EU 各国における個人情報保護制度に関する調査研究報告書

平成 30 年 3 月 29 日

株式会社 IT リサーチ・アート

第１部　総論

第１　公的部門に適用される GDPR について

１　GDPR（一般データ保護規則）とは？

（１）基本権と GDPR との関係

EU においては，個人データの保護が，私生活尊重の権利とは別に EU 基本権憲章において明文で保障されている。EU 基本権憲章第 8 条 1 項では，「何人も自己に関する個人データの保護に対する権利を有する」と規定されており，連合の機能に関する条約第 16 条 1 項においても同様の規定がある。また，憲章において，個人データ保護の権利の遵守については，「独立の機関による監督を受けるものとする」ことが規定され，データ保護監督機関（Data Protection Authority）が置かれている（8 条 3 項，機能条約 16 条 2 項）。このような EU の個人データの保護については，EU 基本権憲章第 7 条及び欧州人権条約第 8 条で保障される私生活尊重の権利を補強する基本的権利としての性格を有している。

このように，EU のデータ保護法制は，基本権憲章の規定を受け，人権として個人データを保護するという思想が根付いている。EU ではデータ保護が基本権としての人権問題であると位置付けられていることから，EU データ保護指令を所管する「データ保護課（data protection unit）」は，欧州委員会の司法総局にあり，「基本権及び連合市民権（Fundamental rights and Union citizenship）」局の中に位置付けられている。また，EU データ保護に関連する事項の審議は，欧州議会の中で人権問題を扱う「市民的自由・司法・内務委員会（Civil Liberties, Justice and Home Affairs）」において行われてきた。

EU データ保護規則提案は，EU 加盟国間における立法の違いを克服するため，その制定により自動的に各国の国内法制度の一部となり，国内立法を必要せず直接適用される「規則（regulation）」[1]として提案された。加盟国は規則を不完全に適用したり，規則の規定を選別する権限を有していない。個人データ保護に関するこの統一的な適用により，企業にとって毎年 23 億ユーロの運用上の負担が削減されることが示された。

また，EU データ保護指令は前文 42 項目及び本文 34 条からなるのに対し，GDPR は前文 173 項及び本文 99 条から構成されており，前文と条文の数が増加した。GDPR の主な概要は次のとおりである。GDPR は EU 加盟国 28 か国におけるミニマムスタンダードを規定しており，加盟国法において追加の要件が規定されることがある。

---

[1] 規則は一般適用性を有する。規則はそのすべての要素について義務的であり，かつ，すべての加盟国において直接適用可能である（機能条約 288 条 2 項）。直接適用可能であるとは，「規則」を国内法に編入または置換するための国内立法を必要としないことを意味する。Zerbone 事件（1978 年）判決によれば，加盟国は「規則」の「[EU]的性格およびそれより生じる帰結が関係者から隠ぺいされるような措置を採択してはならず，また，立法権を有する国内機関にそのような措置を採択することを認めてはならない」庄司克宏『新 EU 法基礎篇』（岩波書店，2013）210－211 頁，参照。

GDPR の概要（第 11 章，99 か条，前文 173 項からなる）

1 総則	目的，範囲，定義
2 原則	処理の原則，処理の適法性，同意の条件，特別の処理類型
3 データ主体の権利	透明性，アクセス権，訂正権，削除権（忘れられる権利），データポータビリティ権，自動処理（プロファイリング）
4 管理者・処理者	一般的義務，データ保護バイデザイン，共同管理者，代理人，処理，処理活動の記録，安全管理，データ侵害通知，データ保護影響評価，事前協議，データ保護責任者の配置，行動規範，認証
5 個人データ移転	十分性決定，適切な保護措置，拘束的企業準則，特例，国際協力
6 独立監督機関	独立性，設置規則，任務，権限
7 協力・一貫性	監督機関の協力，相互支援，一貫性の体制，欧州データ保護評議会
8 救済・責任・罰則	苦情申立権，司法救済権，補償権，制裁金
9 特別の処理状況	表現の自由，公的記録へのアクセス，国の番号制度，雇用管理，統計歴史研究
10 委任行為	委任，手続
11 最終条項	指令廃止，電子プライバシー指令との関係，施行

（2）GDPR の日本への影響

GDPR がもたらす日本への影響はどのようなものが想定されうるだろうか。第 29 条作業部会がアジア太平洋プライバシー機関（Asia Pacific Privacy Authority）の構成員（日本は個人情報保護委員会）向けに示したファクトシートがある。GDPR の一般的な説明として，2018 年 5 月 25 日に適用され，EU 域内におけるデータ保護法の調和を図ること，そして EU 域内に設置された管理者と処理者および EU 市民に対して商品またはサービスを提供している管理者と処理者に適用されることが示されている。このファクトシートの中で示された鍵となるメッセージを基にその影響について以下説明する[2]。

① GDPR の実体的範囲（2 条）

GDPR は個人データの処理に適用される。個人データは識別された，または識別することができる自然人に関するいかなる情報として定義される。個人データには，IP アドレス，電子メールアドレス，または電話番号も含まれる。処理業務には，他にもあるが，データの収集，利用および開示が含まれる。

GDPR は，個人データの特別類型の処理への追加的保護についても規定している。特別類型には，人種，もしくは民族出自，政治的意見，信条もしくは哲学上の信念，労働組合員を明らかにする個人データ，自然人を特別に識別する目的の遺伝・生体のデータを明らかに

[2] Article 29 Data Protection Working Party, EU General Data Protection Regulation: General Information Document, 12 February 2018. 以下，本節はこのファクトシートの日本語訳である。

する個人データ，健康に関するデータまたは自然人の性生活や性的指向に関するデータが含まれる。

加盟国は，遺伝・生体データや健康に関するデータに関して，制限を含め追加の条件を導入することができる。

② GDPR の地理的範囲（3 条）

GDPR は EU 域内に設置された管理者と処理者に適用される。または，商品やサービスを提供することで EU における個人をターゲットにしているか(支払いの有無は関係ない)，もしくは EU 域内における個人の行動を監視している EU 域外に設置されている管理者と処理者にも適用される。商品やサービスの注文の可能性があり，一つまたは複数の加盟国において用いられている言語や貨幣の利用している場合や，EU 域内にいる顧客や利用者に言及している場合，管理者が EU 域内のデータ主体に商品やサービスを提供しようとしていることが明白になる。

EU に設置されていないデータ管理者と処理者が，その活動が GDPR の適用範囲内にある場合，「一般的に EU 加盟国に設置された代理人を任命しなければならない」（一定の例外がある)。代理人は，データ保護監督機関の連絡窓口であり，データ処理に関連するあらゆる問題に関する EU に在住する個人である（27 条)。

【例】日本のウェブショップがユーロでの支払いとともに英語がオンラインで利用可能となっており，製品を提供している。EU 域内の個人から一日に複数の注文の処理を行い，製品を発送している。この場合，GDPR を遵守しなければならない。

③ 処理に関する基本原則（5 条）

GDPR によれば，個人データは「適法性・公平性および透明性の原則」に従い処理されなければならない。さらに，個人データは特定され，明示されかつ正当な目的のために収集されなければならず，これらの目的と両立しえない方法で追加処理されてはならない（「目的制限の原則」)。管理者または処理者は「データ最小限化の原則」を尊重することを確かなものとしなければならず，個人データは，処理される目的との関係において必要なものにとって適切で，関連性があり， かつ限定されなければならない。個人データは「正確」でなければならず，必要に応じ，最新の状態にしておかなければならない。また，「説明責任の原則」も基本原則の一つとして認識されている。最後に，保存制限，完全性および秘密保持の原則が尊重されなければならない。そのため，個人データは目的にとって必要以上データ主体の識別を可能としない形式で保存されなければならない。また，個人データの適切な安全管理を確保する方法で処理されなければならない。

④ 処理の適法性（6 条）

GDPR の下では，個人データの処理は次のいずれかの条件を満たした場合にのみ適法となる。

・データ主体が処理に同意を与えた場合
・データ主体が当事者である処理が契約の締結に必要な場合，または契約締結前にデータ主体の要請の措置を採るために必要な場合
・処理が管理者に適用される法的義務を遵守するために必要な場合
・処理がデータ主体または別の自然人の不可欠な利益を保護するために必要な場合
・処理が公共の利益を実施する任務の遂行のために必要な場合
・処理が管理者または第三者が追求する正当な利益の目的にとって必要な場合，ただし，特にデータ主体が児童であり，個人データ保護を必要とするデータ主体の利益，または基本権と自由が正当な利益を上回る場合は除く。

特別で厳格な要件が「データの特別類型」の処理に関しては示されている（9 条）。

⑤　同意（4 条，7 条，8 条）

GDPR は同意の概念を明確化するためにいくつかの条文を設けている。

GDPR の下では，第 29 条作業部会の同意の要件の意見を反映し，同意は，明確で積極的な行為による声明は処理への合意を示す，自由に与えられ，特定の，情報を受けた，かつデータ主体の要望の明確な意思表示でなければならない。

同意の要請は，分かりやすく容易にアクセスできる方法で，明確かつ簡易な言葉を用いて，他の事項とは明確に区別される方法で提示されなければならない。データ主体は自らの同意をいつでも容易に撤回することができなければならず，撤回の権利はあらかじめ通知されていなければならない。

特別の要件が情報社会サービスのための児童の同意との関係において適用される。もしも 16 歳以下の個人が情報社会サービスを利用したいと希望した場合，同意は対象児童の保護者または対象児童の親権者から同意を得なければならない。しかし，加盟国は 13 歳を下回らない年齢でこの年齢を下げる国内法を導入することができる。

⑥　個人の権利（12－23 条）

GDPR は個人の権利を維持し，様々なところで強化し，さらに発展させている（情報，アクセス，訂正，異議申立，削除，制限，忘れられる権利，データポータビリティ権）。

・「情報への権利」は，管理者が個人に対して個人データの処理に関する一定の情報を無料で提供することを必要としている（14 条に例外が規定されている）。この情報は，正確で，透明で，分かりやすく容易にアクセスできる形式で，明確かつ簡易な言葉を用いなければならない。データ管理者は，容易に見ることができ，意義のある処理の概要を与えるため，標準化されたアイコン（利用者にわかりやすい情報提供するためのフォーマットであり，今後欧州委員会が策定予定）を用いてこの情報を個人に提供することができる。
・「忘れられる権利」は，削除権としても知られており，両方の権利はデータを削除して

もらう権利であり，一定の状況の下リスト化されない権利を含む。個人は一定の状況の下では管理者に対して自らのデータを消去することを要求する権利を有している。この権利には，情報が収集された目的にとってもはや必要がなくなった場合や個人が同意を撤回した場合，またデータの処理の法的根拠がない場合が含まれている。

- 「処理の制限権」は，一定の状況の下で適用される。たとえば，個人データから申し立てられた正確性を管理者が証明するまでの期間，または法的請求などのためデータ主体には必要とされるが，管理者が処理の目的にとって個人データをもはや必要としないときが含まれる。
- 「データポータビリティ権」は，自らが管理者に提供した個人データを体系的で一般に用いられている機械で読み込み可能な形式で受け取り，かつ妨げなく別の管理者にデータを送信する個人の権利をいう。ポータビリティ権は，処理が個人の同意に基づくか，または契約の締結のためである場合，あるいは処理が自動的手段で実施される場合，個人が管理者に提供した個人データにのみ適用される。この新たなデータポータビリティ権は，削除権やアクセス権の存在を損ねることなし存在するものである。

これらの権利については GDPR23 条に基づき制限がある。たとえば，民主的社会における国土の安全，防衛，または公共の安全の保護にとって必要な場合などである。

⑦　管理者の説明責任の義務（5 条，25 条，30 条，35－43 条）

説明責任の原則（5 条 2 項）によれば，管理者（処理の目的と手段を決める主体）は GDPR を遵守していることを確保し，かつこの遵守を論証することができるようにしなければならない。管理者はデータ保護の政策を含む一般に適切な技術的組織的措置を講じなければならない。この措置がどのように実施されるべきかを評価する際，管理者は処理の性質，範囲，文脈および目的とともに個人の権利と自由へのリスクを考慮しなければならない。

GDPR は，管理者に説明責任を論証するための一連のツールを規定し，そのいくつかは強制的に整備しなければならない。たとえば，データ保護責任者（DPO）の配置，データ保護影響評価（DPIA）の実施，プライバシーバイデザインとプライバシーバイデフォルトの原則の尊重は義務である。管理者は説明責任原則の遵守を論証するため，行動規範，認証の体制といった他のツールを用いることを選択することができる。

特別のツールの更なる情報については，第 29 条作業部会のニュースルームにおいて特定のガイドラインを参照することができる。

⑧　処理者の義務（28 条）

GDPR は，特に安全管理措置と国際データ移転に関して，管理者の要件とは別の法的地位にとして処理者に直接適用される新たな要件を導入している。

処理者は，管理者に明示的な保証が及ぶのと同様に，期待された保証を提供しなければならない。管理者は，処理が GDPR の要件を満たすことを確保するための適切な技術的組織

的措置を実施しなければならない。処理者は安全管理，DPIA とデータ侵害通知の事項において管理者を支援しなければならない。処理者は，管理者の処理の指示が GDPR または EU 法や加盟国法の規定に違反する恐れがある場合には管理者に変更を求めなければならない。

処理者による処理は，管理者から処理者に対して拘束力を持つ契約または他の有効な法的行為によって統制されなければならない。契約期間等の契約や他の法的行為における基本情報に加え，GDPR は，たとえば，処理者は管理者からの文書による指示に従いデータ処理を行うことができる，また処理者は管理者の承認なしに別の処理者に委託することができないという事項を含む特別の条項を列挙している。

⑨　データ侵害通知（33 条，34 条）

GDPR の下では，データ保護監督機関（DPA）へのデータ侵害通知は義務である。ただし，データ侵害が個人の権利と自由への影響が生じない場合はこの限りではない。管理者は，遅滞なく，また可能な場合には，侵害を知りえてから 72 時間以内に DPA にその通知をしなければならない。

⑩　国際移転（44－49 条）

GDPR に基づき，EU 域内において付与されている保護水準と「本質的に同等」であることを意味する「十分なデータ保護の水準」を満たしている個人データは EU 域外の第三国または国際機関へ移転することができる。

欧州委員会の十分性の決定が与えられていない第三国または国際機関への個人データの移転は，適切な特別の措置が施されている場合に行うことができる。この措置は，標準的データ保護条項，拘束的企業準則，また新たなツールとして承認された行動規範や認証等のいくつかの利用可能なツールを通して用いることができる。

十分性の決定がなく，かつ個人データの移転に関する適切な措置がない場合，移転に伴うリスクに関するすべての必要な情報を受けた後に予定される移転に足して個人が明示の同意を与えた場合，または移転が不可欠な正当な利益の目的にとって必要な場合などの限定された状況においてのみ行うことができる。

別の第三国への再移転はこれらの要件の対象となる。

【例】EU における支社が，労働者に関する情報を保存するため親会社に属するインドに集中管理される人事システムを用いている。インドにある親会社の支社として EU からのデータ移転を形成するために適切な措置が講じられる必要がある。

⑪　監督，協力，救済（50 条，83 条）

一般的に，GDPR は独立性の要件と DPR の役割を強化している。これらの要件は，広範囲にわたる協議，調査および是正権限から，行政上の制裁金に至るまで恩恵をもたらしている。

GDPR は EU において今後見られることになる行政上の制裁金のアプローチと水準を極めて厳格にし，統一化している。

DPA は 2000 万ユーロまたは全世界の総売上 4%以下の行政上の制裁金を科す権限を有することになる。

GDPR は EU 域内において DPA が集団行動するための新たな手続を導入している。また，国内レベルにおける集団行動を導入したい加盟国の裁判所の前で同様の手続を予見する可能性についても GDPR は規定している。

GDPR は欧州委員会と DPA に対して効果的な適用のための協力を奨励している。第 29 条作業部会の構成員は，この協力を策定するための可能な選択肢を模索しており，この考えがまとまり次第，APPA の構成員からの提案を受け入れるためにも APPA のカウンターパートとともに意見を議論することになるであろう。

⑫ 欧州データ保護評議会（EDPB）（64 条，65 条，66 条，68 条）

第 29 条作業部会は，EU の国の監督機関，欧州データ保護監督官（EDPS）および欧州委員会から構成され，95/46 指令に基づき設置された。第 29 条作業部会は，欧州データ保護評議会（EDPB）に代わることとなる。

EDPB は，多くの詳細な任務のリストが与えられているが，初期の役割は EU 域内における GDPR の一貫した適用に寄与することである。EDPB は国の監督機関の間の紛争解決やリスクの高い処理のリスト，行動規範や認証機関の認定基準等の特定の問題に関する意見の公表など法人格と広範な権限を備える EU の機関としての地位を有することとなる。EDPS はガイドライン, 勧告及びベストプラクティスの公表についても責任を有している。

EDPS は議長により代表される。EDPB は，任務の中で議長と評議会を支える事務局を有する。

⑬ One-Stop-Shop

GDPR は，EU の複数の国における越境処理を行う主体のための”one stop shop”の体制を通じて，協力と一貫性に関する新たな方法を規定している。

越境処理は，管理者や処理者が複数の加盟国において設置を通じて業務を行っている場合，または単一の設置があり実質的効果をもたらす処理業務や複数の加盟国におけるデータ主体に実質的な影響を及ぼす可能性のある処理業務を行う単一の設置がある場合に存在する。

端的に述べると，「主たる監督機関」は，所与の越境処理との関係における管理者と処理者の連絡窓口であり，たとえば主たる監督機関が越境処理に関する調査を「対象となる」監督機関と共に調整する場合などの第一次的責任を有することとなる。

しかし，各 DPA は GDPR の国内の苦情や違反を扱う権限を有している。

GDPR の協力と一貫性の体制は EU 域内に単一または複数設置されている管理者にのみ

適用される。もしも企業が EU 域内に設置されていなければ，加盟国における代理人の存在のみでは one-stop-shop の体制が用いられることはない。このことは，EU 域内におけるいかなる拠点もおかない管理者は，代理人を通じて，業務を行っているそれぞれの加盟国の監督機関により対処されることとなる。

主たる監督機関に関する更なる情報については，第 29 条作業部会のガイドラインを参照されたい。

２　公的部門への影響

（１）公的部門と民間部門との区別

GDPR は，公的部門と民間部門に適用される包括的な個人データ保護の法制度である。そのため，一般的に公的部門にのみ特有の事項は条文で明示的に規定されていない限り，公的部門と民間部門との区別はない。管理者や処理者にも公的機関が含まれている（GDPR 第 4 条 7 号・8 号）

