞なく，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書面により連絡することを定める。その連絡によって第 1 項の下にある目的に支障が生じ得る場合，その連絡は，省略され得る。構成国は，管理者が，データ主体に対し，監督機関に異議を申立て得ること，または，法務上の救済を求め得ることを連絡することを定める。

In the cases referred to in paragraphs 1 and 2, Member States shall provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

4. 構成国は，その判断が基礎とする事実上の根拠及び法律上の根拠を管理者が文書化することを定める。当該情報は，監督機関が利用できるようにされる。

Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

第 16 条 個人データの訂正または削除の権利及び処理の制限

Article 16 Right to rectification or erasure of personal data and restriction of processing

1. 構成国は，管理者から，不適切な遅滞なく，彼または彼女に関する不正確な個人データの訂正を得るデータ主体の権利を定める。その処理の目的を考慮に入れた上で，構成国は，補足的な文言を提供する手段を含め，データ主体が，不完全な個人データを完全なものとすることを得る権利をもつことを定める。

   Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purposes of the processing, Member States shall provide for the data subject to have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

2. 構成国は，処理が，第 4 条，第 8 条もしくは第 10 条により採択された条項に違反する場合，または，その管理者が服する法律上の義務を遵守するために個人情報が削除されなければならない場合，その管理者に対し，個人データの削除を要求し，かつ，データ主体が，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定める。

   Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

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，その個人データの正確または不正確性が確認され得ない場合；または
   (b) その個人データが証拠の目的のために維持管理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，管理者は，その処理の制限を解除する前に，データ主体に対して連絡する。

   Instead of erasure, the controller shall restrict processing where:
   (a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or
   (b) the personal data must be maintained for the purposes of evidence.

   Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall

inform the data subject before lifting the restriction of processing.

4. 構成国は，管理者が，データ主体に対し，個人データの訂正もしくは削除または処理の制限の拒否，及び，その拒否の理由を書面により通知することを定める。構成国は，以下の場合のために，関係する自然人の基本的な権利及び正当な利益を十分に尊重した上で，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，その限りで，そのような情報を提供すべき義務の全部または一部を制限する立法措置を採択できる：
   (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支障を避けるため；
   (c) 公共の保安を防護するため；
   (d) 国家安全保障を防護するため；
   (e) 他の者の権利及び自由を保護するため。

   Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:
   (a) avoid obstructing official or legal inquiries, investigations or procedures;
   (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
   (c) protect public security;
   (d) protect national security;
   (e) protect the rights and freedoms of others.

   構成国は，管理者が，データ主体に対し，監督機関に異議を申立て得ること，または，法務上の救済を求め得ることを連絡することを定める。

   Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

5. 構成国は，管理者が，不正確な個人データの入手元である職務権限のある機関に対し，不正確な個人データの訂正を連絡することを定める。

   Member States shall provide for the controller to communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

6. 構成国は，個人データが第 1 項，第 2 項及び第 3 項によって訂正もしくは削除され，または，

処理が制限された場合，管理者が取得者に対して連絡すること，及び，その取得者がその取得者の責任においてその個人データを訂正もしくは削除し，または，処理を制限することを定める。

Member States shall, where personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3, provide for the controller to notify the recipients and that the recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

第 17 条　データ主体による権利の行使及び監督機関による検査

Article 17 Exercise of rights by the data subject and verification by the supervisory authority

1. 第 13 条第 3 項，第 15 条第 3 項及び第 16 条第 4 項に示す場合において，構成国は，データ主体の権利が職務権限のある監督機関を介しても行使され得ることを定める措置を採択する。

   In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

2. 構成国は，管理者が，データ主体に対し，第 1 項により監督機関を介して彼または彼女の権利を行使できることを連絡することを定める。

   Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1.

3. 第 1 項に示す権利が行使される場合，その監督機関は，データ主体に対し，少なくとも，全ての必要な検査または見直しが監督機関によって行われたことを連絡する。また，その監督機関は，データ主体に対し，彼または彼女の法務上の救済の権利も連絡する。

   Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

第 18 条　犯罪捜査及び刑事手続におけるデータ主体の権利

Article 18 Rights of the data subject in criminal investigations and proceedings

構成国は，法務上の判断，事件記録または犯罪捜査及び刑事手続の過程において処理さ

れた事件ファイルの中にその個人データが含まれている場合，第 13 条，第 14 条及び第 16 条に示す権利の行使が，構成国法に従って行われることを定め得る。

Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

第Ⅳ章　管理者及び処理者
Chapter IV Controller and processor

第 1 節　一般的な義務
Section 1　General obligations

第 19 条　管理者の義務
Article 19 Obligations of the controller

1. 構成国は，処理の性質，範囲，処理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の様々な蓋然性と深刻度を考慮に入れた上で，管理者が，この指令に従って処理が遂行されることを確保し，かつ，それ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ことを定める。それらの措置は，それが必要なときは，見直され，また，最新のものに改められる。

   Member States shall provide for the controller, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive. Those measures shall be reviewed and updated where necessary.

2. 処理活動との関係において比例的な場合，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。

   Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

第 20 条　バイデザイン及びバイデフォルトによるデータ保護
Article 20 Data protection by design and by default

1. 構成国は，この指令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，管理者が，最新技術，実装費用，並びに，処理の性質，範囲，処理過程及び目的，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蓋然性と深刻度のリスクを考慮に入れた上で，処理の手段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実効的な態様で実装するため，及び，その処理の中に必要な安全確保を統合するために設計された，仮名化のような，適切な技術的上及び組織上の措置を実装することを定める。

Member States shall provide for the controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects.

2. 構成国は，管理者が，その処理の個々の特定の目的のために必要な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とを定める。その義務は，収集される個人データの分量，その個人データの処理の範囲，その個人データの記録保存の期間及びその個人データの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，個人の関与なしに，不特定数の自然人に対して個人データがアクセスできるようにされないことを，デフォルトで確保する。

Member States shall provide for the controller to implement appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

第 21 条 共同管理者

Article 21 Joint controllers

1. 構成国は，複数の管理者が共同して処理の目的及び手段を決定する場合，それらの管理者が共同管理者となることを定める。それらの共同管理者は，それらの管理者らが服する欧州連合法または構成国法によってそれらの管理者らそれぞれの責務が定められていない限り，かつ，その範囲内において，それらの管理者間の覚書によって，この指令の遵守に関するそれらそれぞれの管理者の職責，とりわけ，データ主体の権利の行使と関連する職責，及び，第 13 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に関する職責を，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する。構成国は，

どの共同管理者がデータ主体の権利の行使のための単一連絡部局として行動できるかを指定できる。

Member States shall, where two or more controllers jointly determine the purposes and means of processing, provide for them to be joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with this Directive, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate the contact point for data subjects. Member States may designate which of the joint controllers can act as a single contact point for data subjects to exercise their rights.

2. 第 1 項に示す覚書の条件に拘らず，構成国は，データ主体が，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，この指令によって採択される条項に基づき，彼または彼女の権利を行使すべきことを定め得る。

Irrespective of the terms of the arrangement referred to in paragraph 1, Member States may provide for the data subject to exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.

第 22 条 処理者

Article 22 Processor

1. 構成国は，管理者の代わりの者によって処理が遂行される場合，その処理がこの指令の要件に適合するような態様による適切な技術上及び組織上の安全確保を実装すること，及び，データ主体の権利の保護を確保することの十分な保証を提供する処理者のみを管理者が用いることを定める。

Member States shall, where processing is to be carried out on behalf of a controller, provide for the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Directive and ensure the protection of the rights of the data subject.

2. 構成国は，処理者が，管理者からの事前の個別的または一般的な書面による承認を得ることなく，別の処理者を従事させてはならないことを定める。一般的な書面による承認の場合，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の予定を通知し，それによって，管理者に対し，そのような変更に異議を唱える機会を与える。

Member States shall provide for the processor not to engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. 構成国は，処理者による処理が，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，個人データのタイプ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，欧州連合もしくは構成国法に基づく契約以外の法律行為によって規律されることを定める。契約またはそれ以外の法律行為は，とりわけ，その処理者が以下のとおりであることを定める：
   (a) その管理者からの指示のみに基づいて行動すること；
   (b) 個人データの処理の承認を受けた者が，自ら機密性を確約すること，または，制定法上の適切な守秘義務の下にあ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，適切な手段によって管理者を補佐すること；
   (d) データ処理サービスの提供終了後，管理者の選択により，全ての個人データを削除し，または，管理者に返還すること，並びに，欧州連合法または構成国法がその個人データの記録保存を要求しない限り，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) 別の処理者の従事に関する第 2 項及び第 3 項に示す条件を遵守すること。

Member States shall provide for the processing by a processor to be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
   (a) acts only on instructions from the controller;
   (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
   (c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;
   (d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data;
   (e) makes available to the controller all information necessary to demonstrate compliance with this Article;
   (f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.

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

The contract or the other legal act referred to in paragraph 3 shall be in writing, including in an electronic form.

5. この指令に違反して，処理者が処理の目的及び手段を定めた場合，当該処理者は，当該処理との関係においては，管理者と判断される。

If a processor determines, in infringement of this Directive, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing.

第 23 条 管理者または処理者の承認に基づく処理

Article 23 Processing under the authority of the controller or processor

構成国は，処理者，または，管理者もしくは処理者の承認に基づいて行動し，個人データへのアクセスをもつ者が，管理者からの指示による場合を除き，欧州連合法または構成国法によってそのようにすることが要求されない限り，それらの個人データを処理してはならないことを定める。

Member States shall provide for the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, not to process those data except on instructions from the controller, unless required to do so by Union or Member State law.

第 24 条 処理活動の記録

Article 24 Records of processing activities

1. 構成国は，管理者が，その管理者の責任において，全ての類型の処理活動の記録を維持管理することを定める。その記録は，以下の情報の全てを含める：
   (a) 管理者の名称及び連絡先，並びに，それが適用可能なときは，共同管理者及びデータ保護責任者の名称及び連絡先；
   (b) 処理の目的；
   (c) 第三国または国際組織内の取得者を含め，個人データが開示された取得者または開示されることになる取得者の類型；
   (d) データ主体の類型の記述及び個人データの類型の記述；
   (e) それが適用可能なときは，プロファイリングの利用；
   (f) それが適用可能なときは，第三国または国際組織に対する移転の類型；
   (g) 移転の場合を含め，個人データに予定されている処理業務の法律上の根拠の表示；
   (h) それが可能なときは，異なる類型の個人データの削除のために予定されている期限；

(i) それが可能なときは，第 29 条第 1 項に示す技術上及び組織上の防護措置の一般的な記述。

Member States shall provide for controllers to maintain a record of all categories of processing activities under their responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;
(b) the purposes of the processing;
(c) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
(d) a description of the categories of data subject and of the categories of personal data;
(e) where applicable, the use of profiling;
(f) where applicable, the categories of transfers of personal data to a third country or an international organisation;
(g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;
(h) where possible, the envisaged time limits for erasure of the different categories of personal data;
(i) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

2. 構成国は，各処理者が，管理者の代わりに遂行する全ての類型の処理活動の，以下の事項を含む記録を維持管理することを定める：

(a) その処理者が管理者の代わりに処理を遂行している個々の管理者の処理者の名称及び連絡先，及び，それが適用可能なときは，データ保護責任者の名称及び連絡先；
(b) 個々の管理者の代わりに実施される処理の類型；
(c) それが適用可能なときは，管理者によってそのように明示で指示されている場合，当該第三国または国際組織の識別名を含め，第三国または国際組織に対する個人データの移転；
(d) それが可能なときは，第 29 条第 1 項に示す技術上及び組織上の防護措置の一般的な記述。

Member States shall provide for each processor to maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third

country or international organisation;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

3. 第 1 項及び第 2 項に示す記録は，電子的な方式を含め，書面によるものとする。

The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

管理者及び処理者は，要求に応じて，監督機関がそれらの記録を利用できるようにする。

The controller and the processor shall make those records available to the supervisory authority on request.

第 25 条 履歴（ログ）

Article 25 Logging

1. 構成国は，自動化された処理システムにおいて，少なくとも，収集，修正，照会，移転を含め開示，結合及び削除の処理業務に関し，履歴が保存されることを定める。照会及び開示の履歴は，そのような業務の理由，日時，及び，可能な限り，個人データを照会した者または開示を受けた者の識別名及びそのような個人データの取得者の同一性を確定できるようにする。

Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

2. 履歴は，処理の適法性の検証，自己監視，個人データの完全性及び安全性の確保のため，及び，刑事手続のために限り，利用される。

The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

3. 管理者及び処理者は，要求に応じて，監督機関が履歴を利用できるようにする。

The controller and the processor shall make the logs available to the supervisory authority on request.

第 26 条 監督機関との協力

Article 26 Cooperation with the supervisory authority

構成国は，管理者及び処理者が，要請に応じて，その要請上の職務の遂行において，監督機関と協力することを定める。

Member States shall provide for the controller and the processor to cooperate, on request, with the supervisory authority in the performance of its tasks on request.

第 27 条 データ保護影響評価

Article 27 Data protection impact assessment

1. 処理の性質，範囲，過程及び目的を考慮に入れた上で，あるタイプの処理，とりわけ，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発生させるおそれがある場合，構成国は，管理者が，処理の前に，個人データ保護に対する予定されている処理業務の影響の評価を遂行することを定める。

Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. 第 1 項に示す評価は，少なくとも，予定されている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処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，個人データの保護を確保し，この指令の遵守を説明するための安全確保，防護措置及び仕組みを含める。

The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

第 28 条 監督機関の事前協議

Article 28 Prior consultation of the supervisory authority

1. 構成国は，以下の場合においては，以下の場合において，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ことになる処理の前に，管理者または処理者が監督機関と協議することを定める：

(a) リスクを緩和するための措置が管理者によって講じられない場合，その処理が高度のリスクを生じさせ得ることを第 27 条に定めるデータ保護影響評価が示している場合；または

(b) とりわけ，新たな技術，仕組みまたは手順を用いる場合において，その処理のタイプが，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。

Member States shall provide for the controller or processor to consult the supervisory authority prior to processing which will form part of a new filing system to be created, where:

(a) a data protection impact assessment as provided for in Article 27 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

2. 構成国は，処理と関連して，国内議会によって採択される立法措置またはそのような立法措置を基礎とする法令上の措置の提案を準備する間，監督機関が協議に応ずることを定める。

Member States shall provide for the supervisory authority to be consulted during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to processing.

3. 構成国は，第 1 項による事前協議に服する処理業務のリストを監督機関が策定できることを定める。

Member States shall provide that the supervisory authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

4. 構成国は，管理者が，第 27 条によるデータ保護影響評価を監督機関に提供すること，及び，要求に応じて，その処理の法令順守，及び，とりわけ，データ主体の個人データの保護に対するリスク及び関連する安全確保を監督機関が評価できるようにするための影響評価以外の情報を提供することを定める。

Member States shall provide for the controller to provide the supervisory authority with the data protection impact assessment pursuant to Article 27 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

5. 構成国は，本条の第 1 項に示す予定されている処理がこの指令により採択された条項に違反し得る場合，とりわけ，管理者がリスクを十分に特定しておらず，または，リスクを緩和させていない場合，監督機関が，協議の要請を受けた時から 6 週間以内に，管理者に対し，及び，それが適切なときは，処理者に対し，書面による助言を提供することを定め，また，第 47 条に示す監督機関の権限のいずれかを用い得ることを定める。その期限は，予定されている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。その監督機関は，その管理者に対し，及び，それが適切なときは，その処理者に対し，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，そのような期限延長を連絡する。

Member States shall, where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 of this Article would infringe the provisions adopted pursuant to this Directive, in particular where the controller has insufficiently identified or mitigated the risk, provide for the supervisory authority to provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in Article 47. That period may be extended by a month, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

第 2 節　個人データの安全性

Section 2 Security of personal data

第 29 条　処理の安全性

Article 29　Security of processing

1. 構成国は，最新技術，実装費用，処理の性質，範囲，処理過程及び目的，並びに，自然人の権利及び自由に対する様々な蓋然性と深刻度のリスクを考慮に入れた上で，管理者及び処理者が，とりわけ，第 10 条に示す特別類型の個人データの処理と関連して，そのリスクにとって適切なレベルの安全性を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とを定める。

Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.