なお，EU の行政機関に対して適用される規則 45/2001 により，独立した機関である欧州データ保護監督官（European Data Protection Supervisor（EDPS））が監督にあたっている。監督官は Giovanni Buttarelli（2009 年～2014 年まで EDPS 副監督官，1997 年~2009 年までイタリア事務局長，ローマ・ラ・サピエンツァ大学卒業，1957 年生まれ），副監督官は Wojciech Wiewiórowski（2010 年から 2014 年までポーランドコミッショナー，グダニスク大学講師・助教，グダニスク大学卒業，1971 年生まれ）がそれぞれ 2014 年から 5 年任期で職務に当たっている。EDPS の具体的な任務は，EU の行政機関が個人データを処理する際の個人データとプライバシーの保護の監視，EU 行政機関に対する個人データ処理に関する助言，個人データ保護に影響を及ぼす新たな技術の監視，EU 司法裁判所における専門的意見の提供のための介入，国の監督機関との協力である。なお，GDPR 適用後は，EDPS に欧州データ保護評議会（EDPB）の事務局が置かれることとなる。

加盟国のこれまでの運用を見る限りにおいて，公的部門における特徴的な運用として次のようなものを挙げることができる。

第 1 に，公的機関への自らの個人データについては，間接アクセス（indirect access）という方式が採られることもある。特に防衛，外交，警察の分野においては，データ主体本人が直接開示するのではなく，データ保護監督機関に開示をしてもらう方法であり，特にフランス CNIL が毎年多くの件数このような間接アクセスをおこなっている。

第 2 に，データ保護責任者の配置やデータ保護影響評価の実施といった個人データ処理のライフサイクルに関する義務である。一般に，民間の事業者と異なり，公的機関にはデータ保護責任者やデータ保護影響評価の実施が義務化されていることがある。GDPR では，公的機関による処理にはデータ保護責任者の配置が義務化されている（第 37 条）。さらに，公的機関の任務に関する処理については，監督機関との事前協議が必要であることを加盟国に喚起している（前文 93 項）。そして，公的機関によるデータ主体の体系的な監視を伴う

処理業務には，データ保護影響評価が必要となる（前文 97 項）。特にまた，データ主体からの同意の取得においても，特に公的機関の場合には同意が「自由に与えられる」べきことが示されている（前文 43 項）。

第 3 に，制裁金についてであるが，公的機関への制裁金は国庫などの税金から支出されることになるため，適切な運用であるかどうかについて議論がある。GDPR の適用により，民間事業者には高額な制裁金が科される一方で，公的機関に対して制裁金が科されえないとすると，データ保護違反への抑止が不十分ではないかといった議論がある。制裁金に代わり，禁固刑や懲役刑を科すことも想定されうるが，EU においてデータ補侵害を理由としたそのような運用はみられない[3]。なお，加盟国においては，イギリスが国及び地方公共団体の公的機関に制裁金を科す多くの事例がみられる。

（2）公的部門に関連する事項

GDPR は公的部門と民間部門の両方を対象としているが，具体的に公的部門に関連する事項も見られる。特にオーブンデータや公的部門における情報の再利用や刑事司法分野における個人データの処理に関して，公的部門特有の規律が必要となる場合がある。特にオープンデータとの関係においては，比例原則，データ処理の最小限化，そしてデータの質（正確性）に関する原則を考慮に入れる必要がある。

GDPR では，公的部門への直接の言及は前文 154 項での「公的情報の再利用」の箇所のみである。これに関連して，GDPR 第 86 条では，公文書の処理と市民のアクセスに関する規定があり，「公的機関もしくは公的組織または公共の利益において実施される任務を遂行する民間組織が保有する公文書における個人データは，市民の公文書へのアクセスと本規則に従い個人データの保護への権利との調整を行うため，公的機関または組織に適用される EU 法または加盟国法に従い機関または組織に開示することができる」と規定されている。

EU 司法裁判所は，GDPR にも規定されている情報公開との関係について，次の重要な判決を下している。一つは，Bavarian Lager 判決（2010 年）[4]である。EU 司法裁判所は，対象となる記録に個人データが含まれていれば，情報公開規則の例外規定よりもデータ保護規則の規定が全面的に適用されると判示した。本件では，欧州委員会が保有する個人データを含む文書の開示が求められていたが，開示を求めた企業が個人データを利用するための正当な目的を明示していないため拒否した。ここでは，文書開示をすることが「個人のプライバシーと正確性の保護」の例外規定に該当するか否かが問題となった。司法裁判所は，この情報公開の規則の規定が，単に欧州人権裁判所の私生活尊重の権利の判例法のみならず，データ保護規則における個人データ保護の権利も考慮して解釈されるべきであることを示した。このように，情報公開請求におけるプライバシーの例外規定は，私生活尊重の権

[3] Peter Blum, The Public Sector and the Forthcoming Data Protection Regulation, *European Data Protection Law Review*, vol. 1. issue 1(2015) p. 38 n16.
[4] C-28/08P, European Commission v. The Bavarian Lager Co. Ltd. ECLI:EU:C:2010:378.

利と個人データ保護の権利の法理に基づき理解されるべきこととなることが明らかになった。

もう一つは，Volker 判決（2010 年）[5]である。ドイツ連邦機関が農業の補助金受給者の個人データを公表していた事例で，法と比例原則に基づき公表される必要があるが，公表の期間や受給金額などの区別なく公表することは自然人の私生活への干渉となるため公開を定めた規定は無効とされた。

また，個人データの移転について，GDPR では公的部門における例外を設けている。法律で定められた公的任務の遂行のため，公的機関が個人データを開示する場合（たとえば，税関，マネーロンダリング対策の金融部署等），GDPR では個人データの「受領者」とはみなされない（前文 31 項）。そのため，EU 法または加盟国に基づき，公的機関が公的任務の遂行のための個人データの移転については，移転に関する制限が適用されないこととなる。

なお，GDPR では，警察司法の分野においては，適用されないことが明文化されている（2 条 2 項）。これは，警察司法分野に係る指令（2016/680/EU）が別途存在するためである。第 29 条作業部会では，指令に基づく公的部門に関連する事項として，これまで次の項目について意見を公表してきた。

・公的部門における透明性の目的のための個人データの公表に関する意見（2016 年）[6]
・オープンデータと公的部門の情報の再利用に関する意見（2013 年）[7]
・公的部門の情報の再利用と個人データ保護に関する意見（2003 年）[8]
・公的部門の情報と個人データ保護に関する意見（1999 年）[9]

これに関連して，刑事司法分野に関連する意見や勧告としては次のようなものがある。

・法執行分野における必要性及び比例性の概念の適用とデータ保護に関する意見（2014 年）[10]
・法執行目的の乗客氏名記録の利用に係る 2007 年 11 月 6 日付欧州委員会提示による理事会枠組み決定に対する提案に関する共同意見（2007 年，警察司法に関する作業部会との共同意見）[11]
・法執行，関税およびその他の安全に関する機関の業務における技術の探知に係るグリー

[5] Joined Cases C-92/09 andC-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, ECLI:EU:C:2010:662.
[6] Article 29 Data Protection Working Party, Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector, 8 June 2016.
[7] Article 29 Data Protection Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse, 5 June 2013.
[8] Article 29 Data Protection Working Party, Opinion 7/2003 on the re-use of public sector information and the protection of personal data, 12 December 2003.
[9] Article 29 Data Protection Working Party, Opinion on public sector information and the protection of personal data, 3 May 1999.
[10] Article 29 Data Protection Working Party, Opinion 01/2014 on the Application of necessity and proportionality concepts and data protection within the law enforcement sector, 27 February 2014.
[11] Article 29 Data Protection Working Party, Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, 5 December 2007.

ンペーパーに関する意見（2007 年）[12]

・法執行目的のインターネットサービス提供者によるトラフィックデータの保全に関する勧告（1999 年）[13]

3　本調査の対象国における特徴

EU データ保護指令の下では，加盟国における法の制度と運用におけるバラつきがしばしば指摘されたところである。指令に基づき国内法化される際に，目的外利用や本人関与の仕組みなどの条項には大きな違いは見られないものの，特に救済措置や法執行については依然として加盟国における差異を看守することができる。具体的には，「英国，アイルランドよりもドイツ，フランスの規制の方が厳しい」[14]という評価があるとおり，EU 加盟国の中でもドイツとフランスは厳格な法制度と運用を行ってきた。下記に，加盟国間における異同が明らかになりそうな項目についてまとめてみた。

（1）制定の経緯及び時期

ヨーロッパのデータ保護法制はドイツとフランスが牽引してきたことは周知のとおりであるが，法制化においても顕著な違いがみられる。たとえば，データ保護法が整備された時機を見ると，ドイツ 1977 年，フランス 1978 年であり，OECD ガイドラインが採択された 1980 年より前に国レベルの法律が制定されていた。これに対し，ベルギー1992 年，アイルランド 1988 年，イタリア 1996 年，ポーランド 1997 年はいずれも EU データ保護指令案が公表された 1990 年前後になっている。

そのため，これらの加盟国におけるデータ保護法制の背景は異なり，ドイツやフランスは自国における過去の個人情報の乱用に関する反省の上に，具体的にはドイツではナチスがフランスではサファリプロジェクトがそれぞれ大きな要因となり，個人データを保護するための法律が整備されてきた。これに対し，ベルギー，アイルランド，イタリア，ポーランドはむしろ EU データ保護指令が法整備の契機になったものと考えることができる。

（2）救済措置の仕組み

救済の仕組みについては，加盟国の多くの国にみられるように，我が国における助言，勧告，命令といった権限が存在する。アイルランドはこれらの権限に基本的にとどまる。これに対して，制裁金を科す仕組みが担保されている加盟国として，フランス，イタリア，イギリスがあり，データ主体の申立てを受け付けた後，制裁金を伴う直接的かつ効果的に救済を

---

[12] Article 29 Data Protection Working Party, Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities, 9 January 2007.

[13] Article 29 Data Protection Working Party, Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, 7 September 1999.

[14] 藤原静雄「EU の個人情報保護法制の動向」園部逸夫・藤原静雄編『個人情報保護法の解説〔第二次改訂版〕』（ぎょうせい・2018）453 頁。

行う仕組みが存在する。

また，ポーランドやベルギーでは，裁判所を通じて損害賠償等の責任を負わせる仕組みがある。

さらに，GDPR ではいわゆる消費者団体のような組織に苦情申立を肩代わりする規定（80 条 1 項）[15]が置かれ，ドイツではすでに個人データ侵害に対する集団訴訟制度が整備されている。フランスでも同様の制度がデジタル共和国法により改正された消費者法の枠組みの中で運用されることとなる。

（3）監督機関の組織と執行状況

監督機関の規模は，イギリス情報コミッショナーには 422 人（情報公開担当を含む），次いでフランス 195 人である。これに対して，ベルギーやポーランドにおけるデータ保護の職員数は数十名程度の小規模である。もちろん職員数は，加盟国の人口が異なることや，ドイツの連邦制国家のように一律に比較することは困難である。しばしばし指摘されてきたことは，アイルランドには税制面からアメリカの大規模企業が拠点を置くことが多く，2013 年時点では 30 名に満たない職員がこれらの大企業の取り締まりに当たることは困難であると言われてきた。緩やかなデータ保護法制と執行はかえってこれらの大企業が規制逃れをするための「フォーラムショッピング」の場となっていたという指摘もある [16]。そのため，アイルランドでは，わずか 3 年で 85 名に職員を増やすとともに予算の手当てがなされている。

対象国の執行面について比較すると，フランス，ドイツの州レベル，そしてイギリスでは頻繁に制裁金を伴う執行がみられる。フランスやイギリスのように刑事訴追の手続を開始する権限（検察庁への報告を含む）を有する国もあり，また実際刑事手続が開始された事件も存在する。また，執行面については，GDPR を控えて，これまで制裁金を積極的に科してこなかったイタリアが 2017 年以降，データ移転の違反に関する事例で 5 社に対して 110 万ユーロを科した事例 [17]，またダイレクトマーケティング違反で 84 万ユーロの制裁金をそれぞれ科した事例がある [18]。

これに対して，ベルギーでは執行権限がなく，またこれまで鉄道会社による顧客データの

---

[15] 「データ主体は，加盟国法に従い適切に構成され，公益性を有する立法目的を有し，かつ個人データ保護に関連してデータ主体の権利及び自由の保護の分野で活動を行なっている非営利の機関，組織または団体に対し，自らに代わり苦情を申し立て，自らに代わり 77 条から 79 条にいう権利を行使し，かつ加盟国法により規定された場合には自らの代わりに 82 条にいう賠償を請求する権利を行使することを要求する権利を有する」。

[16] Alexander Dix, The International Working Group on Data Protection in Telecommunications: Contribution to Transnational Privacy Enforcement, in Enforcing Privacy, eds by David Wright & Paul De Hert (Springer, 2016) p. 190

[17] DataGuidance, Italy: €11M fines to money transfer enterprises reflect Garante's "major concern", 16 March 2017 (Garante per la protezione dei dati personali, Garante privacy, 11 mln di multa a cinque società per uso illecito di dati, 10 marzo 2017).

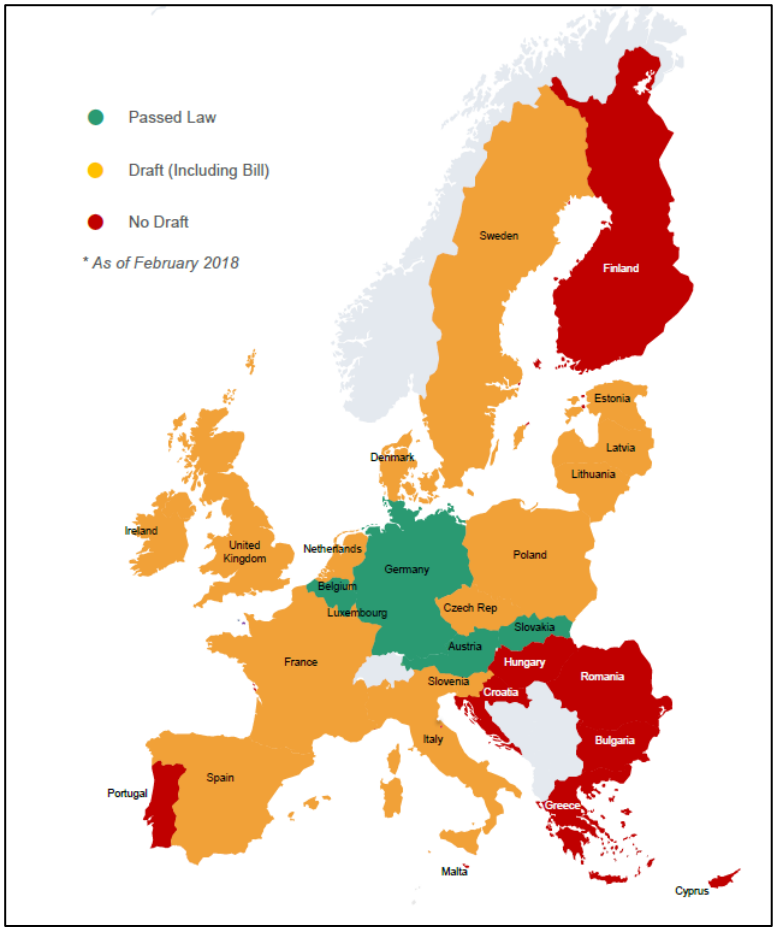
[18] DataGuidance, Italy: Garante’s penalty to Telecom Italia for unsolicited marketing calls ”one of highest ever”, DataGuidance, 15 February 2018（Garante privacy, 840mila euro di sanzione a Telecom per telefonate promozionali senza consenso, 7 febbraio 2018）。

漏えい事件が明らかになっても「吠えない犬」としてのデータ保護機関への不満があったことも事実である[19]。また，ドイツは連邦コミッショナーに制裁権限がなかったことから，州のデータ保護監督機関が制裁を科してきた国もある。このように，データ保護指令に下での，加盟国間において法執行の違いは顕著であったと言うことができる。

（4）GDPR の準備状況

GDPR の準備状況は加盟国において差がみられる。GDPR においては，加盟国法において対処するべき事項が定められている（たとえば，いわゆるセンシティブデータの類型に関する事項，報道等による表現の自由との調整に関する事項，未成年者の年齢要件に関する事項，データ保護責任者の配置の要件に関する事項）。加盟国の中で最も早く GDPR 実施法を整備したのが，2017 年 7 月に実施法を成立させたドイツである。また，オーストリア，スロバキア，ベルギーがそれに続き，実施法を成立させている。

2018 年 2 月現在，弁護士が加盟国の実施法の整備状況をまとめた図は右のとおりとなっている（緑色：実施法成立済み，黄色：草案段階（実施法案を含む），赤色：草案未公表）。



図：Latham & Watkins, The General Data Protection Regulation (GDPR) National Implementation Tracker より

[19] Commission de la protection de la vie privée, Recommandation n° 01/2013 du 21 janvier 2013.

第２　EU 主要国における個人情報保護法制の概要

国名	主要な法律の名称（GDPR 施行法）	制定年月	適用対象機関	保護対象データの範囲	目的外利用の状況	本人関与の仕組	救済措置の仕組	罰則	監督機関の権限
ベルギー	1992 年 12 月 8 日の個人データの処理に関するプライバシー保護法	1992 年 12 月 8 日	公的機関	識別されたまたは識別可能な自然人に関する情報をいう。	法令に基づき，安全保障部局，警察，欧州失踪・被性的搾取児童センター等が利用する場合	アクセス，訂正請求権，異議申立権等	15 条の 2 は，法違反による損害について管理者に損害賠償義務を負わせている	（39 条）：100～10 万ユーロの罰金。公開や同意の強要など	プライバシー保護委員会
ドイツ	連邦データ保護法（新連邦データ保護法 2017 年 5 月成立）	1977 年 2 月	連邦の公的機関（一部州の公的機関）	GDPR の定義	法律の規定がある場合，データ主体が同意した場合，刑事罰または行政罰の訴追の場合等	GDPR の規定に従う，ダイレクトマーケティングにおけるダブル・オプトインの推奨	行政裁判所による救済，データ移転違反の場合は，監督機関から裁判所への救済申立	公的機関による自動処理によりデータ主体に害悪を生じさせた場合 €130,000 以内の賠償責任	連邦データ保護情報公開コミッショナー（別に州の監督機関がある）
フランス	情報処理，情報ファイル及び自由に関する 1978 年 1 月 6 日の法律第 78-17 号（GDPR 施行法案 2017 年 12 月提出）	1978 年 1 月	行政機関（大統領府及び内閣は行政機関に含まれない）	直接的または間接的に識別されたまたは識別することが可能な自然人に関する情報	個別法に基づく，租税機関，社会福祉機関，司法・検察・警察に関わる機関，執行官，またはその他の行政（例えば，高齢者連帯手当）における利用	異議申立，アクセス，訂正，消去等の権利，センシティブデータ処理の同意	違反行為への警告，処理の中断または停止の決定	€150,000 以内金銭的制裁（5 年以内に違反が繰り返された場合は，300,000 ユーロ以内の制裁金）	情報処理及び自由に関する全国委員会

国名	主要な法律の名称（GDPR施行法）	制定年月	適用対象機関	保護対象データの範囲	目的外利用の状況	本人関与の仕組	救済措置の仕組	罰則	監督機関の権限
アイルランド	2003年データ保護法／データ保護法一般枠組法案（2017年5月12日提出）	2003年4月成立 同年7月1日施行	公的部門および民間部門を問わない	そのデータから，またはデータコントローラーが保有する他の情報に関連するデータから，識別されうる生存する個人（a living individual）に関連するデータ	関連する同意のもと，法によって定められた他の合法的根拠	保有目的および保有者をしらされる権利，個人データの存在を確認する権利，アクセスの権利，個人データの訂正および削除に関する権利	情報通知，執行通知	刑事罰	データ保護コミッショナー（An Coimisineir Cosanta Sonrai/Data Protection Commissioner）
イタリア	個人データの取扱に関する個人およびその他の主体の保護に関する法(no.675/1996)	1996年12月施行 1997年5月8日	公的部門および民間部門を問わない（ただし，データ保護法に特定の規定が多数ある）	自然人に関連する，個人識別番号を含む他の情報を参照することによって，個人を識別し，または，識別しうる情報すべて（現行法）	公的部門の目的を行うのに必要な限りでのみ取り扱うこととされる一方で，具体的な取扱に関しては，公的団体は，この法典における前提事項および限界に限定され，法及び規則と，データの特性の配慮によって限定されること	個人データへのアクセス権その他の権利（確認の権利，最新化・修正・統合，消去・匿名化・ブロック，異議権	行政的救済（データ取扱停止・禁止・必要な手段の命令），非司法的救済（部分的・全面的データ利用停止命令等） なお，民事損害賠償制度あり	行政罰／刑事制裁あり	個人データ保護官（Garante per la protezione dei dati personali）

国名	主要な法律の名称（GDPR施行法）	制定年月	適用対象機関	保護対象データの範囲	目的外利用の状況	本人関与の仕組	救済措置の仕組	罰則	監督機関の権限
ポーランド	データ保護法（PDPA）	1997年8月29日。ポーランド共和国憲法（1997年4月2日）が個人情報保護の権利等を保護（51条）	国家行政機関，地方自治体の機関（PDPA3条1項）及び公的業務を行う非国家的主体（同2項1号）	識別された，または識別可能な自然人に関する情報（PDPA6条1項）	法令に基づく場合（PDPA23条1項2号），公的機関がその権限を行使する際に必要な場合（PDPA23条1項4号）など	32条1項各号，アクセス，訂正，異議申立権等。	民事訴訟，PDPA18条1項の措置を求めるGIODOへの申立て	最も重いもので罰金または3年以下の自由制限刑，自由刑。	個人データ保護検査官局（GIODO）
イギリス	1998年データ保護法（なお，データ保護法案提案中）	1998年	公的部門と民間部門との区別はない。ただし，2000年情報の自由法により公的部門における個人情報の相当部分は，情報の自由法による	「『個人データ』は， (a)それらのデータから または， (b)それらのデータおよびデータ管理者の保有する，または，その保有することになるであろう他の情報から 生活する個人を識別することを可能にするのに関連するデータ	明確な行政法上の根拠があればそれによる。ない場合には，同意	主体のアクセス権，処理の停止権，ダイレクト・マーケッティング停止権，自動的意思決定に関する権利，損害賠償権，訂正・停止・消去・破棄請求権，コミッショナーに対する法律違反評価請求権	情報通知，執行通知，金銭制裁通知，強制監査／司法的救済（損害賠償請求，訂正・停止・消去・破棄請求権	金銭制裁通知／刑事罰	情報コミッショナー

第２部　EU 主要国における個人情報保護法制について

第１　ベルギー

１　ベルギーの公的部門における個人情報保護制度の概要

（１）背景・経過

ベルギーは，憲法 22 条 1 項で私生活の尊重を定めており，1992 年には EU データ保護指令に先駆けて 1992 年 12 月 8 日の個人データの処理に関するプライバシー保護法を成立させている。監督機関であるベルギープライバシー保護委員会は，執行権限や制裁権限を有さないデータ保護機関であったが，GDPR の完全適用である 2018 年 5 月 25 日にむけて，データ保護機関に関する実施法を成立させ，十分な権限を有するデータ保護機関が誕生する予定となっている。

（２）年表

1831 年 2 月 7 日	ベルギー憲法制定
1992 年 12 月 8 日	個人データの処理に関するプライバシー保護法成立
2001 年 2 月 13 日	ロイヤル・デクレ（施行令）制定
2017 年 11 月 16 日	データ保護機関設置法成立

２　ベルギーにおける GDPR のための対応について

（１）GDPR のための対応について

ベルギーにおいては，GDPR の完全適用である 2018 年 5 月 25 日に向けて，データ保護機関に関する実施法（データ保護機関設置法，組織法部分）が既に成立している他，実体法部分の実施法の検討及びデータ保護機関（ベルギープライバシー保護委員会，以下，単に「DPA」または「委員会」と呼ぶことがある。なお，データ保護機関に関する実施法によりベルギーデータ保護委員会に名称が変更になる。後述）によるガイドライン等の公表が行われている[20]。

（２）政府における対応について

①　設置法の概要[21]

2017 年 11 月 16 日，ベルギー上院がデータ保護機関設置法（Act on the Establishment

[20] ベルギー法についての情報はオランダ語及びフランス語によるものが充実している。詳細を検討するためにはオランダ語またはフランス語による文書の翻訳または現地でのヒアリングが必要となるが，ここでは英語による文献，情報を中心に情報を整理し，必要に応じてオランダ語及びフランス語による文献，情報を英語または日本語に自動翻訳することで大意を紹介するに留める。

[21] 英語による設置法の概要として Alston&Bird 法律事務所による，Jan Dhont, Lauren Cuyvers and

of the Data Protection Authority[22]，以下単に「設置法」と呼ぶ。）を可決し，ベルギーはオーストリア，ドイツに続き，GDPR 実施法を成立させた 3 番目の国となった。設置法は 114 条からなり，DPA の体制を変更し，主として助言機関であったところから，真に是正を行える，場合によっては懲罰的ですらある機能を備える機関を設置したものである。なお，GDPR の実施法としては設置法のみでは不十分であり，議会は直ちに，実体法部分の立法に着手すると考えられている。2018 年 3 月には，プライバシー担当国務長官である De Backer から，実体法部分に相当する実施法案について，同意可能な年齢（13 歳），統計や科学研究のための例外事由について含むというアナウンスがあったが，議会にはまだ掛けられていないとのことであった[23]。

② 設置法により設置される 6 つの機関

設置法は，現行ベルギーデータ保護法（Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data，1992 年 12 月 8 日の個人データの処理に関するプライバシー保護法，以下，単に「現行法」という。）上の分野別委員会（7 章の 2，36 条の 2）を廃し，委員会の中に以下の 6 つの機関を設置する[24]。それぞれの機関は，独立した専門家に助言を求めることも出来る。それに加えて，独立した，「反省協議会」（Reflection Council）が委員会に助言を行う予定である。これは，現在は，委員会の内部的な機能として行われているものである。反省協議会は，いわゆるマルチステークホルダーで構成される予定である。

i 実行委員会（Comitéde Direction - Directiecomité）

他の 5 つの機関の長で構成され，委員会の委員長が議長を務める。年次予算を管理し，データ保護に関連する技術的および商業的発展についての管理を担当する。毎年，「戦略プラン」を策定するほか，内部規定の制定も所掌する。

Daniel J. Felz "Privacy & Data Security Advisory: Data Protection Litigation to Become a New Reality in Belgium", Dec.20, 2017, https://www.alston.com/en/insights/publications/2017/12/data-protection-litigation （2018 年 1 月 13 日閲覧，以下特段の記載がない限り同じ）及び，Osborne Clarke 法律事務所による，Benjamin Docquir, Ann-Sophie De Graeve, Maïté Zambrano-Braun, and Deven Dobbelaere "Farewell Belgian Privacy Commission, hello Belgian Data Protection Authority", Nov.7, 2017, http://www.osborneclarke.com/insights/farewell-belgian-privacy-commission-hello-belgian-data-protection-authority/ （ただし，法案段階）が充実しており，本報告においてもこれらに多くを寄っている。

[22] 原文はオランダ語及びフランス語である。
http://www.dekamer.be/FLWB/PDF/54/2648/54K2648008.pdf

[23] 前掲 Dhont ら。De Backer からのアナウンスについては，Loyens & Loeff "GDPR Implementation law", Mar 2, 2018, https://www.lexology.com/library/detail.aspx?g=7fe7bec5-ed52-45b9-9bcf-fc4f210cd73a（2018 年 3 月 15 日閲覧）。

[24] 前掲 Dhont ら及び前掲 Docquir ら。原文では zes organen[蘭]，six organs[仏]である。「機関」が複数で委員会を構成するというのは日本の行政組織法的な感覚からは違和感はあるが，「部局」という扱いではないようである。

ii　中央事務局（Secrétariatgénéral - Algemeen secretariat）

DPA の日常業務（Dhont らには”purely clerical”とされており，処分等を伴わないというニュアンスと思われる）を担当する（例えば，苦情の受付，広報等)。もっとも，内部規定の適用，標準契約約款や拘束的企業準則（BCR，GDPR47 条）の受理，データ保護影響評価に必要な個人データの処理のリストの作成など，いくらか実態的な権限も行使する。

iii　フロントラインサービス（Premièreligne - Eerstelijnsdienst）

データ主体（個人データの「本人」）と調査機関（後述「調査機関」）及び紛争機関（後述「紛争解決会議室」）とを仲介する。紛争解決会議室への申立の「フィルター」機能を有する他，（一般的な）ガイドラインや勧告を提供するのもこの機関である。

すべての苦情や申立は，フロントラインサービスによる暫定審査を経て，苦情や申立を受理するかどうかが決定される。認められる苦情は紛争解決会議室に移管され，調査機関による調査等によって十分な証拠が得られたと判断した場合は，紛争解決会議室自身が行う是正措置命令等の行政処分につながる可能性がある。その他の要求や DPA への情報提供はフロントラインサービス自体によって処理される。フロントラインサービスは，両当事者の落とし所を探るべく，調停を開始することを決定することもできる。調停で解決策が見つからない場合，申立は苦情と同じ方法で処理され，紛争解決会議室に移送される。フロントラインサービスによる許可されない決定（不受理決定）には不服を申し立てることができることに注意しなければならない。

iv　ナレッジセンター（Center de connaissance - Kenniscentrum）

個人データの取扱いに関する質問に関する助言や勧告を行う責任を負う。これは，現行法における委員会の主たる機能である。

v　調査機関（Service d’inspection - Inspectiedienst）

ベルギーDPA の全く新しい機能である調査権限を行使する機関であり，調査局長が率いる。調査開始の端緒は，1）委員会または他の行政機関による調査要請，2）紛争解決会議室による補充的調査の要請，3）重大なデータ保護法違反の兆候がある場合の独自の調査開始，である。

その権限には，質問検査，報告の徴収，立入検査，IT システムの監査，関連データのコピー，資産または IT システムの捜索差押等が含まれる。他方，質問検査の対象となる個人に付与される権利とは，法執行機関（警察等）が刑事尋問を行う際に通常存在する権利を思い起こさせるものである（弁護人選任権，尋問調書の写しを得る権利等)。また，調査機関は，一時的な個人データの処理の中止，制限，凍結などの予備的措置を講じることもできる（最大 6 ヶ月間）ため，調査段階でもビジネスに大きな影響を及ぼす可能性がある。予備的措置には不服申立てが可能であるが，自動的に執行停止されるわけではなく，執行停止自体

も申し立てる必要がある。

これらの権限を行使する際に，調査機関は必要に応じて法執行機関の援助を要請することができる。調査の結果は，調査官の報告書が紛争解決会議室に提出される瞬間まで厳密に秘匿される。

刑事手続に類似するが，刑事手続における法執行機関の手続については制定法で制限されているのに対して，DPA の調査機関については DPA 自身が制定する内部規定によることになり，手続保障は刑事手続に比すると劣ることになる。

vi　紛争解決会議室（Chambre contentieuse - Geschillenkamer）

法人格を有し，DPA のための全く新しい権限である。紛争解決会議室の権限は改正前の委員会の権限よりはるかに大きく，裁判所に近い。紛争解決会議室は司法制度からは独立しているが，効果としては，裁判所や審判所における紛争解決に類似する。提訴は侵害救済措置を得るためのデータ主体，団体[25]または DPA 自身によって行われる。

紛争解決会議室での手続は，DPA の行政手続の最終段階であり，同室は制裁を科す権限を与えられた機関である。GDPR の下で監督当局に付与されたいわゆる「是正措置権」を行使することができる。その構造と組織は，司法機関に極めて似ている。室長と 6 人のメンバーから構成され，データ保護，行政管理，情報セキュリティ，情報通信技術等の専門家からなる。是正措置の内容として，個人データの処理の一時的または限定的な凍結または制限（または処理の全面的禁止），刑罰や課徴金の付課，国境を越えたデータ移転の中断，プライバシーに関する認証の取消，決定をウェブサイトでの公表などが可能である。潜在的制裁の観点からは，設置法は GDPR から逸脱するものではない。

紛争解決会議室の決定に対して，両当事者（DPA 及びデータ管理者または処理者）はブリュッセル控訴商事裁判所[26]（”Marktenhof”）に 30 日以内に不服申立てをすることができる。タイムリーな司法救済を可能にする趣旨であるとされている。商事裁判所は，規制当局の決定（特定の専門知識を必要とすることが多い）に対するすべての不服申立てを扱うため，2017 年初めにベルギーでの立法改革の後に制定された。ただし，不服申立てには執行停止効は存在しない（裁判所が執行停止を命ずることは出来る）。

データ保護法違反に関しての紛争解決機関からの決定は，個々の原告が管轄の民事裁判所に損害賠償を請求するための基礎にもなりうるとされている。

---

[25] プライバシー擁護団体（プライバシー・アドヴォケイト）が想定されていると思われる。

[26] http://www.juridat.be/beroep/brussel/index.htm

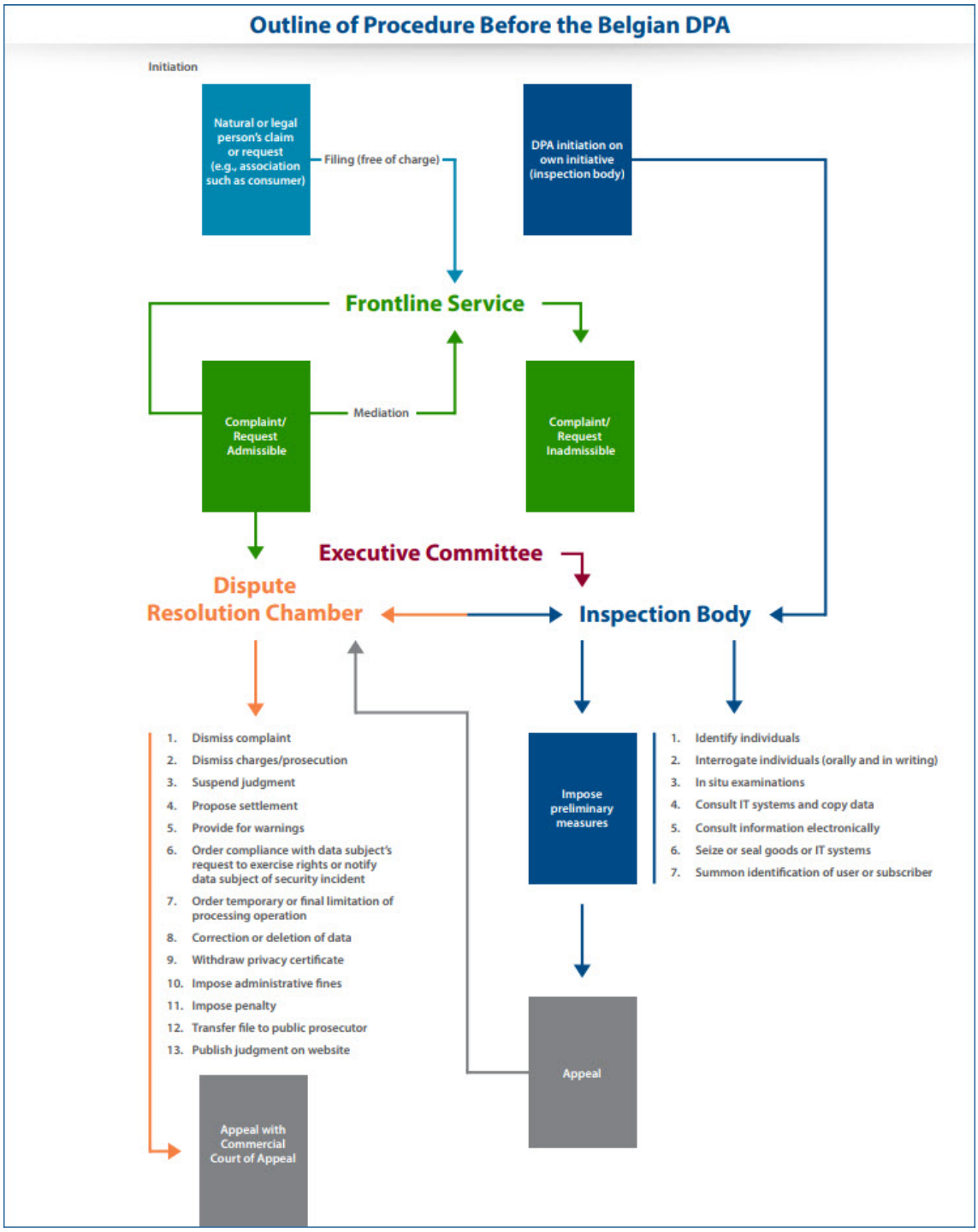


図 1　設置法による手続の流れ（Dhont らによる）

（3）データ保護機関における GDPR 対応について

委員会は GDPR に対応して 2018 年 1 月現在，4 種のパンフレット，ガイドラインを提供している。いずれも，オランダ語及びフランス語版のみが提供されているため，パンフレット（13 STAPPENPLANAANBEVELING）以外については題名のみの紹介に留める。