2. 自動化された処理に関し，各構成国は，管理者及び処理者が，そのリスクを評価した後，以

下のとおりに設計された措置を実装することを定める:

(a) 処理のために使用される処理機器への無権限の者のアクセスの拒否(「機器のアクセス管理」);
(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) 個人データの無権限の入力, 及び, 記録保存された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) データ通信機器を用いる無権限の者による自動化された処理システムの利用の防止(「利用者管理」);
(e) 自動化された処理システムの利用を承認されている者が, その者のアクセス承認に包摂されている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) データ通信機器を用いてどの個人データが送付もしくは利用できるようにされた組織, または, 送信もしくは利用できるようにされ得る組織を検証及び確認することが可能であることの確保(「通信管理」);
(g) どの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, 誰によってその個人データが入力されたのかを事後的に検証及び確認することが可能であることの確保(「入力管理」);
(h) 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) 侵害の場合において, インストールされているシステムが復旧され得ることの確保(「復旧」);
(j) システムの機能な発揮されること, 機能の異常の発生が報告されることの確保(「信頼性」), 及び, システムの不正操作によって記録保存された個人データが損なわれ得ないことの確保(「完全性」)。

In respect of automated processing, each Member State shall provide for the controller or processor, following an evaluation of the risks, to implement measures designed to:

(a) deny unauthorised persons access to processing equipment used for processing (‘equipment access control’);
(b) prevent the unauthorised reading, copying, modification or removal of data media (‘data media control’);
(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (‘storage control’);
(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment (‘user control’);
(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation (‘data access control’);

(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');
(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');
(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');
(i) ensure that installed systems may, in the case of interruption, be restored ('recovery');
(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

第 30 条 監督機関に対する個人データの侵害の通知

Article 30 Notification of a personal data breach to the supervisory authority

1. 構成国は，個人データの侵害の場合，その個人データの侵害が自然人の権利及び自由に対するリスクを生じさせるおそれがないものではない限り，管理者が，不適切な遅滞なく，かつ，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，監督機関に対し，その個人データの侵害を通知することを定める。監督機関に対する通知が 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。

Member States shall, in the case of a personal data breach, provide for the controller to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. 処理者は，個人データの侵害に気づいた後，不適切な遅滞なく，管理者に対して，通知する。

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. 第 1 項に示す通知は，少なくとも：
(a) それが可能なときは，関係するデータ主体の類型及び予想される最大数並びに関係する個人データ記録の類型及び予想される最大数を含め，個人データの侵害の性質を記述し；
(b) データ保護責任者の姓名及び連絡先，または，より多くの情報を入手することのできる他の連絡部局を通知し；

(c) その個人データの侵害の結果としてあり得る事態を記述し；
(d) それが適切なときは，その侵害のあり得る負の影響を緩和するための措置を含め，その個人データの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が行われた措置を記述する。

The notification referred to in paragraph 1 shall at least:
(a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. 同時に情報を提供できない場合，かつ，そのような場合に限り，その情報は，更に不適切な遅滞を伴うことなく，その状況に応じて提供され得る。

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. 構成国は，管理者が，その個人データの侵害に関する事実関係，その影響及び復旧措置を含め，第 1 項に示す個人データの侵害を文書化することを定める。その文書は，本条の遵守を検証するために，監督機関が利用できるようにされる。

Member States shall provide for the controller to document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

6. 構成国は，その個人データの侵害が，他の構成国の管理者によって送付され，または，他の構成国の管理者に対して送付された個人データを含んでいる場合，当該構成国の管理者に対し，不適切な遅滞なく，第 3 項に示す情報を連絡することを定める。

Member States shall, where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, provide for the information referred to in paragraph 3 to be communicated to the controller of that Member State without undue delay.

第 31 条 データ主体に対する個人データの侵害の通知

Article 31 Communication of a personal data breach to the data subject

1. 構成国は，個人データの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場合，管理者が，そのデータ主体に対し，不適切な遅滞なく，その個人データの侵害を通知することを定める。

   Member States shall, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, provide for the controller to communicate the personal data breach to the data subject without undue delay.

2. 本条第 1 項に示すデータ主体に対する通知は，明確で平易な言語により，その個人データの侵害の性質を記述し，かつ，少なくとも，第 30 条第 3 項の(b)，(c)及び(d)に示す情報及び措置を含める。

   The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in points (b), (c) and (d) of Article 30(3).

3. 第1項に示すデータ主体に対する通知は，以下の条件のいずれかに該当する場合，要求してはならない：
   (a) 管理者が，適切な技術上及び組織上の防護措置，とりわけ，暗号のような，そのデータへのアクセスが承認されていない者にはその個人データを識別できないようにされる措置を実装し，かつ，個人データの侵害によって影響を受けた個人データに対してそれらの措置が適用された場合；
   (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しそうになくなることを確保する事後的な措置を講じた場合；
   (c) それが過大な努力を要し得る場合。そのような場合，データ主体が平等に実効的な態様で通知されるような公衆通信またはそれに類する措置が代替する。

   The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
   (a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
   (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
   (c) it would involve a disproportionate effort. In such a case, there shall instead be a public

communication or a similar measure whereby the data subjects are informed in an equally effective manner.

4. 管理者がデータ主体に対して個人データの侵害をまだ連絡をしていない場合，監督機関は，その個人データの侵害が高度なリスクを発生させる蓋然性を考慮した上で，管理者に対し，そのようにすることを要求でき，または，第 3 項に示す条件のいずれかに該当することを判断できる。

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

5. 第 1 項に示すデータ主体に対する通知は，第 13 条第 3 項に示す条件に服し，かつ，同項を根拠として，遅延させ，制限し，または，省略され得る。

The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 13(3).

第 3 節 データ保護責任者
Section 3 Data protection officer

第 32 条 データ保護責任者の指定
Article 32 Designation of the data protection officer

1. 構成国は，管理者が，データ保護責任者を指名することを定める。構成国は，裁判所またはそれ以外の独立の法務機関に対し，その法務上の能力において活動する場合，当該義務を免除し得る。

Member States shall provide for the controller to designate a data protection officer. Member States may exempt courts and other independent judicial authorities when acting in their judicial capacity from that obligation.

2. データ保護責任者は，彼または彼女の専門家としての資質，及び，とりわけ，彼または彼女のデータ保護の法令及び実務に関する専門知識並びに第 34 条に示す職務を満たすための能力を基礎として，指定される。

The data protection officer shall be designated on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law and practice and ability to fulfil the

tasks referred to in Article 34.

3. その組織の構造及び規模を考慮に入れた上で，複数の職務権限のある機関のために，単一のデータ保護責任者が指定され得る。

A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.

4. 構成国は，管理者が，データ保護責任者の連絡先を公表し，かつ，監督機関に対してそれを通知することを定める。

Member States shall provide for the controller to publish the contact details of the data protection officer and communicate them to the supervisory authority.

第 33 条 データ保護責任者の地位

Article 33 Position of the data protection officer

1. 構成国は，管理者が，個人データの保護と関連する全ての問題にデータ保護責任者が適正かつ適時の態様で関与することを確保することを定める。

Member States shall provide for the controller to ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. 管理者は，第 34 条に示す職務の遂行において，その職務を遂行し，個人データ及び処理業務にアクセスするため，そして，彼もしく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，データ保護責任者を支援する。

The controller shall support the data protection officer in performing the tasks referred to in Article 34 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

第 34 条 データ保護責任者の職務

Article 34 Tasks of the data protection officer

構成国は，管理者が，データ保護責任者に対して，少なくとも以下の職務を委任することを定める：

(a) 管理者に対し，及び，処理を遂行する従業者に対し，この指令及び欧州連合または構成国のデータ保護条項によるデータ保護責任者の義務を情報提供し，かつ，助言すること；

(b) 責任の割当て，処理業務に関与する職員の認識向上及び訓練並びに関連する監査を含め，この指令，欧州連合または構成国の他のデータ保護条項並びに個人データの保護と関連する管理者の基本方針の遵守を監視すること；
(c) 第27条によるデータ保護影響評価及びその実施の監視と関連して要請を受けた場合，助言を提供すること；
(d) 監督機関と協力すること；
(e) 第 28 条に示す事前協議を含め，処理と関連する事項に関して監督機関のための連絡部局として行動すること，及び，それが適切なときは，それ以外の事項に関して協議すること。

Member States shall provide for the controller to entrust the data protection officer at least with the following tasks:
(a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to this Directive and to other Union or Member State data protection provisions;
(b) to monitor compliance with this Directive, with other Union or Member State data protection provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 27;
(d) to cooperate with the supervisory authority;
(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 28, and to consult, where appropriate, with regard to any other matter.

第Ⅴ章 第三国または国際組織に対する個人データの移転

Chapter V Transfers of personal data to third countries or international organisations

第 35 条 個人データの移転に関する基本原則

Article 35 General principles for transfers of personal data

1. 構成国は，この指令の他の条項によって採択された国内条項の遵守に服して，別の第三国または国際組織に対する転送を含め，現在実行中の個人データまたは第三国または国際組織に対する移転後の処理が予定されている個人データの職務権限のある機関による移転が，本章に定める条件に適合する場合に限り，すなわち，以下の場合に限り，起きることを定める：
(a) 第 1 条第 1 項に定める目的のために移転が必要となる場合；
(b) 第 1 条第 1 項に示す目的のための職務権限のある機関である第三国または国際組織

の管理者に対して個人データが移転される場合;

(c) 個人データが別の構成国から送付され，または，利用できるようにされた場合，当該構成国が，その構成国の国内法に従った移転に対し，その構成国の事前の承認を与えている場合;

(d) 欧州委員会が第 36 条による十分性の判定を採択している場合，または，そのような判定がないときは，第 37 条による適切な安全確保が提供され，もしくは，存在している場合，または，第 36 条による十分性の判定及び第 37 条に従う適切な安全確保がないときは，第 38 条による特別の状況のための特例が適用される場合;並びに

(e) 他の第三国または国際組織に対する転送の場合において，最初の移転を遂行する職務権限のある機関または同一の構成国の別の職務権限のある機関が，犯罪行為の重大性，その個人データが最初に移転された目的及び個人データが転送される第三国または国際組織における個人データ保護のレベルを含め，関連する全ての要素を十分に考慮に入れて検討した後，その転送を承認する場合。

Member States shall provide for any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation to take place, subject to compliance with the national provisions adopted pursuant to other provisions of this Directive, only where the conditions laid down in this Chapter are met, namely:

(a) the transfer is necessary for the purposes set out in Article 1(1);

(b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1);

(c) where personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in accordance with its national law;

(d) the Commission has adopted an adequacy decision pursuant to Article 36, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37, derogations for specific situations apply pursuant to Article 38; and

(e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

2. 構成国は，第 1 項(c)に従った別の構成国による事前の承認のない移転に関し，その個人デ

ータの移転が，構成国もしくは第三国の公共の保安または構成国の必須の利益に対する差し迫った重大な脅威を防止するために必要であり，かつ，適時に事前の承認を獲得し得ない場合に限り，許容されることを定める。事前の承認を与える職責をもつ機関は，遅滞なく，連絡を受ける。

Member States shall provide for transfers without the prior authorisation by another Member State in accordance with point (c) of paragraph 1 to be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

3. この指令によって確保された自然人の保護のレベルが損なわれないことを確保するために，本章の全ての条項が適用される。

All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined.

第 36 条　十分性の判定に基づく移転

Article 36 Transfers on the basis of an adequacy decision

1. 構成国は，当の第三国，その第三国内の地域もしくは 1 もしくは複数の特定の部門または国際組織が，十分なレベルのデータ保護を確保していると欧州委員会が判定した場合，第三国または国際組織に対する個人データの移転が起き得ることを定める。そのような移転は，個別の承認を要しない。

Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. 保護のレベルの十分性を評価する際，欧州委員会は，とりわけ，以下の要素を考慮に入れる：
   (a) 法の支配，人権及び基本的自由の尊重，（公共の保安，国防，国家安全保障及び犯罪法及び行政機関の個人データへのアクセスと関係する立法を含め）一般的及び部門別の関連立法，並びに，そのような立法の実装，（他の第三国または国際組織に対する個人データの転送に関する規定を含め）データ保護の規定，職業上の規則及び防護措置の実装であって，当該第三国または国際組織内で実施されているもの，判例法，並びに，実効的で執行可能なデータ主体の権利，その個人データが移転されるデータ

主体のための実効的な行政上及び法務上の救済;

(b) データ主体がその権利を行使する際の支援と助言のための，及び，構成国の監督機関との間の協力のための十分な執行権限を含め，データ保護法令の遵守を確保すること及びそれを執行することに関して職責を負う，第三国内の，または，国際機関がそれに服する1もしくは複数の独立の監督機関が存在し，かつ，実効的に稼働していること;並びに

(c) とりわけ，個人データの保護に関し，関係する第三国もしくは国際組織が加入している国際的な確約，または，法律上の拘束力のある条約もしくは法律文書から生ずる義務，並びに，多国間制度または領域制度への参加から生ずる義務。

the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are transferred;

When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. 欧州委員会は，保護のレベルの十分性を評価した後，実装行為により，第三国，第三国内の地域または 1 もしくは複数の特定の分野または国際組織が，本条第 2 項の意味における十分なレベルの保護を確保していると判定できる。その実装行為は，少なくとも 4 年毎の定期的な見直しの仕組みを定め，その見直しは，その第三国または国際組織における関係する全ての発展を考慮に入れる。その実装行為は，その領域別の適用及び部門別の適用を識別し，かつ，それが適用可能なときは，本条第 2 項(b)に示す監督機関を識別する。その実装行為は，第 58 条第 2 項に示す審議手続に従って採択される。

The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide a mechanism for periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 58(2).

4. 欧州委員会は，継続的に，第 3 項によって採択された判定の有効性に影響を与え得る第三国及び国際組織内における発展を監視する。

The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3.

5. 欧州委員会は，とりわけ，本条の第 3 項に示す見直しの後，第三国，第三国内の地域または 1 もしくは複数の特定の分野または国際組織が本条第 2 項の意味における十分なレベルの保護を確保しなくなったことを利用可能な情報が明らかにしたときは，必要な範囲内で，実装行為により，遡及効をもつことなく，本条第 3 項に示す判定を取消し，修正し，または，停止とする。それらの実装行為は，第 58 条第 2 項に示す審議手続に従って採択される。

The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

緊急性という正当化される優先的な根拠がある場合，欧州委員会は，第 58 条第 3 項に示す手続に従い，直ちに，適用可能な実装行為を採択する。

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 58(3).

6. 欧州委員会は，第 5 項によって行われた決定から生じている状況を解消するため，その第三国または国際組織との間の協議に入る。

The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. 構成国は，本条の第 5 項による決定が，第 37 条及び第 38 条による当の第三国，第三国内の地域または 1 もしくは複数の特定の分野または国際組織に対する個人データの移転を妨げてはならないことを定める。

Member States shall provide for a decision pursuant to paragraph 5 to be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 37 and 38.

8. 欧州委員会は，EU 官報及びその Web サイト上において，第三国，第三国内の地域もしくは特定の分野または国際組織のリストを公開し，それによって，十分なレベルの保護があると判定されたこと，または，それが確保されなくなったと判定されたことを公表する。

The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

第 37 条　適切な安全確保に服する移転

Article 37 Transfers subject to appropriate safeguards

1. 第 36 条第 3 項による判定がない場合，構成国は，以下の場合において，第三国または国際組織に対する個人データの移転が起き得ることを定める：
   (a) 法律上の拘束力のある法律文書の中で，個人データの保護に関する適切な安全確保が約定されている場合；または
   (b) 個人データの移転と関連する全ての状況を評価した管理者が，個人データの保護に関して適切な安全確保が存在すると判断する場合。

In the absence of a decision pursuant to Article 36(3), Member States shall provide that a transfer of

personal data to a third country or an international organisation may take place where:

(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

(b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

2. 管理者は，監督機関に対し，第 1 項(b)に基づく移転の類型に関して連絡する。

The controller shall inform the supervisory authority about categories of transfers under point (b) of paragraph 1.

3. 移転が第 1 項(b)を基礎とする場合，そのような移転は，移転の日時，取得者である職務権限のある機関に関する情報，移転の正当性及び移転される個人データを含め，文書化され，かつ，その文書は，要請に応じて，監督機関が利用できるようにされる。

When a transfer is based on point (b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

第 38 条 特別な状況のための特例

Article 38 Derogations for specific situations

1. 第 36 条による十分性の判定がない場合，または，第 37 条による適切な安全確保がない場合，構成国は，以下の場合に移転が必要であることを条件とする限り，第三国または国際組織に対する個人データの移転またはある類型の個人データの移転が起き得ることを定める：

(a) データ主体または他の者の生存の利益を保護するため；

(b) 個人データの移転元構成国法がそのように定める場合，データ主体の正当な利益を保護するため；

(c) 構成国または第三国の公共の保安に対する差し迫った重大な脅威を防止するため；

(d) 個別の案件において，第 1 条第 1 項に定める目的のため；または

(e) 個別の案件において，第 1 条第 1 項に定める目的と関連する訴訟の提起，攻撃または防御のため。

In the absence of an adequacy decision pursuant to Article 36, or of appropriate safeguards pursuant to Article 37, Member States shall provide that a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that the transfer is necessary:

(a) in order to protect the vital interests of the data subject or another person;

(b) to safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;
(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;
(d) in individual cases for the purposes set out in Article 1(1); or
(e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1(1).