・13 STAPPENPLANAANBEVELING

「GDPR 遵守のための 13 ステッププラン」。2017 年 2 月 28 日までパブリックコメントに付された。カラーで，アイコンを用いたパンフレットとなっている。

図 2　13 STAPPENPLANAANBEVELING 表紙

図 3　13 STAPPENPLANAANBEVELING 2 頁目

・BETREFFENDE DE CUMULATIE VAN DE FUNCTIE DPO MET ANDERE FUNCTIES

「一般データ保護規制（GDPR）の適用におけるデータ保護責任者の任命，特にセキュリティコンサルタントの機能を含む他の機能とのこの機能の累積の許容性に関する勧告（CO-AR-2017-008）」。

・ONTWERP VAN AANBEVELING UIT EIGEN BEWEGING DPI

「データ保護の影響評価と公開協議の事前協議に関する草案の勧告（CO-AR-2016-004）」

・AAANBEVELING BETREFFENDE HET REGISTER VAN VERWERKINGSACTIVITEITEN[27]

「処理活動登録に関する勧告（GDPR 第 30 条）（CO-AR-2017-011）」。

GDPR30 条で新たに処理活動の記録が義務付けられたが，ベルギーでは処理活動については単に記録するのではなく，委員会に登録することを求めるようである。この登録のためのテンプレートを含むのが本勧告である。

3　GDPR 適用前の公的部門に関する個人情報保護制度の運用実態等 [28]

（1）公的部門の個人情報保護の法的枠組と議論動向

ベルギー憲法 [29]は 22 条 1 項で「何人も，自分の私生活と家族生活を尊重される権利を有する」としており，私生活の尊重が憲法上認められている。それ以外にも，欧州評議会第 108 条約，欧州人権及び基本的自由条約，欧州基本権憲章にそれぞれ加盟している。

データ保護法は現行法の他，2001 年 2 月 13 日のロイヤル・デクレ（政令レベルであり，データ保護法から詳細についての委任を受けた，いわゆる施行令）が存在する。これら以外に特別法として，2005 年 6 月 13 日の電気通信法が，情報通信プロバイダーに適用される法律としてあげられている。

（2）適用対象

現行法 3 条 1 項は「この法律は，個人データの全部または一部を自動的手段で処理すること，およびファイルシステムの一部を構成するか，またはファイルシステムの一部を形成

---

[27] DLA Piper 法律事務所による英語版の解説として，
http://blogs.dlapiper.com/privacymatters/belgium-belgian-dpa-provides-guidance-on-gdpr-article-30-publishing-template-for-records-of-processing-activities/

[28] Hunton & Williams 法律事務所による解説として，Wim Nauwelaerts and David Dumont “Data Protection & Privacy Belgium”, Sep. 2017,
https://gettingthedealthrough.com/area/52/jurisdiction/31/data-protection-privacy-belgium/

[29] ベルギー憲法裁判所のウェブサイトに掲載されているベルギー憲法の英語版につき，
http://www.const-court.be/en/basic_text/belgian_constitution.pdf

することを意図した個人データの自動的手段による処理以外の処理に適用される」と定め，現行法 1 条 4 項は「「管理者」とは，個人データの処理の目的および手段を単独でまたは共同で決定する，自然人または法人，非公認団体または公的機関を意味する。処理の目的と手段が法律，デクレ（政令）または条例により決定された場合，管理者は当該法律，デクレまたは条例によって定められた自然人，法人，非公認団体または公的機関となる。」同 5 項は，「「処理者」とは，管理者の直接権限のもとでデータを処理する権限を有する者を除き，管理者の代わりに個人データを処理する自然人，法人，非公認団体または公的機関を意味する。」と定義している。概ね，データ保護指令及び GDPR の規定ぶりと同様である。

（3）目的外利用の状況（目的外利用の根拠規定，件数等）

① 目的外利用禁止の根拠規定

現行法 4 条 1 項 2 号は「（個人データは）特定の，明示的かつ合法的な目的のために収集され，関連するすべての要素，特にデータ主体の合理的な期待と適用される法律および規制の条項を考慮に入れ，その目的と両立しない方法で処理してはならない。（ただし）プライバシー保護委員会の意見を受けた上で国王が確立した条件の下，歴史的，統計的または科学的目的のために行われるデータのさらなる処理は目的と両立しないとみなされない。」とし，同 4 号は，「（個人データは）正確で，必要に応じて最新の状態に保たれなければならない。収集された目的または処理される目的に関して不正確または不完全なデータが確実に消去または修正されることを保証するために，あらゆる妥当な手段が講じられなければならない。」，同 5 号は，「（個人データは）データが収集または処理される目的を考慮して必要以上にデータ主体の識別を可能にする形式で保管されてはならない。国王は，プライバシー保護委員会の意見を受けて，歴史的，統計的または科学的目的のために，上記よりも長時間保管される個人データの適切な保護手段を確立するものとする。」と定めており，典型的な目的外利用の禁止（2 号）の他，目的外保存の禁止（4 号），目的外識別の禁止（5 号）が管理者に義務付けられている（同 2 項）ものといえる。

② 目的外利用禁止に関する執行件数等

2013 年度にプライバシー委員会が受領した苦情は 450 件であり，そのうち，目的外利用禁止を含むプライバシー原則違反が 27.6%，同様に 2012 年度の苦情は 303 件であった（内訳不明）[30]。目的外利用が行われた件数についての統計は存在しないようである。

[30] European Commission Justice and Consumers “Sixteenth Report of the Article 29 Working Party on Data Protection Covering the year 2012” Adopted on 25 November 2014.p.90., European Commission Justice and Consumers “Seventeenth Report of the Article 29 Working Party on Data Protection Covering the year 2013” Published on 1 December 2016.p.96.

（4）本人関与の仕組み（開示，訂正，利用停止請求）と運用実態（請求件数等）

①　本人関与の仕組みについての一般的規定

第 3 章（9 条ないし 15 条の 2）が，データ主体の権利について定めているが，権利（"right to ***"）の形で定められているものとしては，ダイレクトマーケティングに対する異議申立権（9 条 1 項 c 号，2 項 c 号），アクセス権及び訂正請求権（同 1 項 d 号，2 項 d 号），管理者からの情報受領権（right to obtain，10 条 1 項柱書），健康に関連して処理される個人データについての情報受領権（10 条 2 項第 1 文），不適法な処理に関する異議申立権（12 条 1 項第 2 文），プライバシー保護委員会への申出権（13 条第 1 文）が存在する。

②　公的部門における本人関与の制限

国家安全保障局（the State Security Service），総合情報部（the General Intelligence），軍保安部（Security Service of the Armed Forces）等の安全保障部局による個人データの処理については，6 条（センシティブデータの取扱い禁止），10 条（管理者からの情報受領権等），12 条（訂正及び利用停止請求権），14 条（裁判所における情報受領権等の紛争処理），15 条（訂正請求等を受領した管理者の義務），17 条（個人データ取扱い前の委員会への通知），17 条の 2 第 1 文（個人データ取扱いへの条件付与），18 条（自動処理の登録），20 条（分野別委員会による認証等）及び 31 条 1 項から 3 項（委員会への苦情申し立て）は適用されない（3 条 4 項）。

司法警察の職務遂行のために公的機関が管理する個人データの処理等については，9 条，10 条 1 項及び 12 条は適用されない（3 条 5 項）。

6 条，8 条（訴訟等に関するデータの取扱い禁止），9 条（通知受領権），10 条第 1 項，12 条は，閣僚理事会における審議後のデクレによる王権の承認後は，欧州失踪・被性的搾取児童センターで行われる処理に適用されない（3 条 6 項）。

10 条は，データ対象が検査，調査または関連する準備活動の対象となる期間，連邦公共財政サービスによって管理される個人データの処理業務には適用されない（3 条 7 項）。

③　公的部門における本人関与の実態

2013 年度にプライバシー委員会が受領した苦情は 450 件であり，そのうち，本人への通知義務違反を含むプライバシー原則違反が 27.6%，同様に 2012 年度の苦情は 303 件であった（内訳不明）[31]。これ以上詳細な統計は存在しないようである。

（5）執行における特別事情／救済措置の仕組み（第三者機関，訴訟等）とその運用実態（件数等）

①　執行

現行法下のプライバシー委員会は執行権限を有さない。

---

[31] 前掲注 30。

② 司法的救済，責任および制裁

現行法下のプライバシー委員会は制裁権限も有していない。

15 条の 2 は，現行法違反による損害について管理者に損害賠償義務を負わせている。

（6）公的部門の個人データ保護の法執行における刑事罰の位置づけ

① 刑事罰概観

現行法 37 条から 43 条に以下のような刑事罰が定められている。

プライバシー委員会委員または職員の秘密保持義務違反（37 条）

→200～1 万ユーロの罰金

15 条または 16 条 1 項に反した管理者等（38 条）

→100～2 万ユーロの罰金

以下に反した場合（39 条）

→100～10 万ユーロの罰金

・4 条 1 項，5～9 条に反した管理者等（1 号～4 号）

・請求を受けて 45 日以内に，または誤った情報であることを知りつつ 10 条 1 項に反して訂正を行わなかった管理者等（5 号）

・個人データの公開や同意を強要した者（6 号）

・17 条に反して自動処理を継続した管理者等（7 号）

・17 条に反して不正確な情報を提供した管理者等（8 号）

・19 条に反し，委員会の指示に従わなかった管理者等（10 号）

・21 条 2 項及び 22 条に反して越境データ移転を行った者（12 号）

・委員会の調査妨害（13 号）

代理人等に罰金が課せられた場合，民法上，管理者またはそのベルギーにおける代理人が支払い義務を負う（42 条）。

ベルギー刑法[32]第 1 分冊（7 章及び 85 条を含む）は現行法及び委任されたデクレに適用される。

② 公共部門と刑事罰

特段，公共部門であることによる規定は見受けられない。

[32] ベルギー刑法に関する法語文献としては，横山潔「ベルギー刑法典-1～5 完-（立法紹介　ベルギー」外国の立法 22 巻 5 号（1983 年）259-284 頁，同 6 号（1983 年）373-388 頁，同 23 巻 1 号（1984 年）35-54 頁，同 2 号（1984 年）79-100 頁，同 3 号（1984 年）141-158 頁，末道康之「ベルギー刑法改正の動向：刑法改正草案第 1 編の検討(1)」南山法学 41 巻 1 号（2017 年）115-181 頁参照。

（7）公的部門における個人データの保護に関する著名判決例

現行法の委員会には執行及び制裁権限が存在せず，これに関する裁判例も見当たらないようである。

第２　ドイツ

１　ドイツの公的部門における個人情報保護制度の概要

（１）背景・経緯

①　背景

ドイツ基本法においては，人間の尊厳の不可侵性（第１条）及び人格の自由な発展を求める権利（第２条）が規定されている[33]。憲法裁判所は，自由な人格発展の権利が憲法秩序の最高位に位置付けられることを示した[34]。

1970 年，世界で初めてとなるデータ保護法がヘッセ州において制定された。ドイツにおいては，1977 年連邦データ保護法のほかに，16 州（Länder）においてそれぞれデータ保護州法が整備されてきた。連邦法は，原則として，公的部門と民間部門に適用されるが，州法は公的部門を規律する性格となっている。

データ保護の権利については，連邦憲法裁判所の判決においてもみられる。たとえば，1983 年，国勢調査法一部違憲判決において，連邦憲法裁判所は「情報自己決定権」を憲法上の権利であることを認めた。すなわち，情報自己決定権は，自らの個人データの開示および利用について，原則として自ら決定する権限であり，この権利が人格の自由な発展に寄与するものであると説明される[35]。この判決において，連邦憲法裁判所は，国勢調査法自体は合憲としつつ，国勢調査の調査事項の利用に関する届出記録簿との照合を認める規定，調査分野を専門的に所管する連邦及び州の最上級行政庁等への提供を認める規定及び一定の行政目的のために市町村等への提供を認める規定を情報の自己決定を求める権利に反するとの理由で違憲と判断した[36]。

ドイツにおいて厳格なデータ保護法が整備された背景には，ナチスによる秘密国家警察や東ドイツにおけるシュタージによる監視活動の反省と共に，ナチスが個人情報を管理するためのパンチカードを用いてユダヤ人を大量殺戮したという苦い歴史がある。

②　経緯

1960 年代には，官民両部門において，効率的なデータの自動処理が普及していった。当初，連邦政府は，民法等の既存の法律によりプライバシー権を十分に保護することができると考え，データ処理の追加的規制の必要性を示さなかった。しかし，他国における立法化の動向などもみられ，1973 年，連邦議会にデータ保護法案が提出された。そして，議会での

---

[33] ドイツ基本法の法語訳については，初宿正典･辻村みよ子編『新解説世界憲法集第４版』（三省堂・2017），参照。

[34] Constitutional Court, Judgment of November 6, 1958, 7 BVerfG 377, 405

[35] 藤原静雄「西ドイツ国勢調査判決における『情報の自己決定権』」一橋論叢 94 巻 5 号（1985）728 頁，玉蟲由樹「ドイツにおける情報自己決定権について」上智法学論集 42 巻 1 号（1998）115 頁，小山剛「『安全』と『情報自己決定権』」法律時報 82 巻 2 号（2010）99 頁，高橋和広「情報自己決定権論に関する一理論的考察」六甲台論集 60 巻 2 号（2014）105 頁，参照。

[36] 藤原・前掲注 35, 728 頁，参照。

審議を経て，1977 年 2 月 1 日連邦データ保護法が公布された。

2016 年 5 月 4 日に公布された GDPR については，ドイツは EU の立法審議において大きな影響力を有してきた。欧州議会の報告者はドイツから選出された Jan Philipp ALBRECHT 議員（緑の党）[37]が議会における修正案の取りまとめを行ってきた。なお，ドイツのデータ保護機関は規則提案の強力な支持者であるのに対し，ドイツ政府は規則提案について反対の表明を示してきた。この背景には，規則提案が公表される直前に，ドイツ憲法裁判所のある裁判官が，ドイツ憲法で保障されてきたデータ保護の枠組みが失われることの悲嘆を論文で公表したことで，規則提案の正統性がドイツ国内で揺らいだ，と Albrecht 議員は論文で指摘する [38]。

（2）年表

1970 年	ヘッセン州個人データ保護法制定（9 月 30 日）
1977 年	連邦データ保護法 Bundesdatenschutzgesetz（BDSG）公布（2 月 1 日）
1983 年	憲法裁判所国勢調査法一部違憲判決
1990 年	連邦法改正
1995 年	EU データ保護指令（1998 年施行）
2001 年	指令に対応した法改正公布（1 月 14 日）
2009 年	連邦法改正（データ主体の権利，通知義務，労働者のデータ保護等）
2017 年	GDPR に対応した連邦法改正制定（6 月 30 日）

2　GDPR 施行に向けたドイツの公的部門に関する法整備等の状況

（1）2017 年法改正の概要

2017 年 6 月 30 日，GDPR 施行に向けて連邦データ保護法（以下，「連邦法」という。）が全面改正された。なお，この法改正は，刑事司法分野の個人データ指令を国内法化する内容も含まれている。

第 1 部　第 1 章　　適用範囲

連邦法は，連邦の公的機関及び州法で規律されていない連邦に基づく行為を行っている場合または司法機関として行動している場合の州の公的機関に適用される（第 1 条）。

また，個人データの処理を行う民間の事業者にも適用される。民間の事業者については，

[37] 1982 年生まれ，ドイツフンボルト大学，ハノーファー大学を卒業後，研究員を経て，2009 年欧州議会議員に当選。欧州議会市民的自由・司法及び内務委員会の副委員長（Vice-Chair）を務めている（2018 年 3 月現在）。

[38] Jan Philipp Albrecht, Uniform Protection by the EU: The EU Data Protection Regulation Salvages Informational Self-Determination, in DATA PROTECTION ANNO 2014: HOW TO RESTORE TRUST? 125 (Hielke Hijmans & Herke Kranenborg eds., 2014).