2. 第 1 項の(d)及び(e)に定める移転における公共の利益よりも関係するデータ主体の基本的な権利及び自由の方が優先すると移転元である職務権限のある機関が判断する場合，個人データを移転してはならない。

Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.

3. 移転が第 1 項を基礎とする場合，そのような移転は，移転の日時，取得者である職務権限のある機関に関する情報，移転の正当性及び移転される個人データを含め，文書化され，かつ，その文書は，要請に応じて，監督機関が利用できるようにされる。

Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

第 39 条 第三国に設けられた取得者に対する個人データの移転

Article 39 Transfers of personal data to recipients established in third countries

1. 第 35 条(b)の特例により，かつ，本条第 2 項に示す国際協定を妨げることなく，欧州連合法または構成国法は，個別の特別の案件において，この指令の他の条項が遵守されており，かつ，以下の条件が全て満たされている場合に限り，第 3 条第 7 項(a)に示す職務権限のある機関が，第三国内に拠点のある取得者に対し，直接に個人データを移転することを定め得る：
(a) 第 1 条第 1 項に定める目的のために欧州連合法または構成国法が定める移転元である職務権限のある機関の職務を遂行のために，その移転が厳格に必要であること；
(b) 関係するデータ主体のいかなる基本的権利及び自由も，当の案件において移転を必要とする公共に利益に優先しない旨を移転元である職務権限のある機関が判断すること；
(c) とりわけ，その移転が適時に達成され得ないという理由により，第三国内の第 1 条第 1

項に示す目的のための職務権限のある機関への移転が非実効的かつ不適切である旨を移転元である職務権限のある機関が判断すること;

(d) それが非実効的かつ不適切でない限り, 第三国内の第 1 項第 1 項に示す目的のための職務権限のある機関が, 不適切な遅滞なく, 連絡を受けること;

(e) 移転元である職務権限のある機関が, 取得者に対し, そのような処理が必要であることを条件としてその個人データが取得者に限って処理されるための特定された目的を連絡すること。

By way of derogation from point (b) of Article 35(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, Union or Member State law may provide for the competent authorities referred to in point (7)(a) of Article 3, in individual and specific cases, to transfer personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled:

(a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1);

(b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

(c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

(d) the authority that is competent for the purposes referred to in Article 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;

(e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

2. 第 1 項に示す国際協定は, 刑事における法務上の協力及び警察の協力の分野の, 構成国と第三国との間において有効な 2 国間または多国間の国際協定とする。

An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

3. 移転元である職務権限のある機関は, 監督機関に対し, 本条に基づく移転に関して連絡する。

The transferring competent authority shall inform the supervisory authority about transfers under

this Article.

4. 移転が第 1 項を基礎とする場合，そのような移転は，文書化される。

Where a transfer is based on paragraph 1, such a transfer shall be documented.

第 40 条 個人データの保護のための国際協力

Article 40 International cooperation for the protection of personal data

第三国及び国際組織に関し，欧州委員会及び構成国は，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実効的な執行を促進するための国際的な協力の仕組みを構築すること；

(b) 個人データの保護及びそれ以外の基本的な権利及び自由の保護のための適切な安全確保に服して，連絡の媒介，苦情相談，調査の補助及び情報交換を含め，個人データの保護のための立法の執行において，国際的な相互補助を提供すること；

(c) 関連する利害関係者との間の意見交換，及び，個人データ保護のための立法の執行における国際的な協力を更に進めることを狙いとする活動に従事すること；

(d) 第三国との間の裁判管轄権の抵触に関するものを含め，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。

In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

第VI章 独立の監督機関
Chapter VI Independent supervisory authorities

第 1 節 独立の地位
Section 1 Independent status

第 41 条 監督機関
Article 41 Supervisory authority

1. 各構成国は，処理と関連する自然人の基本的な権利及び自由を保護するため，並びに，欧州連合内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，この指令の適用の監視に関する職責を負う 1 または複数の独立の行政機関（「監督機関」）を定める。

   Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).

2. 各監督機関は，欧州連合全域におけるこの指令の一貫性のある適用のために貢献する。その目的のために，監督機関は，第 VII 章に従い，相互に協力し，かつ，欧州委員会と協力する。

   Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.

3. 構成国は，規則(EU) 2016/679 に基づいて設けられる監督機関をもってこの指令に示す監督機関とし，かつ，本条第 1 項に基づいて設けられる監督機関の職務に関して職責を負う者とみなすことを定め得る。

   Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

4. 1 つの構成国において複数の監督機関が設けられる場合，当該構成国は，第 51 条に示す委員会内でそれらの監督機関を代表すべき監督機関を指定する。

   Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which are to represent those authorities in the Board referred

to in Article 51.

第 42 条 独立性

Article 42 Independence

1. 各構成国は，各監督機関が，この指令に従ってその職務を遂行し，その権限を行使する際，完全に独立して行動することを定める。

   Each Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.

2. 構成国は，その構成国の監督機関の構成員が，この指令に従ってその職務を遂行し，その権限を行使する際，直接または間接の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ことを定める。

   Member States shall provide for the member or members of their supervisory authorities in the performance of their tasks and exercise of their powers in accordance with this Directive, to remain free from external influence, whether direct or indirect, and that they shall neither seek nor take instructions from anybody.

3. 構成国の監督機関の構成員は，その構成員の義務と適合しない行動を控えることとし，かつ，その在任期間中は，有償であるか否かを問わず，その職務と適合しない仕事に従事してはならない。

   Members of Member States' supervisory authorities shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. 各構成国は，各監督機関が，相互補助，協力及び委員会への参加の過程において遂行されるものを含め，その職務を実効的に遂行し，その権限を行使するために必要となる人員，技術上及び資金上の資源，施設及びインフラの提供を受けることを確保する。

   Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. 各構成国は，個々の監督機関が，その監督機関自身の職員を選任し，もつことを確保する。その職員は，専ら，関係する監督機関の構成員の指示に服する。

Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. 各構成国は，各監督機関がその監督機関の独立性に影響を与えない会計監査に服すること，及び，区分された公式の年次予算を受けることを確保する。その予算は，国全体の予算または国家予算の一部とされ得る。

Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

第 43 条 監督機関の構成員となるための一般的な条件

1. 構成国は，以下の機関の透明性のある手続により，その構成国の個々の監督機関の個々の構成員が任命されることを定める：
   － 構成国の議会；
   － 構成国の政府；
   － 構成国の首長；または
   － 構成国法に基づく指定によって信任された独立の組織。

Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:
   － their parliament;
   － their government;
   － their head of State; or
   － an independent body entrusted with the appointment under Member State law.

2. 個々の構成員は，とりわけ，その構成員の義務を履行し，権限を行使するために要する，とりわけ，個人データの保護の分野における資格，経験及び技能をもつ者とする。

Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform their duties and exercise their powers.

3. 構成員の義務は，関係する構成国の法律に従い，その任期が終了した時，辞任の時または強制的な退任の時に終了する。

The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. 構成員は，重大な非違行為があった場合，または，その義務の履行のために要求される条件を満たさなくなった場合に限り，解任される。

A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

第 44 条 監督機関の設置に関する規定

Article 44 Rules on the establishment of the supervisory authority

1. 各構成国は，法律によって，以下の全ての事項を定める：
   (a) 各監督機関の設置；
   (b) 各監督機関の構成員として任命されるために要求される資格及び適格性の条件；
   (c) 各監督機関の構成員の任命のための規定及び手続；
   (d) 各監督機関の構成員の少なくとも 4 年以上の任期，ただし，2016 年 5 月 6 日の後の最初の任命に関しては，交互的な任命手続により監督機関の独立を保護するために必要な場合，その一部がより短い任期で行われ得る；
   (e) 各監督機関の構成員が再任されるか否か，及び，再任可能な場合，その再任のための資格をもつ回数；
   (f) 各監督機関の構成員及び職員の義務を規律する条件，行動の制限，在任期間中及びその後を通じての職務と適合しない仕事及び収益，並びに，雇用の終了を規律する規定。

Each Member State shall provide by law for all of the following:
   (a) the establishment of each supervisory authority;
   (b) the qualifications and eligibility conditions required to be appointed as a member of each supervisory authority;
   (c) the rules and procedures for the appointment of the member or members of each supervisory authority;
   (d) the duration of the term of the member or members of each supervisory authority of not less than four years, except for the first appointment after 6 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
   (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;
   (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. 各監督機関の構成員及び職員は，欧州連合または構成国法に従い，その在任中及びその

後においても，それらの者の職務の遂行及びそれらの者の権限の行使の過程でそれらの者が知った全ての機密情報に関し，職業上の守秘の義務に服する。その在任中，当該職業上の秘密の義務は，とりわけ，この指令の違反行為に関する自然人からの通報に適用される。

The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or the exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Directive.

第 2 節　職務権限，職務及び権限
Section 2 Competence, tasks and powers

第 45 条　職務権限
Article 45 Competence

1. 各構成国は，各監督機関が，その機関自身の構成国の領土において，この指令に従って，その機関に対して与えられた職務を遂行し，かつ，その機関に対して与えられた権限を行使するための職務権限をもつことを定める。

   Each Member State shall provide for each supervisory authority to be competent for the performance of the tasks assigned to, and for the exercise of the powers conferred on, it in accordance with this Directive on the territory of its own Member State.

2. 各構成国は，各監督機関が，その裁判所の法務上の権限において行動する際における裁判所の処理業務の監督に関する職務権限をもたないことを定める。構成国は，その構成国の監督機関が，裁判所以外の独立の法務機関の法務上の権限において行動する際の裁判所以外の独立の法務機関の処理業務を監督する職務権限をもたないことを定め得る。

   Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity. Member States may provide for their supervisory authority not to be competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.

第 46 条　職務
Article 46 Tasks

1. 各構成国は，その領土において，各監督機関が，以下の職務を行うことを定める：

(a) この指令によって採択された条項及びその実装措置の適用を監視し，執行すること；
(b) 処理と関連するリスク，規定，安全確保及び権利の公衆の認識及び理解を向上させること；
(c) 構成国法に従い，国内議会，政府並びにそれ以外の機関及び組織に対し，処理と関連する自然人の権利及び自由の保護に関する立法上の措置及び行政上の措置に関し，助言すること；
(d) この指令に基づく管理者及び処理者の義務の，それらの者の認識を向上させること；
(e) 要請に応じて，データ主体に対し，この指令に基づくデータ主体の権利の行使に関する情報を提供し，また，それが適切なときは，その目的のために，別の構成国の監督機関と協力すること；
(f) データ主体によって申立てられた異議，または，第 55 条に従って組織，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，異議申立事項を調査し，かつ，とりわけ，更に調査することまたは他の監督機関と協力することが必要な場合には，合理的な期間内に，その異議申立人に対し，その調査の進捗状況及び結果を連絡すること；
(g) 第 17 条による処理の適法性を点検し，かつ，データ主体に対し，合理的な期間内に，同条第 3 項による点検の結果を連絡し，または，点検が遂行されなかった理由を連絡すること；
(h) この指令の一貫性のある適用及び執行を確保するという観点から，情報共有による場合を含め，他の監督機関と協力し，かつ，相互補助を提供すること；
(i) 他の監督機関または別の行政機関から受領した情報を基礎とする場合を含め，この指令の適用に関して調査を行うこと；
(j) その発展が個人データの保護に影響を与えるものである限り，関連する発展，とりわけ，情報通信技術の発展を監視すること；
(k) 第 28 条に示す処理業務に関し，助言を提供すること；並びに，
(l) 委員会の活動に貢献すること。

Each Member State shall provide, on its territory, for each supervisory authority to:
(a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;
(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;
(c) advise, in accordance with Member State law, the national parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
(d) promote the awareness of controllers and processors of their obligations under this Directive;
(e) upon request, provide information to any data subject concerning the exercise of their rights under this Directive and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 55, and investigate, to the extent appropriate, the subject-matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
(g) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;
(h) cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this Directive;
(i) conduct investigations on the application of this Directive, including on the basis of information received from another supervisory authority or other public authority;
(j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;
(k) provide advice on the processing operations referred to in Article 28; and
(l) contribute to the activities of the Board.

2. 各監督機関は，他の通信手段を排除することなく，電子的にも完了され得る異議申立書の提出を提供することのような措置によって，第 1 項(f)に示す異議申立書の提出を容易にする。

Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. 各監督機関の職務の遂行は，データ主体及びデータ保護責任者に対しては，無料とする。

The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer.

4. 要求が，特にその反復性という理由により，要求が，明らかに根拠のないもの，または，過剰なものである場合，監督機関は，事務処理費用を基礎とする合理的な手数料を課金し，または，その要求にかかる行動を拒否できる。監督機関は，その要求が明らかに根拠のないものであることまたは過剰なものであることを説明する責任を負う。

Where a request is manifestly unfounded or excessive, in particular because it is repetitive, the supervisory authority may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating that the request is manifestly unfounded or excessive.

第 47 条 権限

Article 47 Powers

1. 各構成国は，法律によって，各監督機関が，実効的な調査の権限をもつことを定める。それらの権限は，少なくとも，処理されている全ての個人データへのアクセス及び監督機関の職務を遂行するために必要となる全ての情報へのアクセスを，管理者及び処理者から得る権限を含める。

   Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

2. 各構成国は，法律によって，各監督機関が，例えば，以下のような，実効的な是正の権限をもつことを定める：
   (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指令により採択された条項に違反する可能性があるという警告を発すること；
   (b) 管理者または処理者に対し，それが適切であるときは，指定された態様により，かつ，指定された期間内に，とりわけ，第 16 条による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によって，処理業務を，この指令により採択された条項を遵守するものとさせるように命ずること；
   (c) 処理に対し，禁止を含め，一時的または確定的な制限を加えること。

   Each Member State shall provide by law for each supervisory authority to have effective corrective powers such as, for example:
   (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions adopted pursuant to this Directive;
   (b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 16;
   (c) to impose a temporary or definitive limitation, including a ban, on processing.

3. 各構成国は，法律によって，監督機関が，第 28 条に示す事前協議手続に従って管理者に対して助言するための実効的な助言の権限をもつこと，また，監督機関が，自らの発意により，または，要請に応じて，その構成国の国内議会及びその構成国の政府に対し，または，その構成国の国内法に従い，それら以外の機関及び組織並びに公衆に対し，個人データの保護と関連する全ての問題に関し，意見を発する権限をもつことを定める。

Each Member State shall provide by law for each supervisory authority to have effective advisory powers to advise the controller in accordance with the prior consultation procedure referred to in Article 28 and to issue, on its own initiative or on request, opinions to its national parliament and its government or, in accordance with its national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

4. 本条によって監督機関に対して与えられた権限の行使は，憲章に従って欧州連合法及び構成国法に定められている実効的な法務上の救済及び適正手続を含め，適切な安全確保に服する。

The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, as set out in Union and Member State law in accordance with the Charter.

5. 各構成国は，法律によって，この指令に従って採択された条項の違反行為に対して法務機関の注意を向けさせる権限をもつこと，及び，それが適切なときは，この指令によって採択された条項を執行するため，訴訟を提起することまたは訴訟手続に関与する権限をもつことを定める。

Each Member State shall provide by law for each supervisory authority to have the power to bring infringements of provisions adopted pursuant to this Directive to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, in order to enforce the provisions adopted pursuant to this Directive.

第 48 条 違反行為の通報

Article 48 Reporting of infringements

構成国は，職務権限のある機関が，この指令の違反行為を秘密裡に通報することを推進するための実効的な仕組みを設けることを定める。

Member States shall provide for competent authorities to put in place effective mechanisms to encourage confidential reporting of infringements of this Directive.

第 49 条 活動報告書

Article 49 Activity reports

各監督機関は，その監督機関の活動に関する年次報告書を作成する。その報告書は，通知を受けた違反行為のタイプ及び科された制裁のタイプのリストを含め得る。その報告書は，国内議会，政府及び構成国法によって指定されたその他の機関に対して送付される。その報

告書は，公衆，欧州委員会及び委員会が利用できるようにされる。

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of penalties imposed. Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, the Commission and the Board.