①ドイツ域内で個人データを処理する管理者または処理者，②ドイツ域内の管理者または処理者の設置の活動において個人データを処理する場合，または③加盟国内に管理者または処理者の設置がない場合でも GDPR の規定に基づく場合には，連邦法が適用される。ただし，自然人による処理がもっぱら個人的または家庭的活動において生じた場合においては適用されない。

第 2 章　　定義

連邦の公的機関とは，連邦の機関，司法機関及びその他の公法上の組織を言う。州の公的機関とは，州の機関，司法機関及びその他の公法上の組織を言う。連邦及び州の公的機関の私法上に基づき設置された組織は，州の境界を越えて処理を行っている場合などに連邦の公的機関とみなされる。（第 2 条）

第 3 章　　個人データ処理の法的根拠

公的機関による個人データ処理については，職務の遂行のために必要な場合または管理者に付与された公的資格を行使するために必要な場合に認められている（第 3 条）。

また，公共の場におけるビデオカメラについては，（ⅰ）公的機関の職務において必要な場合，（ⅱ）アクセス制限を行う権利を行使する場合，または（ⅲ）特定された目的の正当な利益のために必要な場合においてのみ設置・運用が認められている。

カメラの設置については，管理者の氏名及び連絡先を公表するとともに適切な措置が講じられなければならず，GDPR 第 13 条及び第 14 条に従い，特定の人を対象とした監視についてはビデオ監視について情報提供を行わなければならない。さらに，利用目的の必要性を超えた場合，またはデータ主体の正当な利益を害する場合，データは遅滞なく消去されなければならない（第 4 条）[39]。

第 4 章　　データ保護及び情報公開連邦コミッショナー
（公的機関におけるデータ保護責任者）

（ⅰ）任命

公的機関はデータ保護責任者を配置しなければならない（第 5 条）。組織の構造及び規模を考慮して，複数の公的機関に一人のデータ保護責任者を配置することができる。データ保護責任者は，公務員または契約に基づく者とされ，データ保護の法と実務の専門的知識及び任務を遂行する能力等の専門的資質に基づき任命されるものとする。公的機関はデータ保護責任者の連絡先を公表し，データ保護情報公開の自由連邦コミッショナーに連絡しなければならない。

[39] 2017 年 3 月 1 日，連邦コミッショナーはビデオ監視に関する簡単なガイドを公表したとのことである（Datenschutz kompakt: Videoüberwachung, 1 März 2017（ドイツ語のみ））。

（ⅱ）地位

公的機関は，データ保護責任者が適切かつ時期に適って個人データ保護に関連するすべての事項に関与することを確保しなければならない（第 6 条）。データ保護担当者は，自らの職務についていかなる指示も受けないことを保証され，公的機関の組織の最高責任者層に直接報告しなければならない。また，データ保護責任者は職務の遂行について公的機関から解職されたり罰則を受けたりすることがないものとする。任命の任期は 1 年未満とすることができない[40]。

（ⅲ）任務

GDPR で定められた任務[41]に加えて，①公的機関及び連邦法に従い処理を行う公務員に対して情報とアドバイスの提供を行うこと，②連邦法及びその他のデータ保護立法の遵守を監視すること，③データ保護影響評価に関するアドバイスを行うこと，④監督機関と協力を行うこと，⑤監督機関のコンタクトポイントとして処理に関する事項について行動することがデータ保護責任者の任務とされている（第 7 条）。

（連邦データ保護情報公開コミッショナー）

（ⅰ）設置

連邦データ保護情報公開コミッショナー（以下，「コミッショナー」という）は，連邦の最高機関と位置付けられている（第 8 条）。コミッショナーの職員は連邦公務員であり，事務局はボンに置かれている。

（ⅱ）権限

コミッショナーは，連邦の公的機関を監督する権限を有しており，民間の事業者に対しても権限が及ぶ。ただし，司法権の行使における連邦裁判所における処理業務には権限が及ばない。（第 9 条）

---

[40] バイエルン州監督機関は，2016 年 10 月，企業の IT 管理部門の担当者に内部のデータ保護責任者を任命することは利益相反にあたり，独立性が確保できていないとしてこの企業に制裁金を科した。
Datenschutzbeauftragter darf keinen Interessenkonflikten unterliegen
https://www.lda.bayern.de/media/pm2016_08.pdf（ドイツ語）

[41] GDPR 第 39 条では次の規定がある。
1. データ保護責任者は少なくとも次の任務を行うものとする。
（a）本規則および他の欧州連合または加盟国のデータ保護の条項に従い，処理の義務を遂行する管理者または処理者および労働者に対し通知し忠告すること
（b）本規則，他の欧州連合または加盟国のデータ保護の条項，および個人データの保護に関連する管理者または処理者の政策への法令遵守を監視すること
（c）データ保護影響評価に関する要請があった場合の忠告をすることおよび第 35 条に従い任務の監視を行うこと
（d）監督機関との協力を行うこと
（e）第 36 条にいう事前の協議を含む処理に関連する問題について監督機関への連絡先として行動すること，および必要に応じ他の問題に関する協議を行うこと
2. データ保護責任者は，処理の性質，範囲，文脈および目的を考慮に入れ，自らの任務を遂行において処理の運用に取り巻くリスクに配慮するものとする。

（iii）独立性

コミッショナーは完全に独立して権限行使を行うこととされている。外部からの直接または間接の影響を受けてはならず，また，いかなる者からも指示を受けたたり求めてはならない。ただし，独立性の影響を受けない限りにおいて，会計検査院（Bundesrechnungshof）による監査を受けるものとされている。（第 10 条）

（iv）任期

コミッショナーは連邦大統領からの任命を受け，35 歳以上の者とされる。個人データ保護の分野における専門性，経験及び技術を有する者とされる。就任に際して，宣誓を行うこととされる。任期は 5 年間とし，一度だけ再任されることができる。（第 11 条）

コミッショナーは，重大な違法行為を犯した場合または任務遂行の要件を満たさない場合，大統領の要請により解任される。（第 12 条）

（v）任務

コミッショナーは，①連邦法及びその他のデータ保護法の適用の監視及び執行，②個人データ処理に関するリスク，規則，安全管理及び権利に関する市民の意識向上及び理解の向上，③連邦政府等への個人データ処理に係る自然人の権利及び自由の保護に関する立法及び行政措置に対する忠告，④管理者及び処理者の連邦法及びその他のデータ保護法に基づく義務に関する意識向上，⑤権利行使に関してデータ主体の情報に対する情報提供，⑥データ主体または組織により提起された苦情の処理及び苦情に関する問題についての調査，⑦他の監督機関との情報共有を含む協力及び相互扶助，⑧連邦法及び他のデータ保護法の適用に関する調査，⑨個人データ保護に影響を及ぼす関連する動向の監視，⑩処理業務に関する忠告，⑪欧州データ保護委員会の活動への寄与である。（第 14 条）

コミッショナーは，違反の類型リストを含む年次活動報告書を作成し，連邦政府等へ提出するものとされている（第 15 条）。

（vi）権限

コミッショナーは，GDPR 第 58 条にいう権限[42]を有するものとされている。コミッショ

[42] GDPR 第 58 条における権限とは次のものをいう。
1. 各監督機関は，次のすべての調査権限を有するものとする。
（a）管理者および処理者に対して，また該当する場合には管理者または処理者の代理人に対して，監督機関の任務の遂行のため要求した情報の提供の命令
（b）データ保護監査の形式における調査の実施
（c）42 条 7 項に従い発行された認証の審査の実施
（d）申立てられた本規則の違反に関する管理者または処理者への通知
（e）管理者および処理者から業務遂行のため必要なすべての個人データと情報へアクセスすること
（f）EU 法または加盟国法に従い，データ処理の備品と手段を含む，管理者および処理者の施設への立ち入り
2. 各監督機関は，次のすべての是正権限を有するものとする。
（a）予定されている処理業務が本規則の規定に違反する可能性がある管理者または処理者に対する警告の発出
（b）処理業務が本規則の規定に違反した場合の管理者または処理者に対する懲戒処分の発出
（c）本規則に従う権利の行使のデータ主体の要請を遵守させるための管理者または処理者に対する命令
（d）処理業務を，該当する場合には具体的方法および具体的期間内において，本規則の規定に遵守させ

ナーは，連邦の公的機関が違反をしたと認定した場合，コミッショナーは連邦の最高機関に対して苦情申立を行うものとされている。コミッショナーの権限は，郵便並びに通信に関する連邦の公的機関が保有する個人データ及び税の秘密を含む専門的または特別の公的秘密に関する個人データに対しても及ぶ。

連邦の公的機関は，コミッショナー及びその職員に対して，①いつでもデータ処理の設備並びに手段を含め職場及びすべての個人データと任務遂行に必要なすべての情報へのアクセス，②任務遂行のために必要なすべての情報を提供しなければならない。

連邦コミッショナーは，州におけるデータ保護法の順守の監視に責任を有する公的機関と協力して職務を行うものとされている。（第 16 条）

第 5 章　　欧州データ保護委員会への代表，連邦と州との関係等

欧州データ保護委員会へは，連邦コミッショナーが共同代表を務めることとし，州の監督機関が共同代表の一員となることができる。（第 17 条）

監督機関に関する連邦と州との関係については，それぞれの監督機関が協働して早い段階でコメントの調整を行い，共通の立場を他の加盟国，欧州委員会及び欧州データ保護委員会へ提出するものとする。連邦と州の機関との間で共通の立場の実現ができない場合，主たる監督機関が共通の立場の提案を行うこととする（第 18 条）。主たる機関については，GDPR 第 7 章に従うワンストップショップの仕組み（主たる監督機関が関係するその他の加盟国の監督機関と協力する仕組み）が採られるものとする（第 19 条）。

るための管理者または処理者に対する命令
（e）データ主体に対する個人データ侵害の連絡を取るための管理者への命令
（f）処理の禁止を含む暫定的または確定的制限
（g）16 条，17 条ならび 18 条に従う個人データの訂正もしくは削除または処理の制限の命令および 17 条 2 項ならびに 19 条に従い個人データが開示された受領者への当該措置の通知
（h）42 条および 43 条に従う認証の撤回または認定機関に対する発行された認証の撤回の命令，または認証の要件が満たされないもしくはもはや満たされていない場合の認証を発行しないようにする認定機関に対する命令
（i）個々の事案の状況に応じ，本節にいう措置に加えて，もしくはそれに代わり，83 条に従う行政上の制裁金を科すこと
（j）第三国または国際機関における受領者へのデータ移転の停止の命令
3.　各監督機関は，次のすべての認可および助言の権限を有するものとする。
（a）36 条にいう事前相談の手続に従う管理者への助言
（b）自ら進んでまたは要求に応じ，加盟国法に従い，国の議会，加盟国の政府またはその他の組織ならびに機関と市民に対する個人データ保護に関連するいかなる問題についての意見の付与
（c）加盟国の法律が事前の認可を要求する場合，36 条 5 項にいう処理の認可
（d）40 条 5 項に従い行動規範案への意見の付与および承認
（e）43 条に従う認定機関の認証
（f）42 条 5 項に従い認証の発行および認証の基準の承認
（g）28 条 8 項および 46 条 2 項 d 号にいう標準データ保護条項の採択
（h）46 条 3 項 a 号にいう契約条項の認可
（i）46 条 3 項 b 号にいう行政取決めの認可
（j）47 条に従う拘束的企業準則の承認

第 6 章　　法的救済

自然人・法人と連邦とまたは州の監督機関との間の紛争については，行政裁判所において救済を求めることができる（第 20 条）。

このほか，監督機関が欧州委員会の十分制認定，または標準データ保護条項もしくは行動規範について，法に違反すると思料した場合，そのデータ移転手続を停止し，裁判所の決定を求めることができる（第 21 条）。2015 年 10 月 6 日，EU 司法裁判所が欧州委員会のセーフハーバー決定を無効とする判決を下し，これにより EU 及び欧州経済地域から米国への個人データの移転が同決定に基づき行うことができないことを理由として，ハンブルク州コミッショナーは，セーフハーバー決定に基づきデータ移転を継続していた 3 社に対し，制裁金（合計 28,000 ユーロ）を科した[43]。

第 2 部　第 1 章　　個人データ処理の法的根拠

（個人データの特別類型（センシティブデータ））

GDPR 第 9 条の特例により，公的部門と民間部門において，次の場合には個人データの特別類型の処理が認められるものとされている。すなわち，（ｉ）社会の安全及び社会の保護の権利から生じる権利の行使のために必要な処理，（ⅱ）予防医学，労働者の労働能力の評価，医療診断，医療ケア・社会ケアの提供のために必要な処理，（ⅲ）公衆衛生の分野における公共の利益の理由として必要な処理の 3 つの場合である。

また，公的機関においては，（ｉ）実質的な公的利益の理由のため緊急に必要な場合，（ⅱ）公共の安全の実質的脅威の防止のため必要な場合，（ⅲ）共通善への実質的害悪を防止し，もしくは共通善の実質的憂慮から保護するため緊急に必要な場合，または（ⅳ）危機管理または紛争防止の分野もしくは人道的措置のため連邦の公的機関の政府間の義務を守る緊急の理由にとって必要な場合，もしくはその義務を履行するために必要な場合，において管理者の利益がデータ主体の利益を上回る場合には特別類型のデータ処理が許されている（第 22 条）[44]。

（公的機関による他の目的のための処理）

公的機関の個人データについては，次のいずれかの場合に職務の遂行にとって必要な処理が認められている。（第 23 条）

（ｉ）明らかにデータ主体の利益になり，データ主体が同意を拒否すると推定する根拠が

---

[43] Adobe に対し 8000 ユーロ，Punica に対し 9000 ユーロ，Uniliver に対し 11000 ユーロの制裁金がそれぞれ科された。The Hamburg Commissioner for Data Protection and Freedom of Information, Press release, Inadmissible data transfer to the USA, 6 June 2016. Available at https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-06-06_Data-Transfer_to_the_USA.pdf

[44] GDPR 第 9 条 1 項では，個人データの特別類型の処理について規律している。
「1 人種もしくは民族の出自，政治的見解，信仰もしくは哲学上の信念または労働組合の構成員を明らかにする個人データの処理，および自然人を特定して識別する目的の遺伝データ，生体データ，健康に関するデータまたは自然人の性生活もしくは性的指向に関するデータの処理は禁止する」。

ない場合，

（ⅱ）情報が不正確であると考えるためにデータ主体により提供された情報を確認するために必要な場合，

（ⅲ）共通の利益への実質的害悪または公共の安全への脅威の防止ために必要な場合，

（ⅳ）刑事または行政上の罰則の訴追のため必要な場合，

（ⅴ）別の者の権利への深刻な害悪を防止するために必要な場合，または

（ⅵ）管理者の監査または組織的検査の実施のため，監督及び監視の権限を行使するために必要な場合。

（公的機関によるデータ移転）

公的機関から公的機関への個人データの移転については，移転先の機関または第三者が職務の遂行において必要な場合または公的機関による他の目的のための処理（第 23 条）に従い処理が認められている条件を満たす場合に許容されるものとされている。データが移転された第三者は，移転された目的にのみ当該データを処理することができる。

公的機関から民間機関への個人データの移転については，(i) 移転先の機関の職務の遂行のために必要な場合もしくは第 23 条に従い処理される条件を満たしている場合，(ii) データが移転された第三者が，移転されたデータを知り得る正当な利益を提示し，かつデータ主体がデータが移転されることについて正当な利益を有しない場合，または (iii) 法的請求の証明，行使もしくは弁護のために必要な場合，において認められている。（第 25 条）

（雇用関連の目的のデータ処理）

労働者の個人データは，雇用の決定，雇用後の雇用契約の締結もしくは終了，または労働者の権利及び義務の行使のために必要な場合，雇用関連の目的のため処理することができる。労働者の個人データを同意に基づいて処理する場合，雇用関係への労働者の依存度及び同意が与えられた状況が，自由な意思の同意において考慮されなければならない。同意は，他の形式が適当な場合を除き，書面で行わなければならない。（第 26 条）

連邦労働裁判所は，就業規則に違反した疑いのある労働者について一週間で 50 時間，また必要に応じ特定の労働者を 48 時間追加でビデオ監視することは違法であると判断した[45]。

第 2 章　　データ主体の権利

（個人データ収集の際における情報提供）

データ主体への情報提供についての例外（GDPR 第 13 条 4 項）に加えて，GDPR 第 13 条 3 項に従いデータ主体に情報を提供する義務については，次の場合には追加の利用に関する情報を提供する場合には適用されない。

（ⅰ）アナログ媒体で蓄積された個人データの追加処理について，管理者がデータ主体と

[45] Federal Labour Court of 29 June 2004, file no. 1 ABR 21/03.

直接契約を締結し，当初の目的と両立可能な追加処理を行い，デジタル媒体でデータ主体との連絡が行われておらず，かつデータ主体の情報受領の利益が小さなものであるとみなされる場合

（ⅱ）公的機関においては，任務の適切な遂行に支障を及ぼし，かつ情報提供しない管理者の利益がデータ主体の利益を上回る場合

（ⅲ）公共の安全もしくは公序への危険が生じ，または連邦もしくは州の福利を害し，かつ情報提供を行わない利益がデータ主体の利益を上回る場合

（ⅳ）法的請求の証明，行使または弁護に影響を及ぼし，かつ情報提供を行わない利益がデータ主体の利益を上回る場合

（ⅴ）公的機関へのデータ移転の機密が害される場合（第 32 条）

また，GDPR 第 14 条 5 項の例外に加えて，データ主体への情報提供の義務は，公的機関について，職務の適切な遂行に危険を及ぼす場合または公共の安全もしくは公序への危険が生じ，または連邦もしくは州を害する場合には適用されないものとする（第 33 条）。

（アクセス権）

GDPR 第 15 条におけるアクセス権について，連邦の公的機関がデータ主体に対し情報を提供しない場合，連邦最高機関が連邦または州の安全が脅かされると決定しない限り，かかる情報はデータ主体の要請により連邦コミッショナーに通知されなければならない（第 34 条）。

（異議申立権）

データ主体の利益を上回る緊急の公共の利益があり，または法により処理が要求されている場合，GDPR 第 21 条 1 項 [46]の異議申立権は公的機関に対して適用しないものとされる（第 36 条）。

第 3 章　　管理者及び処理者の義務

GDPR43 条に従う認証機関として行動する権限は，認証機関のデータ保護監督に責任を有する連邦または州の監督機関により認定されるものとする。（第 39 条）

なお，シュレスヴィッヒ・ホルシュタイン州において，2009 年にデータ保護シール制度を導入し，IT 関連製品に対するシールとデータ保護監査に対するシールの 2 種類の運用を

[46] GDPR 第 21 条の異議申立権及び個人の自動決定については，「1. データ主体は，自らの特定の状況に関する根拠に基づき，第 6 条 1 項 e 号または f 号に基づき，ならびにこれらの規定に基づくプロファイリングを含め，個人データの処理に対し，いつでも異議申立の権利を有する。管理者は，データ主体の利益，権利および自由もしくは法的請求の確定，行使あるいは擁護を上回る処理のための不可欠な正当な根拠を示さない限り，個人データの処理をもはやすることができない。」と規定されている。21 条については，加盟国法でこの権利の制限を認める規定がないため，いかなる場合に法により処理が要求されている場合にこの規定の適用除外となるかについては定かではない。

行っている[47]。

第 4 章　　民間事業者によるデータ処理に対する監督機関

州法に従う機関は，GDPR におけるデータ保護の規定の民間事業者による運用を監視しなければならない。ドイツ域内に複数の管理者または処理者が存在する場合，権限ある監督機関を決定するため GDPR の主たる機関に従い決定する。権限が不明確な場合は共同決定を行うものとする。（第 40 条）

2009 年 9 月の法改正により，管理者は安全管理措置違反があった場合，監督機関に対して速やかに通知をしなければならない（第 42a 条)。対象は，金融データ，クレジットカードデータ，通信データ，オンラインで収集されたデータ，犯罪歴に関するデータ，その他のセンシティブデータである（GDPR 施行後は GDPR 第 33 条･第 34 条に従うこととなる)。

2014 年，連邦ネットワーク庁と連邦データ保護監督機関は，113 件の安全管理措置の侵害通知を受領した[48]。また，バイエルン州監督機関は，2016 年 10 月，サイバーセキュリティイニシアティブを公表し，ウェブの暗号化の脆弱性に関して調査を開始するとともに，監督機関のホームページにおいて対象となるホームページの安全性チェックの依頼を受け付けている[49]。