第Ⅶ章 協力
Chapter VII Cooperation

第 50 条 相互補助
Article 50 Mutual assistance

1. 各構成国は，その構成国の監督機関が，一貫性のある態様でこの指令を実装及び適用するため，関連情報及び相互補助を相互に提供すること，並びに，実効的な協力のための仕組みを相互に設けることを定める。相互補助は，とりわけ，情報提供の要請，並びに，協議，検査及び調査を遂行することの要請のような，監督上の措置を包摂する。

Each Member State shall provide for their supervisory authorities to provide each other with relevant information and mutual assistance in order to implement and apply this Directive in a consistent manner, and to put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

2. 各構成国は，各監督機関が，不適切な遅滞なく，かつ，その要請を受けてから遅くとも 1 か月以内に，他の監督機関の要請に応えるために要求される全ての適切な措置を講ずることを定める。そのような措置は，とりわけ，調査の実施に関する関連情報の送信を含め得る。

Each Member States shall provide for each supervisory authority to take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. 補助の要請書は，その要請の目的及び理由を含め，必要な全ての情報を含める。交換される情報は，それが要請された目的のために限り，利用される。

Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. 要請先監督機関は，以下の場合でない限り，その要請の遵守を拒否してはならない:
   (a) その要請の対象事項に関し，または，執行の要請を受けた措置に関し，職務権限がない場合;または
   (b) その要請に従うことが，この指令の違反となり得る場合，または，その要請先監督機関が服する欧州連合法もしくは構成国法の違反となり得る場合。

   The requested supervisory authority shall not refuse to comply with the request unless:
   (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
   (b) compliance with the request would infringe this Directive or Union or Member State law to which the supervisory authority receiving the request is subject.

5. 要請先監督機関は，要請元監督機関に対し，その結果を連絡し，または，場合により，その要請に応ずるために講じられた措置の進捗状況を連絡する。要請先監督機関は，第 4 項により要請の遵守を拒否する場合，その理由を提供する。

   The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. 要請先監督機関は，原則として，電子的な手段により，標準化されたフォーマットを用いて，別の監督機関から求められた情報を提供する。

   Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. 要請先監督機関は，相互補助を求める要請により当該監督機関によって講じられた措置に関し，手数料を課金してはならない。監督機関は，例外的な状況において，相互補助の提供から生ずる特別の支出を相互に補填するための規定に同意できる。

   Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. 欧州委員会は，実装行為により，本条に示す相互補助のためのフォーマット及び手続，並びに，各監督機関の間及び監督機関と委員会との間における電子的な手段による情報交換のための手立てを定め得る。それらの実装行為は，第 58 条第 2 項に示す審議手続に従って採択される。

The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

第 51 条 委員会の職務

Article 51 Tasks of the Board

1. 規則(EU) 2016/679 によって設けられた委員会は，この指令の適用範囲内にある処理との関係において，以下の全ての職務を遂行する：
   (a) この指令の改正提案に関するものを含め，欧州連合における個人データの保護と関連する検討課題に関し，欧州委員会に対して助言すること；
   (b) 委員会自らの発意により，委員会の構成員のいずれかからの要請に応じて，または，欧州委員会の要請に応じて，この指令の適用に包摂される全ての問題を検討すること，並びに，この指令の一貫性のある適用を推進するため，運用指針，勧告及びベストプラクティスを発行すること；
   (c) 第 47 条第 1 項及び第 3 項に示す措置の適用に関する監督機関のための運用指針を作成すること；
   (d) 個人データの侵害の確認，第 30 条第 1 項及び第 2 項に示す不適切な遅滞の判断に関し，並びに，管理者または処理者が個人データの侵害の通知を要求される特別の状況に関し，本副項の(b)に従って，運用指針，勧告及びベストプラクティスを発行すること；
   (e) 第 31 条第 1 項に示す自然人の権利及び自由に対する高度なリスクを個人データの侵害がもたらす可能性のある状況に関し，本副項の(b)に従って，運用指針，勧告及びベストプラクティスを発行すること；
   (f) 運用指針，勧告及びベストプラクティスの実務上の適用を見直すこと；
   (g) 第三国，第三国内の地域もしくは特定の分野または国際組織が十分なレベルの保護を確保しなくなったか否かの評価のための場合を含め，第三国，第三国内の地域もしくは特定の分野または国際組織における保護のレベルの十分性を評価するための意見を欧州委員会に対して提供すること；
   (h) 監督機関の間において，協力並びに 2 国間及び多国間の情報及びベストプラクティスの実効的な交換を促進すること；
   (i) 監督機関の間において，及び，それが適切なときは，第三国の監督機関または国際組織との間において，共通の訓練計画を促進し，また，人の交流を推進すること；
   (j) 世界中のデータ保護監督機関との間で，データ保護の法律及び実務に関する知識及び文書の交換を促進すること。

The Board established by Regulation (EU) 2016/679 shall perform all of the following tasks in

relation to processing within the scope of this Directive:

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;
(b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Directive and issue guidelines, recommendations and best practices in order to encourage consistent application of this Directive;
(c) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 47(1) and (3);
(d) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph for establishing personal data breaches and determining the undue delay referred to in Article 30(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;
(e) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons as referred to in Article 31(1);
(f) review the practical application of the guidelines, recommendations and best practices;
(g) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country, a territory or one or more specified sectors within a third country, or an international organisation, including for the assessment whether such a third country, territory, specified sector, or international organisation no longer ensures an adequate level of protection;
(h) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;
(i) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;
(j) promote the exchange of knowledge and documentation on data protection law and practice with data protection supervisory authorities worldwide.

第 1 副項(g)に関し，欧州委員会は，委員会に対し，第三国の政府との間，当該第三国内の地域もしくは特定の部門との間または国際組織との間のやりとりを含め，必要な全ての文書を提供する。

With regard to point (g) of the first subparagraph, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with the territory or specified sector within that third country, or with the international organisation.

2. 欧州委員会が委員会から助言を求める場合，欧州委員会は，その事柄の緊急性を考慮に入

れた上で，期限を指定できる。

Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. 委員会は，欧州委員会及び第 58 条第 1 項に示す委員会に対し，その意見書，運用指針，勧告及びベストプラクティスを転送し，かつ，それを公表する。

The Board shall forward its opinions, guidelines, recommendations and best practices to the Commission and to the committee referred to in Article 58(1) and make them public.

4. 欧州委員会は，委員会に対し，意見書，運用指針，勧告及びベストプラクティスが委員会から発行された後，欧州委員会が行った活動を連絡する。

The Commission shall inform the Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the Board.

第Ⅷ章 救済，法的責任及び制裁

Chapter VIII Remedies, liability and penalties

第 52 条 監督機関に異議申立てする権利

Article 52 Right to lodge a complaint with a supervisory authority

1. 他の行政上の救済または法務上の救済を妨げることなく，構成国は，彼または彼女と関係する個人データの処理がこの指令によって採択された条項に違反するとそのデータ主体が考えるときは，全てのデータ主体が単一の監督機関に異議を申立てる権利をもつことを定める。

Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.

2. 構成国は，その異議が第 45 条第 1 項により職務権限のある監督機関に申立てられたものではない場合，異議の申立てを受けた監督機関が，職務権限のある監督機関に対し，不適切な遅滞なく，その異議を移送することを定める。

Member States shall provide for the supervisory authority with which the complaint has been lodged to transmit it to the competent supervisory authority, without undue delay if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 45(1). The data subject

shall be informed about the transmission.

3. 構成国は，異議の申立てを受けた監督機関が，そのデータ主体の求めに応じて，更に補助を提供することを定める。

Member States shall provide for the supervisory authority with which the complaint has been lodged to provide further assistance on request of the data subject.

4. データ主体は，職務権限のある監督機関から，第 53 条による法務上の救済の可能性を含め，その異議の進捗状況及び結果の連絡を受ける。

The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 53.

第 53 条 監督機関を相手方とする実効的な法務上の救済の権利

Article 53 Right to an effective judicial remedy against a supervisory authority

1. 他のいかなる行政上の救済または裁判外の救済も妨げることなく，構成国は，自然人または法人に関する監督機関の法律上の拘束力のある決定を不服として，実効的な法務上の救済の自然人または法人の権利を定める。

Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. 他のいかなる行政上の救済または裁判外の救済も妨げることなく，第 45 条第 1 項により職務権限のある監督機関がその異議申立てを取り扱わない場合，または，第 52 条により申立てられた異議の進捗状況もしくは結果をデータ主体に対して 3 か月以内に連絡しない場合，各データ主体は，実効的な法務上の救済の権利をもつ。

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Article 45(1) does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged pursuant to Article 52.

3. 構成国は，その監督機関が設けられている構成国の裁判所において，監督機関を相手方とする訴訟手続が提起されることを定める。

Member States shall provide for proceedings against a supervisory authority to be brought before

the courts of the Member State where the supervisory authority is established.

第 54 条　管理者または処理者を相手方とする実効的な法務上の救済の権利

Article 54 Right to an effective judicial remedy against a controller or processor

第 52 条により監督機関に異議を申立てる権利を含め，利用可能な行政上の救済または裁判外の救済を妨げることなく，構成国は，彼または彼女の個人データのこの指令に従って採択された条項を遵守しない処理の結果として，それらの条項に定める彼もしくは彼女の権利が侵害されたと考えるときは，実効的な法務上の救済のデータ主体の権利を定める。

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.