第 5 章　　罰則

連邦法で特別の定めがある場合を除いて，罰則は GDPR の規定に従うこととされている（第 41 条)。連邦法による特別の定めがある場合として，大規模な個人データを対象に意図的に，商業目的の個人データの第三者提供または第三者にアクセスできる状態においた行為に対し， 3 年以下の懲役または罰金が科せられる。また，許可なしに処理を行った場合または欺瞞的に取得した場合で，金銭の支払いを見返りに受領したり，第三者を害した行為に対しては，2 年以下の懲役または罰金が科されうる。（第 42 条）消費者信用情報について，不正確，不完全または著しく遅滞して消費者に情報提供した場合は，50,000 ユーロ以下の制裁金が科されうる（第 43 条)。

（2）年表

2016 年 4 月 14 日	GDPR が欧州議会にて可決，5 月 4 日公布
2017 年 4 月 27 日	新連邦データ保護法 Bundesdatenschutzgesetz が連邦議会で可決（5 月 12 日参議院で可決）
2017 年 7 月 5 日	新連邦データ保護法公布

[47] 藤原静雄「ドイツ・シュレスヴィッヒ・ホルシュタイン州のマーク制度」情報公開・個人情報保護 25 号（2007）25 頁，参照。
[48] Monika Kuschewsky, Germany, op cit.
[49] Bayerisches Landesamt für Datenschutzaufsicht, Pressemitteilung BayLDA prüft Verschlüsselung von Webseiten, 10. Oktober 2017. https://www.lda.bayern.de/media/pm2017_08.pdf

3　GDPR 施行前の公的部門に関する個人情報保護制度の運用実態等

（1）概要

①　公的部門を規律する法律

連邦データ保護法

このほか，テレメディア法，電気通信法，刑法，マネーロンダリング法，薬物法，電子診断法，市民の登録法，電子健康法等において個別分野の個人データ保護に関する規定がある。また，2015 年には IT セキュリティ法が施行され，重要インフラの責任者への義務が定められているほか，違反した場合の制裁金（10 万ユーロ以下）が定められている。

②　公的部門を監督する機関

データ保護及び情報公開連邦コミッショナー

Ms Andrea VOSSHOFF（2017 年 12 月現在）…2013 年 12 月に任命。前職は弁護士兼ドイツキリスト教民主同盟の連邦議会の議員であり，就任時 55 歳であった。

議会では，403 票（全 585 票）の支持を得た一方で，当時 GDPR のレポーターを務めていた欧州議会 Jan Philip Albrecht 議員は反対を表明した [50]。

2010 年，EU 司法裁判所は，ドイツのいくつかの州における監督機関について，内務省が監督機関であったため，EU データ保護指令が定める「完全な独立性」（第 28 条）に違反するという判決を下した [51]。EU 司法裁判所の判決において「完全な独立性（complete independence）」とは，「監督の対象となる機関によって行使されるあらゆる影響のみならず，私生活への権利の保護と個人データの自由な流通との公正な衡量を図るという監督機関による任務の遂行に疑義が生じうる，直接または間接を問わず，いかなる指示もその他のいかなる外部の影響力も排除すること」[52]と定義されている。監督機関の特別な地位を付与するために独立性の要件が設けられたわけではなく，個人の保護を強化するために監督機関は独立していなければならない。この任務を遂行するため。監督機関は客観的かつ公平に行動しなければならない。EU 司法裁判所判決によれば，ドイツは約 30 年にわたり効果的な監督機関を築き上げてきたが，この完全な独立性の要件は指令の目的の平等な水準の維持のためすべての加盟国において要求されるものである。

EU 司法裁判所の判決を受けて，2016 年 1 月までに各州の監督は，もはや内務省の影響を一切受けないものとして組織改革が行われた。

---

[50] IAPP, German Parliament Elects Andrea Voßhoff New Federal Data Protection Commissioner, 19 December 2013. Available at https://iapp.org/news/a/german-parliament-elects-andrea-vosshoff-new-federal-data-protection-commis/ なお，欧州議会で GDPR のレポーターである Jan Philipp Albrecht 議員の共著による解説書”Das Neue Datenschutzrecht Der Eu”（2016）が公刊されている

[51] C-518/07, European Commission v. Federal Republic of Germany, EU:C:2010:125.

[52] C-518/07, European Commission v. Federal Republic of Germany, EU:C:2010:125 para 30.

（2）各項目の分析

① 適用対象機関

（対象機関）

連邦の公的機関及び州法で規律されていない連邦に基づく行為を行っている場合または司法機関として行動している場合の州の公的機関

（通知）

データ保護責任者を任命する義務がない中小企業及び商業目的で第三者定業するためデータ保存する企業等は州の監督機関への通知が必要な場合がある。たとえば，バイエルン州監督機関は153件の登録を受領（うち約半数はデータブローカや探偵業者）（2013－14年），またハンブルク州監督機関は57件の企業登録を行った[53]。

② 保護対象データの範囲

（保護の範囲）

ドイツ法はGDPRの定義をそのまま利用している。一般に公開されている連邦機関がIPアドレスを保存していたことが問題となり，ドイツ連邦最高裁判所は，EU司法裁判所の先決判決のとおり，IPアドレス（動態的IPアドレスを含む）が個人データに該当することを認めたうえで，サイバー攻撃の調査のために必要な限りでIPアドレスの情報を保全することを認めた[54]。

（ファイリングシステム）

民間事業者においては，ファイリングシステムを構成するまたは構成する意図がある個人データの自動的手段またはそれ以外の手段による処理について連邦法が適用される（第1条2項）。

（電子医療）

2015年12月，電子医療法が成立し，2018年7月1日に施行される[55]。この法律により，任意ではあるものの，新たに患者の「電子医療カード」が作成されることとなり，アレルギー，血液型，過去の病歴などのデータが保存される予定である。医師の紹介状についてもデジタル化される予定である。

法案審議中には，テレマティクスインフラストラクチャーや電子医療カードについては

---

[53] Monika Kuschewsky, Germany, in Data Protection & Privacy, 3rd ed. European Lawyer (2016).

[54] Bundesgerichtshof , VI ZR 135/13, 16 May 2017. German Federal Supreme Court confirms: Dynamic IP addresses may constitute personal data. Available at https://www.technologylawdispatch.com/2017/05/in-the-courts/german-federal-supreme-court-confirms-dynamic-ip-addresses-may-constitute-personal-data/

[55] Ned Stafford, Germany is set to introduce e-health cards by 2018, British Medical Journal, vol.31 (2015).

機微情報の取扱いに関するデータ保護が不十分である旨シュレースヴィヒ＝ホルシュタイン州コミッショナーは声明を公表した[56]。

（警察のボディカメラ）

ハンブルク州における立法の成立のほか，バーデン＝ヴュルテンベルク州をはじめとする複数の州において，警察の肩へのカメラの装着に関する法律の審議が行われている。個人の画像のビデオ録音については，対象者となる個人への情報提供を行う必要があるとともに，保存期間（ハンブルク州法では 4 日間）の設定が定められている[57]。

（適用除外）

科学的または歴史的研究及び統計目的のための処理は，管理者の処理の利益がデータ主体の処理されない利益を上回る場合には，同意なしで処理することが認められる（第 27 条 1 項）。ただし，データ主体の正当な利益と矛盾しない限り，可及的速やかに匿名化されなければならない（第 27 条 3 項）。

（未成年者の保護について）

未成年者のデータ保護に関する規定は，連邦コミッショナーの任務の一つとして，特に児童への措置について格別の留意を行う規定が存在する（第 14 条 2 項）。また，未成年者のデータ保護専用の特設サイトを設けるなど広報啓発を行っている[58]。

2017 年 11 月 20 日，ドイツネットワーク機関は，5 歳から 12 歳までの児童の保護者に対し，いわゆるスマートウォッチが児童を取り巻く環境を聴き，データを送るシステムであり，プライバシー侵害となり得るため，使用を禁ずるため破壊するよう声明を公表した[59]。

③　目的外利用の状況

個人データはデータが収集された時の目的にのみ利用することが認められる（第 14 条 1 項）。ただし，次に掲げる場合には，他の目的のために個人データの蓄積，修正または利用が認められる（第 14 条 2 項）。

・法律の規定がある，または必ずそのことを推定している場合
・データ主体が同意した場合

---

[56] Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, E-Health-Gesetzentwurf ist für ULD enttäuschend, 16 Januar 2015. https://www.datenschutzzentrum.de/artikel/861-E-Health-Gesetzentwurf-ist-fuer-ULD-enttaeuschend.html

[57] Dennis-Kenji Kipker, Transparency Requirements for Police Use of Body Cams, European Data Protection Law Review, vol.3 (2017) p.98.

[58] https://www.youngdata.de/#

[59] Bundesnetzagentur, Press release: Bundesnetzagentur takes action against children's watches with "eavesdropping" function, 17 November 2017. Available at https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2017/17112017_Verbraucherschutz.pdf?__blob=publicationFile&v=4

・データ主体の利益になることが明白であり，かつ，他の目的を知った時に同意を与えない理由が存在しない場合
・不正確な事実があるため，データ主体による確認が行われるべき事項
・データ主体が目的の変更に伴う優越する正当な利益を有しておらず，データが一般にアクセス可能であり，または管理者が公表することを認めている場合
・共通の福利や公共の安全への脅威にとって実質的損害を回避するために必要である場合
・刑事罰または行政罰の訴追のために必要な場合
・他者の権利の重大な侵害を回避するために必要な場合
・データ主体の利益を実質的に上回る研究プロジェクトにおける科学研究等の実施のために必要な場合

なお，ドイツでは，オープンデータの専用サイトを政府が公表している（https://www.govdata.de）。もっとも，NSA の監視活動が明らかになり，ドイツではプライバシーへの脅威になるとの指摘がある[60]。

（データ保全）

ドイツでは，テロ対策のための通信履歴の保全に関する法律が 2006 年 12 月 31 日に施行された[61]。連邦刑事庁，連邦警察，州刑事庁，連邦及び州の憲法擁護官庁，軍事防諜局，連邦情報局並びに税関刑事庁においてテロ組織の加入者支援者等のデータを共有する仕組みである。対象となるデータは，氏名，性別，生年月日，出生地・国，身体的な特徴，言語，写真のほか，通信端末機の番号等，電子メールアドレス，銀行口座，登録車両，家族状況，民族，宗教，爆薬等に関する知識である。2016 年 6 月時点で約 15000 人が登録されていた。連邦憲法裁判所は，2013 年 4 月 24 日，テロ対策のデータベースの基本的枠組みそのものは合憲と判断したものの，緊急で例外的な場合を除き，対象機関におけるデータ共有が情報自己決定権への重大な侵害となると判断した。

その後，EU 司法裁判所において，データ保全指令の無効判決[62]が下され，ドイツのテロ対策データベース法が 2015 年に改正された。保存の対象となる通信を，固定電話，携帯電話，インターネット電話・通信（電子メールは除外）に限定し，また通信履歴の保存は 10 日間，また携帯電話及びインターネットの通信開始場所に関する情報は 4 週間に限定された。

---

[60] Carlo Piltz, Open Data & Privacy, https://www.stiftung-nv.de/de/projekt/open-data-privacy
[61] 渡辺富久子「ドイツにおけるテロ防止のための情報収集」外国の立法 269 号（2016）24 頁以下，参照。
[62] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238.

④　本人関与の仕組み

（同意）

同意はGDPR第7条における条件と同様ではあるものの，旧法では，同意を提供しなければ，契約上の恩恵が得られない状況の下では，かかる同意は無効とされる，と規定されていた（第28条3項）。データ主体への不利益を伴うプライバシーポリシーは民法によっても無効とされうると考えられてきた。

また，マーケティング目的でEメール等を配信する場合は，管理者の利用目的への同意とは別にEメール等の配信について再度同意を取得する「ダブル・オプトイン」が奨励されてきた[63]。

（スマートテレビ）

2015年9月，ドイツのすべての州の監督機関は，スマートテレビに関するガイドラインを採択した[64]。このガイドラインに従えば，スマートテレビにおける個人データの処理は，法令で認められるかまたは本人の同意がない限り認められない。テレメディア法に基づき，利用者に関するデータや利用者サービスのデータの処理は法令上の根拠に基づき処理が認められるが，コンテンツデータの処理についてはデータ保護法の対象となり，本人の同意が必要となる。ガイドラインでは，スマートテレビを通じて自動的にURLへの接続を行うのではなく，「赤いボタン（Red Button）」を押して利用者に選択を与える方法を奨励している。

（データ主体の権利）

GDPRとほぼ同様の規定ではあるが，前述のとおり一部修正がされている。

⑤　救済措置の仕組み

（監督機関による救済）

監督機関は連邦議会，連邦政府及びその他の公的機関等に対して勧告することができる（第14条2項）。また，連邦コミッショナーがデータ保護法に違反したと認定した場合，GDPR第58条2項b号～g号，i号及びj号の権限を行使する前に，法的または技術的事項について権限ある機関に通知することができる（第16条1項）。

公的機関による自動処理によりデータ主体に害悪を生じさせた場合，当該機関は過失の有無にかかわらず，130,000ユーロ以内の賠償責任を負うものとされている（第8条1項・3項）。

行動規範については，たとえば2011年ドイツ産業界（BITKOM）が作成した位置情報サービスの行動規範を拒否する決定を行なった。また，2015年，ベルリン州監督機関は位置

---

63 Axel von dem Bussche & Paul Voigt, Data Protection in Germany 2d ed. C.H. Beck, 2017, p.12.
64 Sebastian Schweda, German Data Protection Authorities Issue Privacy Guidelines for Smart TV Services, European Data Protection Law Review, vol. 2. p.108 (2016).

情報サービスに関する行動規範を認める決定を下した。

（訴訟による救済）

2016 年 2 月 17 日，一定の資格を有する消費者団体が消費者の個人データの収集，処理及び利用に関する規則に違反した場合，差止請求を求める集団訴訟を認める法律が制定された [65]。また，2010 年 11 月には，通信の秘密に関する規則違反で通信会社のチーフ情報担当者が 3 年半の禁錮刑に処せられた事案もある [66]。

⑥ 罰則

GDPR 施行前の連邦及び州のコミッショナーによって科された罰則の例は次の一覧表のとおりである [67]。州ごとに異なるようであるが，たとえば，ベルリン州の 2015 年年次報告書によれば，37 件の制裁金または警告及び制裁金を科しており，その総額は 4 万ユーロとなっており，さらに 22 件の刑事訴追事件がある。ハンブルク州では，2015 年に 14 件に制裁金を科しており，バイエルン州では，2015－16 年の年次報告書によれば，173 件の調査を行い，内 52 件に制裁金を科している。

なお，2017 年 12 月 19 日，ドイツのカルテル庁は，フェイスブックの第三者からのソースによる個人データの取扱いが支配的地位の乱用にあたるおそれがあるとともに，データ保護法に違反するおそれがあるとの予備評価を下した [68]。

バーデン・ヴュルテンベルク州：146 万ユーロ（2008 年）	スーパーマーケットにおける社員の私生活，財政状況及び労働者の行動を体系的に監視し，データ保護責任者を任命しなかった。2009 年にはノルトライン・ヴェストファーレン州監督機関からも制裁金が社員の健康データの不正入手について科された。
ベルリン州 110 万ユーロ（2009 年 10 月）	鉄道会社が労働者の電子メールを大規模に監視していた。
ノルトライン・ヴェストファーレン州：12 万ユーロ（2010 年 5 月）	金融機関がセールス目的で外部の機関に顧客の口座情報へのアクセスを認めていた。

[65] Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts available at http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Verbesserung_zivilrechtlich_verbraucherschutz_Vorschriften_Datenschutzrecht.html （ドイツ語）

[66] Monika Kuschewsky, Germany, op. cit.

[67] Monika Kuschewsky, Germany, op. cit.ほか，ウェブニュース記事に基づき作成。

[68] Bundeskartellamt, Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive, 17 December 2017. http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html;jsessionid=FAB7BD6064269E0CDA891D29F2819F43.2_cid378?nn=3591568

ハンブルク州：20 万ユーロ（2010 年 11 月）	金融機関が外部の機関に顧客の同意なしに口座情報へのアクセスを認めていた。
ハンブルク州:5 万 4000 ユーロ（2012 年）	自動車レンタル会社が GPS を通じて顧客の知らないところで顧客を追跡していた。この会社は処理者との間にサービス提供の契約も締結していなかった。
ハンブルク州：14 万 5000 ユーロ（2013 年）	ストリートビューの車両の WiFi データから違法に個人データを収集，保存していた。
シュレースヴィヒ・ホルシュタイン州：7 万ユーロと 3 万ユーロ（2013 年）	適切な技術的組織的措置を講じていなかったため，患者のセンシティブデータを含む約 3600 の文書が非営利の精神病患者受入れ団体からインターネット上に漏えいした。
ラインラント・プファルツ州（2014 年）：130 万ユーロ	健康保険会社がダイレクトマーケティングの規則に違反した。
バイエルン州：1 万ユーロ（2015 年）	オンラインショップ企業が顧客の E メールアドレスを違法に共有していた。
ハンブルク州：（2016 年）	セーフハーバー決定に基づきアメリカ企業が個人データの移転を行っていた。

⑦ 監督機関の権限

（連邦コミッショナーの組織）

職員数は 2016 年で 110 名（2015 年は 90 名）。2017 年には 160 名に増員予定。

予算は，2016 年で 1370 万ユーロ（約 18 億円：2017 年 12 月のレート）（2015 年は 930 万ユーロ（約 12 億円：2017 年 12 月のレート））[69]

（執行）

連邦コミッショーによる制裁金の例はなし。

（相談件数）

2016 年度，連邦コミッショナーは 10,386 件の問い合わせを受け付けた（書面 3,699 件，電話 6,687 件）[70]。ホームページの訪問者数は約 2126 万件となっている。

⑧ 個人データの第三国の移転に関する憲法裁判所の判決

2016 年 4 月 20 日，ドイツ憲法裁判所は，連邦刑事庁が秘密の監視装置から収集した個人データを海外の公的機関等への移転に関する判決を下した。憲法裁判所判決によれば，個

[69] Tätigkeitsbericht zum Datenschutz p.185
[70] Tätigkeitsbericht zum Datenschutz

人データを受領する第三国の機関において同一の法制度が整備されていることを要求するものではないが，第三国の機関による裁量判断の問題にならないよう，法の支配に照らし，基本権としての保護が及ぶよう個人データの取扱いへの必要な保護が必要とされる。

具体的には，個人データの国際移転については，i 移転され，処理されることとなるデータの十分に重要な目的の制限があること，ii 第三国における利用が法の支配と合致することの信頼があること，iii ドイツの機関による処理への効果的な統制が及ぶ保証があること，かつ，iv これらの要件がドイツ法において明確な規範に基づいていることの 4 つの要件が示された[71]。また，憲法裁判所は，第三国におけるデータ保護の合理的な水準の必要性として，EU 司法裁判所の Schremes 判決，欧州人権裁判所の Zakharov v. Russia 判決，市民的及び政治的権利に関する国際規約，世界人権宣言，そして国連 2013 年 12 月のデジタルプライバシーに関する決議を考慮に入れるべきであることを言及した。

（参照条文）

2017 年規則 2016/679 及び指令 2016/680 のデータ保護適合法（英訳版を翻訳）（抄）

第 3 条　公的機関による個人データの処理

公的機関は，管理者から付与された官吏の責任を負いまたはその権限行使のための任務の遂行に必要な限りにおいて，個人データの処理が認められる。

第 5 条　公的機関におけるデータ保護責任者

⑴　公的機関は，データ保護責任者を任命しなければならない。このことは，競争入札に参入する第 2 条⑸にいう公的機関に対しても適用されるものとする。

⑵　組織の構造及び規模を考慮に入れて，一人のデータ保護責任者が複数の公的機関に対して任命されてもよいものとする。

⑶　データ保護責任者は，専門的資質，特にデータ保護の法律と実務に関する専門知識及び第 7 項にいう任務を遂行する能力に基づき任命されなければならない。

⑷　データ保護責任者は，公的機関の職員またはサービス契約に基づく職務を満たす者であることとされる。

⑸　公的機関はデータ保護責任者の連絡先を公表し，連邦データ保護情報公開コミッショナーに通知しなければならない。

第 20 条　司法救済

⑴　行政裁判所への救済は，EU 規則 2016/679 第 78 条 1 項及び 2 項に従い，自然人または法人と連邦または権利が関係する州の監督機関との間の紛争に対して提供されるものとする。

⑵　行政訴訟手続法は，本条 3 項から 7 項に従って適用されるものとする。

---

[71] German Federal Constitutional Court Judgment, 20 April 2016 (BVerfGE 141, 220) para 329. 本判決の概要について，Christopher Kuner 教授（ブリュッセル自由大学）からドイツ語の翻訳を判決のポイントについて整理していただいた。この場を借りて御礼申し上げる。

⑶　第 1 項に従う手続のため，第一審は，各監督機関の地区が位置する行政裁判所が地方において権限を有するものとする。

⑷　第 1 項に従う手続のため，第一審に監督機関が関与する権限を有する。

⑸　第 1 項に従う手続の当事者は，第一審において，⑴原告もしくは申立人として自然人または法人及び⑵被告として監督機関とする。

⑹　いかなる予備審理も行われてはならない。

⑺　権限または法的主体に関して，監督機関は行政訴訟手続法の第 80 条 2 項第 1 文 4 番に従い命令の即時強制をすることができない。

第 23 条　公的機関による他の目的のための処理

⑴　公的機関の個人データについては，次のいずれかの場合に職務の遂行にとって必要な処理が認められ，収集されたデータの目的以外の目的で個人データを処理することが認められるものとする。

（ｉ）明らかにデータ主体の利益になり，他の目的を知り得たときにデータ主体が同意を拒否すると推定する根拠がない場合，

（ii）情報が不正確であると考える理由によりデータ主体により提供された情報を確認するために必要な場合，

（iii）共通善への実質的害悪または公共の安全，防衛もしくは国土の安全への脅威を防止し，共通善の実質的関心事を守り，または税並びに税関収益を確保するために必要な場合，

（iv）刑事上または行政上の罰則を訴追し，刑法第 11 条 1 項 8 号にいう罰則もしくは措置または少年法にいう教育的措置もしくは規律措置を執行し，または罰則を科すために必要な場合，

（ｖ）別の者の権利への深刻な害悪を防止するために必要な場合，または

（vi）データ主体の正当な利益と矛盾しない限りにおいて，管理者の監査または組織的検査の実施，監督及び監視の権限を行使するために必要な場合。このことは，管理者による研修及び試験を目的とした処理にも適用されるものとする。

⑵　データが収集された目的以外の目的のための EU 規則 2016/679 の第 9 条 1 項にいう個人データの特別類型の処理は，前項の条件を満たしかつ，EU 規則 2016/679 第 9 条 2 項に従う例外または第 22 条の例外が適用される場合に認められる。

第３　フランス

１　フランスの公的部門における個人情報保護制度の概要

（１）背景・経緯

①　背景

1970 年，フランス民法第 9 条において，「すべてのものは私生活尊重の権利を有する」と規定された私生活尊重の権利が保障されて以降，人格権が発展してきた。また，刑法においても私生活尊重の権利への侵害行為を処罰する規定が設けられている。判例上，明確な私生活の定義は確立されていないとされるが，一定の条件を除き，私生活に関する情報の公表・伝達は，個人の私生活の侵害として基本的にはすべて民法第 9 条違反となり得ると説明される[72]。

1978 年，フランスでは，公権力による個人情報の乱用を防止することを狙いとして，情報処理，情報ファイル及び自由に関する法律が制定された[73]。この法律第 1 条は，情報処理が，人間のアイデンティティ，人権，私生活，または個人の自由ないし公的な自由を侵害するものであってはならない，と規定している。そして，2015 年デジタル共和国法により，「何人も自己に関する個人情報の利用を決定またはコントロールする権利」が 1978 年法の第 1 条に明文で追加された。

②　経緯

フランスにおいては，身分制社会の歴史があり，プライバシー保護は一定の身分を有する者にのみ手厚く保障されてきた経緯があり，すべての国民が享受し得る権利として，私生活尊重の権利をもとに発展してきた。

1970 年代初頭「サファリ（SAFARI）（Système automatisé pour les fichiers administratifs et le répertoire des individus）」と呼ばれるプロジェクトの下，国家統計局（Institut national de la statistique）が社会保障番号（Numéro d'Inscription au Répertoire）を個人識別のための排他的な道具として用い，教育，軍隊，医療，税，雇用等に関係する他の行政機関とのデータ・マッチングを可能とさせることとなった[74]。

このような行政機関が保有する個人のファイルの自動処理の進展に伴い個人 の自由が脅かされるという国民の危惧が高まり，スウェーデンのオンブズマンをモデルにして，1978 年の情報処理，情報ファイル及び自由に関する法律が制定されるとともに新たな独立行政機関として情報処理及び自由に関する全国委員会（Commission nationale de

---

本稿の執筆にあたり，ルブルトン・カロリーヌ（法政大学大学院博士課程）さんからの多大な支援を受けた。ここに記し，謝意を申し上げる。

72 大石泰彦『フランスのマスメディア法』（現代人文社・1999）211 頁，参照。

73 フランス個人データ保護法の制定経緯については，Lebreton Caroline「フランスにおける個人情報の保護制度の変遷」法政大学大学院紀要 79 号（2017）179 頁以下，参照。

74 「フランス人狩り」とも呼ばれ，行政による個人情報保護侵害の危険性が指摘された。清田雄治「フランスにおける個人情報保護法制と第三者機関」立命館法学 2005 年 2・3 号（2005）146 頁，参照。

l'informatique et des libertés（以下，「CNIL（クニール）」という。））が設立された。2004 年には，EU データ保護指令に対応するため，CNIL の権限強化等を含めた法改正が行われた。主な改正内容として，CNIL の義務違反の管理者に対する，警告発出（45 条），150,000 ユーロを上限とする金銭的制裁（5 年以内に違反が繰り返された場合は，300,000 ユーロが制裁金の上限）（47 条），さらに他国に設置された管理者に対する捜査権限（48 条）などが整備された。

また，フランスでは SAFARI 事件により，行政機関における個人情報の共有への規制が厳格に規律されてきた。そのため，個人データ保護を図りつつ，イノベーションの促進やオープンデータ等への課題に対処するため，2015 年にはデジタル共和国法が公布された。同法には，未成年者の忘れられる権利など新たな権利も規定されている。

そして，2017 年 12 月 13 日，法務省は，GDPR に対応するための法律案を公表した。2018 年 1 月時点，本法案について議会における審議が行われる見込みである。

（2）年表

1970 年	フランス民法第 9 条（私生活尊重の権利）が制定
1978 年	情報処理，ファイルおよび自由に関する 1978 年 1 月 6 日の法律成立
1992 年	新刑法典の導入に伴う 1978 年法の処罰規定の改正
2004 年	EU 指令に対応するため全面改正（8 月 6 日）CNIL 権限強化
2015 年	デジタル共和国のための法律
2017 年	GDPR に対応するための法律案の公表（法務省・12 月 13 日）

2　GDPR 施行に向けたフランスの公的部門に関する法整備等の状況

（1）概要

①　2015 年デジタル共和国のための法律の概要

（経緯）

2016 年 10 月 7 日，フランスでは 2016-1321 号法律（以下，「デジタル共和国法」という。）が公布された[75]。当初提出されたデジタル共和国のための法律案は，手段としてのデジタル技術に関連する利用者の権利及び将来の利用を規定することを目的としている。イノベーションの開放，権利の平等，すべての者にアクセス可能なデジタルの友愛，そして国を現代化させるための模範となることを趣旨として法案が整備されてきた。

この法案審議の過程において，初めてオンライン国民参加を実現させ，デジタル国務院（Conseil national du numérique）によるインターネット利用者に対する直接的な調査が実施された。意見の募集期間は 2015 年 9 月 26 日から 10 月 18 日までの 3 週間であり，この期間に約 2 万 1000 人が参加し，8492 件の意見が寄せられた。

---

[75] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. 本法律の概要については，ルブルトン・前掲注，参照。

デジタル共和国法の公布により，1978 年法の一部が改正されることとなった。

（概要［公的部門との関連について］）

デジタル共和国法は，4 編・113 条から成る。第 1 編情報知識の通信（1－39 条），第 2 編デジタル社会における権利保護（40－68 条），第 3 編デジタルへのアクセス（69－109 条），第 4 編外国に関する規定（110－113 条）がある。

公的部門に関連する事項としては，オープンデータへのアクセスに関する規定（第 40 条）がある。行政機関の間で，公共的サービスのため，他の行政機関が収集した情報を収集の目的以外においても利用することが可能とされた。この規定により，各行政機関は従来それぞれ情報を収集してきたが，相互接続まではいえないものの，個人情報の提供や共有をすることが容易になる，という指摘がある[76]。他方で，個人情報を保護する観点からは，行政行為に判断基準が，機械の自動処理によるアルゴリズムによってなされる場合，国民への通知義務があること（第 4 条），また，国民からの申請により，処理のルールと適用の特徴の説明に応ずることとされている。

デジタル共和国法により，地方自治体法の改正も行われ，それぞれの地方自治体にも個人データ保護に関する一定の権限を有することとなった。地方自治体法の改正に伴い，個人情報ファイルの移動が想定される。旧（地方自治体）個人情報処理責任者には，情報移転の対象になる個人情報の特定，移転の必要なセキュリティの確保，個人情報の対象である本人に対する移転の通知・説明や個人情報のアーカイブ化または削除といったそれぞれのステップを経るべきである。個人情報処理責任者になる地方自治体にとって，移転された情報のセキュリティの確保，移転された情報処理の請負業者の特定やその請負契約の更新手続き，個人情報の対象になる本人に対する通知や権利の説明，CNIL に対して行うべき手続きを行うことといったステップが示されている[77]。

（その他の個人情報保護に関連する規定）

デジタル共和国法には，「自らの個人データに関する決定しコントロールする権利」が規定された（「情報処理はすべての国民のためのものである。その発展は国際協力の下に行うべきである。人格，人権，プライバシー及び公的並びに個人の自由に侵害してはならない。本法が規定する条件の下，何人も，自らの個人情報の利用をコントロールまたは決定する権利を有する」（第 1 条）。いわゆる情報自己決定（l'autodétermination informationnelle）の権利が明文化された。ドイツにおける情報自己決定権が由来であり，人間がデジタル環境における主役となり，人間による最終決定に基づきデータが取り扱われることを趣旨としていることが示されている[78]。

---

[76] ルブルトン・前掲注，参照。

[77] CNIL, Réforme territoriale et protection des données, 22 juillet 2016 https://www.cnil.fr/fr/reforme-territoriale-et-protection-des-donnees

[78] CNIL, Rapport d'activité 2016, p.40.

デジタル共和国法は，1978 年法を一部改正する形で，透明性を担保するための措置（55 条，1978 年法 31 条），未成年者の忘れられる権利（63 条，1978 年法 40 条），死者の個人情報の保護（63 条）や交際解消後における交際中に同意を得て入手した写真・情報等の第三者への提供の制限（67 条）などがある。

また，消費者法を改正する内容として，データポータビリティ権（消費者法典 224-42-1 条）や利用者への説明義務（49 条）の新たな規定が設けられた。データポータビリティ権については，「消費者は，いかなる状況においても，自らの情報に対するポータビリティ権を有する」（消費者法典 L.224-42-1）ことが規定され，「ポータビリティの詳細手続は欧州連合の 2016 年規則第 20 条による」（消費者法典 L.224-42-2）こととされた。

フランスの集団訴訟については，必ずしもそのような制度が担保されているわけではなく，法案と比較すると，消費者保護法に直接かかわる規定が削除された。もっとも，消費者保護団体の訴訟能力に関する規定として，①プライバシーや個人情報の保護を目的とする団体，②個人情報処理が消費者に影響を及ぼす場合に，消費法に従って承認された消費者の保護を全国に代表する団体，③情報処理は労働者に影響を及ぼす場合に，労働組合，④この民事訴訟を行う目的で結成された団体は共通の個人情報保護訴訟を提起することができると規定された（43 条文［ter（第 3 版）］）。

② GDPR 施行に向けた法律案の公表

フランス法務省は 2017 年 12 月 13 日，GDPR 施行に向けた法律案を公表した[79]。5 編 24 条から成る。その概要は次のとおりである。CNIL はこれに先立ち，政府に対して，2017 年 11 月 30 日，法律案への意見を公表している[80]。なお，CNIL の意見において，GDPR の施行に伴い，1978 年法の規定との重複がある場合には GDPR の規定が優先され 1978 年法の規定が無効となるため，1978 年法の法形式が分かりにくく，全面改正が必要であることが指摘された。

（CNIL の権限に関する規定［1～7 条］）

CNIL が，ガイドライン作成や行動規範の作成の奨励，健康データへの追加安全管理措置，認証の提供，高度なリスク処理業務に関する事前相談，GDPR 及び国内法に基づき裁判所に提訴する権限，他の機関との協力などが改正事項として含まれる。

また，制裁金については，処理の差止について，一日につき 100,000 ユーロの制裁金を科す権限が追加された。

---

[79] Projet de loi relatif à la protection des données personnelles (JUSC1732261L). https://www.legifrance.gouv.fr/affichLoiPreparation.do;jsessionid=A4D5CFD18BC7602F5D962D9B53D71361.tplgfr41s_1?idDocument=JORFDOLE000036195293&type=contenu&id=2&typeLoi=proj&legislature=15

[80] CNIL, Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978.

さらに，個人データの越境移転については，CNIL が国務院[81]に対して，データの移転停止の命令と，十分性決定その他欧州委員会によるデータ移転の措置に関して EU 司法裁判所への適法性の提訴を要請する権限が改正として検討されている。

（GDPR の補足［8～19 条］）

データ侵害通知義務が免除される場合（国土の安全，防衛，公共の安全への脅威となる情報など）[82]のリスト作成のための今後政令が制定されるべきこと，同意に関して未成年者の年齢を 16 歳とすること（15 歳にするべきであるという議論がある），健康データの処理について詳細な規定が必要であること，疫学目的または社会介護の目的の利用の承認手続（自己認証，CNIL からの事前許可），アルゴリズムをコントロールすることを条件とした行政機関による自動処理決定などが改正事項として示された。

（個人情報保護法［20 条］）

1978 年法の改正，GDPR の適用に関する一貫性の確保に関して規定がある。

（その他の規定［21～24 条］）

1978 年法の改正手続に関するその他の雑則が規定された。

（２）年表

2015 年 12 月 9 日	デジタル共和国法の法案提出（閣議決定）
2016 年 1 月 26 日	国民議会（下院）可決（元老院における修正を受けて，7 月 20 日に可決）
2016 年 9 月 28 日	元老院（上院）可決（デジタル社会のための法案と名称変更）
2016 年 10 月 7 日	2016-1321 号法律が公布

３　GDPR 施行前の公的部門に関する個人情報保護制度の運用実態等

（１）概要

①　公的部門を規律する法律

情報処理，情報ファイル及び自由に関する法律（1978 年，2004 年指令対応の改正）

上記の法律のほか，公的部門については，2014-2019 年軍隊の訓練に関する法律（2013

[81] 国務院(Conseil d’État）は，政府が法律案や政令案などを準備する際に，政府から 諮問を受けて答申を行うとともに，行政最高裁判所の機能も有しており，国務院は，国，地方公共団体，行政施設などの行為に対する最終審裁判所でもある。

[82] CNIL との協議を経て，国務院による政令により，GDPR34 条のデータ主体へのデータ侵害の連絡に関する特例を設けることとする。すなわち，この特例には，不正アクセス等によるデータ主体に通知することで，国土の安全，防衛，または公共の安全にリスクをもたらす可能性がある場合を含むこととする（施行法案第 15 条）。

年 12 月 18 日）がある。

② 公的部門を監督する機関

情報処理及び自由に関する全国委員会（CNIL）

委員長及び 16 名の委員から構成される合議制の独立委員会[83]。

委員長：Isabelle FALQUE-PIERROTIN（2011 年 9 月から現在に至る）

1960 年生まれ，HEC 経営大学院修了後，文化庁及び国務院（政府諮問機関並びに行政最高裁判所の役割を担う機関）での公務を経て，2009 年 2 月内閣により任命され副委員長に就任，2011 年 9 月から委員長（前任はフランス上院議員 Alex Turk）。2014 年 1 月再任。Falque-Pierrotin 委員長は，データ保護プライバシーコミッショナー国際会議及び第 29 条データ保護作業部会においてもそれぞれ委員長の職を務めている（2018 年 1 月現在）

委員の構成は，4 名国会議員（2 名国民議会，2 名上院），2 名経済社会環境審議会，6 名裁判官，5 名の公人（1 名国民議会，1 名上院，3 名内閣）である。任期は 5 年で，再選可能であるが 10 年を超えてはならない。