第 55 条　データ主体の代理者

Article 55 Representation of data subjects

構成国は，構成国の手続法に従い，データ主体が，構成国法に従って適法に組織構成され，公共の利益における制定法上の目的をもち，かつ，データ主体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能動的な非営利の組織，団体または協会に対して，彼または彼女の代わりに異議を申立てること，及び，彼または彼女の代わりに第 52 条，第 53 条及び第 54 条に示す権利を行使することを委任する権利をもつことを定める。

Member States shall, in accordance with Member State procedural law, provide for the data subject to have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 52, 53 and 54 on his or her behalf.

第 56 条　弁償を受ける権利

Article 56 Right to compensation

構成国は，違法な処理業務の結果として，または，この指令によって採択された国内条項に違反する行為の結果として，財産上の損害または非財産上の損害を受けた者が，構成国法に基づき，職務権限のある管理者またはそれ以外の機関から，被った損害の弁償を受ける

権利を定める。

Member States shall provide for any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive to have the right to receive compensation for the damage suffered from the controller or any other authority competent under Member State law.

第 57 条 制裁
Article 57 Penalties

構成国は，この指令によって採択された条項の違反行為に対して適用可能な制裁に関する規定を定め，かつ，その条項が実装されることを確保するために必要となる全ての措置を講ずる。定められる制裁措置は，実効的であり，比例的であり，かつ，抑止力のあるものとする。

Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

第IX章 実装行為
Chapter IX Implementing acts

第 58 条 委員会の手続
Article 58 Committee procedure

1. 欧州委員会は，規則(EU) 2016/679 の第 93 条によって設けられる委員会から補佐を受ける。この委員会は，規則(EU) No 182/2011 の意味における委員会である。

The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. 本項が参照される場合，規則(EU) No 182/2011 の第 5 条が適用される。

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. 本項が参照される場合，規則(EU) No 182/2011 の第 5 条と重畳的に同規則の第 8 条が適用される。

Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in

conjunction with Article 5 thereof, shall apply.

第X章 最終規定
Chapter X Final provisions

第 59 条 枠組み決定 2008/977/JHA の廃止
Article 59 Repeal of Framework Decision 2008/977/JHA

1. 枠組み決定 2008/977/JHA は，2018 年 5 月 6 日をもって廃止される。

   Framework Decision 2008/977/JHA is repealed with effect from 6 May 2018.

2. 第 1 項に示す廃止される決定に対する参照は，この指令に対する参照として解釈される。

   References to the repealed Decision referred to in paragraph 1 shall be construed as references to this Directive.

第 60 条 既に発効している欧州連合の法行為
Article 60 Union legal acts already in force

刑事における法務上の協力及び警察の協力の分野において 2016 年 5 月 6 日以前に発効した法行為であって，構成国間における処理及びこの指令の適用範囲内にある条約によって設けられた情報システムへの構成国の指定された機関によるアクセスを規律する欧州連合の法行為中の個人データの保護に関する個別の条項は，影響を受けないままとする。

The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected.

第 61 条 刑事における法務上の協力及び警察の協力の分野において従前に締結された国際協定との関係
Article 61 Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation

2016 年 5 月 6 日よりも前に構成国によって締結された第三国または国際組織に対する個人データの移転に適用される国際協定であって，かつ，同日よりも前に適用可能なものとして

欧州連合法を遵守する協定は，それが改正され，廃止され，または，廃棄されるまでの間，有効なままとする。

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked.

第 62 条 欧州委員会の報告書

Article 62 Commission reports

1. 2022 年 5 月 6 日までに，かつ，その後は 4 年毎に，欧州委員会は，欧州議会及び理事会に対し，この指令の評価及び見直しに関する報告書を提出する。この報告書は，公表される。

   By 6 May 2022, and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Directive to the European Parliament and to the Council. The reports shall be made public.

2. 第 1 項に示す評価及び見直しの過程において，欧州委員会は，とりわけ，第 36 条第 3 項及び第 39 条によって採択された判定と特に関連する第三国または国際組織に対する個人データの移転に関する第 V 章の適用及びその稼働を吟味する。

   In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 36(3) and Article 39.

3. 第 1 項及び第 2 項の目的のために，欧州委員会は，構成国及び監督機関に対し，情報の提供を求め得る。

   For the purposes of paragraphs 1 and 2, the Commission may request information from Member States and supervisory authorities.

4. 第 1 項及び第 2 項に示す評価及び見直しを遂行する際，欧州委員会は，欧州議会，理事会並びにそれら以外の関連する組織及び情報源の意見及び判断を考慮に入れる。

   In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council and of other relevant bodies or sources.

5. 欧州委員会は，必要があるときは，とりわけ，情報技術における発展を考慮に入れ，かつ，情報社会における進展状態に照らし，この指令を改正するための適切な提案書を提出する。

The Commission shall, if necessary, submit appropriate proposals with a view to amending this Directive, in particular taking account of developments in information technology and in the light of the state of progress in the information society.

6. 2019 年 5 月 6 日までに，欧州委員会は，この指令と整合性させる必要性を評価するため，及び，それが適切なときは，この指令の適用範囲内にある個人データの保護への一貫性のあるアプローチを確保するためのそれらの法行為の改正の提案をする必要性を評価するため，第 60 条に示す法行為を含め，欧州連合によって採択され，第 1 条第 1 項に定める目的のための職務権限のある機関による処理を規律する他の法行為を見直す。

By 6 May 2019, the Commission shall review other legal acts adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60, in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive.

第 63 条 移植

Article 63 Transposition

1. 構成国は，2018 年 5 月 6 日までに，この指令を遵守するために必要となる法律，行政規則及び行政条項を採択し，かつ，公示する。構成国は，欧州委員会に対し，それらの条項の正文を送付する。構成国は，2018 年 5 月 6 日から，それらの条項を適用する。

Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018.

構成国がそれらの条項を採択したときは，それらの条項は，この指令への参照を含めるものとし，または，それらの条項の公示の際にそのような参照を伴うものとする。構成国は，どのようにしてそのような参照が行われるかを決定する。

When Member States adopt those provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. 第 1 項からの特例により，構成国は，不適切な負担を要する場合，2016 年 5 月 6 日以前に設置された自動化された処理システムを 2023 年 5 月 6 日までに第 25 条第 1 項に適合させることを，例外として，定め得る。

By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.

3. 本条第 1 項及び第 2 項からの特例により，構成国は，例外的な状況において，当該特定の自動化された処理システムの運用にとって何らかの重大な困難を生じさせ得る事由がある場合，本条第 2 項に示す期間経過後の指定される期間内に，本条の第 2 項に示す自動化された処理システムを第 25 条 1 項に適合させ得る。関係する構成国は，欧州委員会に対し，それらの重大な困難に関する根拠及び当該特定の自動化された処理システムを第 25 条第 1 項に適合させる指定される期間に関する根拠を通知する。この指定される期間は，いかなる場合においても，2026 年 5 月 6 日よりも遅れるものとしてはならない。

By way of derogation from paragraphs 1 and 2 of this Article, a Member State may, in exceptional circumstances, bring an automated processing system as referred to in paragraph 2 of this Article into conformity with Article 25(1) within a specified period after the period referred to in paragraph 2 of this Article, if it would otherwise cause serious difficulties for the operation of that particular automated processing system. The Member State concerned shall notify the Commission of the grounds for those serious difficulties and the grounds for the specified period within which it shall bring that particular automated processing system into conformity with Article 25(1). The specified period shall in any event not be later than 6 May 2026.

4. 構成国は，欧州委員会に対し，この指令が適用される分野において採択する国内法の主要な条項の正文を送付する。

Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

第 64 条 発効

Article 64 Entry into force

この指令は，EU 官報に公示された翌日に発効する。

This Directive shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

第 65 条 発出
Article 65 Addressees

この指令は，構成国に宛てて発出される。

This Directive is addressed to the Member States.

ブリュッセルにおいて，2016 年 4 月 27 日に行われた。
Done at Brussels, 27 April 2016.

欧州議会として	理事会として
議長 M. SCHULZ	議長 J.A. HENNIS-PLASSCHAERT

2021 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 6 巻第 6 号（通巻第 46 号）（第 2 分冊）
The Law and Information Magazine vol.6 no.6 (consecutive no.46) part 2

2021 年 12 月 5 日発行
発行者　夏井高人
発行所　法と情報研究会（代表 夏井高人）
東京都千代田区神田駿河台 1－1
学校法人明治大学研究棟
（非売品）