1958 年憲法第 20 条 2 項では，政府は行政を司ることを規定していたため，独立行政機関の政府への帰属に関する合憲性が問題となる。フランス憲法院では独立行政機関の合憲性について正面から争われたわけではないが，先例からすると，CNIL の独立行政委員会の違憲性の判断を導くことはできないという指摘がある[84]。

③ GDPR に向けたガイドライン等

CNIL は，2017 年 3 月 15 日，GDPR に向けた 6 つのステップを公表した[85]。

i パイロット役であるデータ保護責任者を設置する（公的機関の場合は必須，現行法の CNIL ）
ii 現在行われている個人情報処理活動や担当しているファイルなどをマッピングする（組織内における個人データ処理に関するサービスと業務への連絡，データリストの一覧表の作成，各処理業務におけるデータ処理者の特定，データの移転先とその期間）。
iii これからの活動の優先順位などを決定する（利用目的の制限，データ処理の適法性，既存のプライバシーポリシーの見直し，また，特別の注意点として，特別類型のデータ，体系的な大規模モニタリング，EU 域外へのデータ移転が列挙）。

83 独立行政委員会（autorité administrative indépendante）は，「本質的に基本的人権と経済活動にかかわる部門において，独立規制の組織を設置するという要請に応えたもの」であり，「独立性を理由として，行政内部で特別な地位を占めている」。P. ウェール /D. プイヨー著，兼子仁・滝沢正訳『フランス行政法』（三省堂・2007）36-37 頁。

84 清田雄治「フランスにおける『独立行政機関（les autorité administrative indépendante）』の憲法上の位置」立命館法学 2008 年 5・6 号（2008）130 頁。

85 CNIL, Règlement européen：se préparer en 6 étapes, 15 mars 2017.
https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

iv　リスク管理する。個人情報の処理・管理の際に生じる侵害のおそれやセキュリティの問題を把握し，それに関する適当な対応をとる（2015 年 CNIL のプライバシーインパクトアセスメントに関するガイドライン)。
v　内部プロセスを整理する（処理業務におけるデータ保護原則の設計，労働者の意識向上，データ主体からの苦情申し立ての対応，CNIL のデータ侵害通知の所定用紙（72 時間以内に通知）及び CNIL の認証ラベルへの申請)。
vi　適法性を証明するため文書（処理に関する文書，情報提供に関する文書，責任・契約に関する文書）を確保する。

上記 ii のファイルマッピングに関する CNIL が用意した一覧表は次のようなものである。

処理の内容	
名称	
番号	
作成日	
更新日	

関係者	名称	住所	国
管理者			
データ保護責任者			
代表者			
共同管理者			

処理の目的	
主目的	
副目的 1	
副目的 2	
副目的 3	
副目的 4	
副目的 5	

安全管理措置	
技術的措置	
組織的措置	

対象となる個人データの類型	説明	保有期間
地位，ID，番号データ，画像等		
私生活（ライフスタイル，家族構成等）		
経済的財政的情報（収入，財政状況，納税状況等）		
接続データ（IP アドレス，ログ等）		
位置データ（旅行，GPS，GSM 等）		

センシティブデータ	説明	保有期間
人種または民族的出自を明らかにするデータ		
政治的意見を明らかにするデータ		
宗教的哲学的信仰を明らかにするデータ		
労働組合の組合員であることを示すデータ		
遺伝データ		
自然人を特有の方法で識別する目的の生体データ		
健康データ		
性生活または性的志向に関するデータ		
前科または犯罪歴に関するデータ		
国の識別番号（NIR）		

対象となる個人の類型	説明	保有期間
類型 1		
類型 2		

受領者	説明	受領者の類型
受領者 1		
受領者 2		
受領者 3		
受領者 4		

EU 域外への移転	受領者	国	保護措置	文書へのリンク
移転先 1				
移転先 2				
移転先 3				
移転先 4				

（処理者の支援のためのガイド）

CNIL は，2017 年 11 月 27 日 GDPR の施行に向けて処理者向けのガイドを公表した（18 頁）。内容は GDPR における対象者，現行法と GDPR との違い，GDPR における義務，対策の手順等から成る。何から始めるべきか，として手順を示している箇所では，①データ保護責任者の任命の必要の有無の確認（公的機関は任命が必要），②現在の契約の分析と改訂，③処理業務の記録の作成が示されている。また，外部契約をする場合のモデル契約条項を公表している。

（データ侵害通知義務に関するガイド）

CNIL は，2017 年 7 月 26 日，ISO / IEC 27035 に基づき，データ侵害通知義務に関する手順を公表した [86]。その手順の内容は，①計画と準備（インシデントの管理手順作成），②検出と報告（インシデントと検出ツールによる監視），③インシデントの評価，④インシデントへの回答，⑤再発防止策である。

なお，個人データの漏えいの内容により，コンピューターセキュリティーのための国家機関や地方の保健所にも同様の通知が必要となる。

（データ保護影響評価に関するガイドライン）

CNIL は，2017 年 12 月から 2018 年 1 月にかけて，GDPR 第 35 条におけるデータ保護影響評価の実施ツールとして，一連の文書及び無料のソフトウェアを公表した [87]。データ保護影響評価については，①新たな処理の立ち上げ，②処理の検討，③プライバシーリスクの評価，④リスクへの対処の 4 段階でそれぞれチェック項目が示された。

（パスワードに関する勧告）

CNIL は，2017 年 1 月 19 日付の決定においてパスワードに関する勧告を採択した [88]。管理者は，適切な保護措置（34 条）及び委託者の監督（35 条）の責任を負っているため，その一環としてパスワードに関しては，ⅰパスワード単独で利用する場合は，最低限 12 文字とし，大文字，小文字，数字，特殊文字を含むこと，ⅱアカウント保有者によるアクセスの場合は，最低限 8 文字とし，4 種類の文字の中から 3 種類を含め，アカウント制限を設けること（1 分間で 5 回以上また 24 時間ごとに最大 25 回の打ち間違えの場合のタイムアウトの設定），ⅲパスワードと追加情報を必要とする場合は，最低限 5 文字とし，認証の追加情報（7 文字以上と IP アドレス等の技術パラメーター）に加え，アカウント制限を設けること，ⅳ認証が対象の個人の端末である場合，最低限 4 文字とし，SIM カード等のハードウェアデバイスを用い，かつ 3 回以上連続で認証を失敗した場合の制限を設けること，が示された。

（アルゴリズムと人工知能における倫理問題）

CNIL は，2017 年中にアルゴリズムとプロファイリングにおける倫理的問題に関するセミナーを開催し，45 回の討論において約 3000 人が参加した。CNIL は同年 12 月 26 日に

---

[86] CNIL, Notifications d'incidents de sécurité aux autorités de régulation : comment s'organiser et à qui s'adresser ?, 26 juillet 2017.

[87] CNIL, The open source PIA software helps to carry out data protection impact assessment, 29 January 2018. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

[88] CNIL, Deliberation no. 2017-012 of 19 January 2017 on the adoption of a recommendation relating to passwords. また，CNIL では，安全管理措置に関するガイド（LA SÉCURITÉ DES DONNÉES PERSONNELLES）や委託先に関するガイド（GUIDE DU SOUS-TRAITANT EDITION SEPTEMBRE 2017）をそれぞれホームページで公表している。

報告書を公表した[89]。同報告書において，アルゴリズムと人工知能がもたらす 6 つの懸念は次のようにまとめられる。i 実質的な選択を自動的に導くことで，自律的機械が自由意思と責任への脅威がもたらしうること， ii 機械学習のアルゴリズムが個人や集団に対して偏見，差別及び排除を生み出す可能性があること，iiiアルゴリズムによるプロファイリングによるパーソナライゼーションが可能になる一方で，政治的文化的多様性などの集団的恩恵への脅威を導きうること， iv 人工知能を推進する一方で大規模なデータファイルが生み出されることに伴い，データ保護法における新たなバランスが必要となること，v データの質，正確性，関連性があり，偏見がないものというデータの選別の課題が生じること，vi 人間と機械との交差がみられる中，人工知能時代における人間のアイデンティティの再考が求められていること，である。

そして，報告書では，2 つの基本原則が示された。すなわち，第 1 に，利用者の利益がいかなる場合においても中心に据えるべきであるとする「忠誠（loyauté）の原則」と，②デジタル社会における進化する技術への疑問を持ち続け継続的な啓発が必要であるとする「警戒（vigilance）の原則」である。そして，この基本原則を基に，以下の 6 つの政策勧告が示された。

i　アルゴリズムのシステムに関与するすべてのプレイヤーへの啓発の促進，アルゴリズムによる危険をすべての者が理解し得るデジタルリテラシー
ii　既存の権利の強化と利用者との仲介の在り方の再考により，アルゴリズムシステムを分かりやすいものとすること
iii　「ブラックボックス」効果を防止するため，アルゴリズムシステムのデザインの改善
iv　アルゴリズムを監査するための国のプラットフォームの創設
v　倫理的人工知能に関する研究のインセンティブの向上及び研究プロジェクトの立ち上げ
vi　企業における倫理委員会の創設，グッドプラクティスの共有，倫理規程の改正等による倫理観の向上

（サイバーセキュリティ対策について）

サーバーセキュリティ基準は，CNIL ではなく，政府が設定したものであり，一般的なセキュリティ基準が定められている。近時のサイバーセキュリティに関連する事例として，オンラインの行政手続が完了したサイトの URL のアドレスを変更すると他の個人の情報にアクセスできる状態にあったため，安全管理措置違反を理由に web edition 社に対し CNIL が 25.000 ユーロの制裁金を科した例がある[90]。

---

[89] CNIL, Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, décembre 2017.
https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
[90] CNIL, Délibération n°SAN-2017-012 du 16 novembre 2017.

（2）各項目の分析

① 適用対象機関

1978 年法には対象となる行政機関が列挙されているわけではないが，公的部門については，各省及び基礎自治体（コミューン）などが規律の対象となると理解されてきた。なお，大統領府及び内閣は行政機関には含まれていない(行政と国民の関係に関する法典第 3 条)。また，司法機関に対しても 1978 年法の適用は及ばず，司法行政機関法典に基づく判例のオープンデータ化が行われている。

② 保護対象データの範囲

（保護の範囲）

個人データとは，直接的または間接的に識別されたまたは識別することが可能な自然人に関する情報を意味する。識別の可能性については，管理者が用いるあらゆる手段を考慮に入れる必要がある。

IP アドレスが個人データに該当し，データ保護法が適用されるか否かについて争われていたが，民事，商事，労働及び刑事の各訴訟におけるフランスの最高裁判所にあたる破毀院は 2016 年 11 月 3 日, EU 司法裁判所の判断に従い, 個人データに該当することとされた[91]。

＜スマートスピーカー＞

スピーカーとマイクを備えた自動音声アシスト機器のスマートスピーカーについて，CNIL は，ⅰ家庭内での子どもとの会話が記録されていることの喚起，ⅱ話を聞かれたくないときには電源をオフにしておくこと，ⅲゲストなどの第三者への周知，ⅳ子どもにはフィルタリングまたは初期設定でオフにしておくこと，の注意喚起を行った。また，CNIL は，ダッシュボードにアクセスして会話の履歴の削除をすることを推奨している。さらに，CNIL はスマートスピーカーの利用とプライバシー保護に関する質問を受け付けている[92]。

（要配慮個人情報）

ⅰ 機微情報

民族出自，政治的・哲学的・宗教的意見，労働組合への所属に関する情報，健康若しくは性的生活に関する個人情報を処理された保存システムへの記入または保存については，本人の同意なしに許されない。ただし，教会及び宗教的・哲学的・政治的・労働組合の機関は構成員の自動化された名簿を作成することが認められる（第 8 条)。

生体情報について，CNIL は機微情報として扱い，2016 年 6 月 30 日にアクセス制限に関する決定を公表した[93]。決定では，未成年者からの生体情報の収集禁止，生体情報の最大

---

[91] Cour de cassation, civile, Chambre civile 1, 3 novembre 2016, 15-22.595.
[92] CNIL, Enceintes intelligentes : des assistants vocaux connectés à votre vie privée, 5 décembre 2017.
[93] CNIL, Délibération n° 2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de

で 5 年間までの保存期間，収集した生体情報の暗号化による保存義務等が示された。2016 年に CNIL は 5,754 件の生体情報の取扱いについて対応を行った [94]。

ⅱ　公共の安全

行政活動の一つとして，国民（市民）の治安を守ることがあり，そこに，最も重要とされているテーマとして，防犯・監視カメラの設置とそのデータである。カメラの設置には，届け出が必要な場合とそうでない場合が示されている（たとえば，公道や一般に公開されている場所では届け出は不要，店舗，行政機関，住宅団地において一般に公開されていない場所への設置は届け出が必要）[95]。また，学校におけるカメラの設置には，プライバシーポリシーを定めたうえで，学生，保護者，教職員への周知を行い，最大で 1 か月間の保存期間を遵守することを喚起している [96]。

また，基礎自治体（コミューン）における犯罪予防を目的とする対象となる個人の監視のための届け出 [97]や，刑事捜査の強力のための公衆の場で利用可能な WiFi のトラフィック情報（IP アドレス，接続日時，時間等）の保存に関する説明（保存に関する義務などの説明と条文のリンク）を公表している [98]。WiFi サービスの提供者は，1 年間トラフィック情報を保全するとともに，法律で定められた司法当局の手続のためであればこの情報を提供することとされている。

さらに，CNIL は，顔認証カメラによる匿名性へのリスクなどを含むスマートシティにおけるプライバシー保護に関する政策文書を公表してきた [99]。

（オープンデータとの関係）

フランスでは，公的部門の情報を最低限加工した利用可能なデータとしてのオープンデータ専用のサイト（data.gouv.fr）が設けられ，2017 年現在 2 万以上のデータセットが公表ⅴされている。オープンデータは，すべてが個人情報の保護と直接関係するものではないが，

---

dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique; Délibération n° 2016-187 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable du traitement.

94 CNIL, Rapport d'activité 2016, p.25.

95 CNIL, Des caméras autorisées ou déclarées ?, 21 juin 2012. https://www.cnil.fr/fr/des-cameras-autorisees-ou-declarees

96 CNIL, La vidéosurveillance – vidéoprotection dans les établissements scolaires, 4 mai 2016. https://www.cnil.fr/fr/la-videosurveillance-videoprotection-dans-les-etablissements-scolaires

97 CNIL, Autorisation unique AU-038. https://www.cnil.fr/fr/declaration/au-038-prevention-de-la-delinquance-par-les-mairies

98 CNIL, Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations ?, 28 septembre 2010. https://www.cnil.fr/fr/conservation-des-donnees-de-trafic-hot-spots-wi-fi-cybercafes-employeurs-quelles-obligations

99 CNIL, Smart city et données personnelles : quels enjeux de politiques publiques et de vie privée ? 12 octobre 2017. https://www.cnil.fr/fr/smart-city-et-donnees-personnelles-quels-enjeux-de-politiques-publiques-et-de-vie-privee

情報の公表と再利用の際に，再識別の可能性が拡大しており，個人情報とプライバシーに特別な配慮をしなければならない。また，行政におけるアルゴリズムの利用の際に，透明性の原則を徹底的に適用しなければならない。

オープンデータに関する CNIL のサイトにおいて，オープンデータに関する一般的な説明と個人情報保護との関係の説明がされている[100]。CNIL は，公的情報へのアクセス権と個人情報の保護のバランスをいかに図るかという問題があり，なお透明性の観点からオープンデータに対する期待が大きいとする。しかしながら，個人情報の対する侵害のおそれが存在するため，適切な対策を備えるべきであると指摘される。具体的に司法のオープンデータとエネルギーに関するオープンデータが紹介されている。

オープンデータに関しては一般的な体制として，行政資料の公開を規定した 1978 年 7 月 17 日法律（CADA 法）とデジタル共和国法がある。CADA 法により，情報の公表と情報の再利用が規定された。また，デジタル共和国法により，行政に関する情報の公開の前提要件として 3 つが定められた。それらは，①明示的な立法の存在，②個人情報の対象である本人の同意，あるいは③情報の再特定性が不可能であること（完全匿名性）である。すなわち，デジタル共和国法により，私人による行政機関への請求に基づく情報提供から，行政機関による情報提供サービスの規律へと情報提供の仕組みが変更されたことが指摘されている。今後，行政機関による情報提供において，情報の秘匿性および再利用におけるデータ保護が重要になるため，CNIL と CADA という専門的な機関の権限が強調され，CNIL-CADA の合議体委員会が設定された[101]。

③　目的外利用の状況

1978 年法において，利用目的の制限については，「特定され，明示され，かつ正当な目的」（第 6 条 2 項）においてのみデータが収集されることとされている。当初の目的と整合しえない方法により事後的な処理もまた禁止されている。また，犯罪，前科および安全に関連する個人データの処理は，裁判所，公的機関及び公共サービスを管理する法人がそれらの管轄においてのみ利用することとされている（第 9 条 1 項）。

原則的に，地方団体が処理・管理している個人情報を他の行政的機関に提供することができない。しかし，例外的に法律が定める場合には，この限りではない。情報提供に該当する

---

[100] CNIL, Open data : la protection des données comme vecteur de confiance, 29 août 2017. https://www.cnil.fr/fr/open-data-la-protection-des-donnees-comme-vecteur-de-confiance なお，フランスの行政文書へのアクセスに関する委員会（Commission d'acces aux documents administratifs（CADA））については，井上禎男「フランスにおける個人情報保護第三者機関の機能と運用」人間文化研究 5 号（2006）155 頁以下，高橋信行「情報公開法と権利救済（1）・（2）」国学院法学 43 巻 2 号・3 号（2005）63 頁以下・1 頁以下，参照。

[101] 第 1 回の会議が 2017 年 10 月 5 日に開催され，今後オープンデータパックが作成されると報告された。CNIL, Première réunion du collège unique CADA-CNIL : une approche conjointe de la donnée publique, 24 octobre 2017. https://www.cnil.fr/fr/premiere-reunion-du-college-unique-cada-cnil-une-approche-conjointe-de-la-donnee-publique

ためには，請求は参考条文を列挙したうえで，文書，識別または識別可能な人を対象にし，全ファイルを対象とすることができないこと，限定された請求及び提供請求の対象情報が明らかな請求でなければならない。また，現在，個別法に認められる提供が認められる機関としては，租税機関，社会福祉機関，司法・検察・警察に関わる機関，執行官，またはその他の行政目的の利用（例えば，高齢者連帯手当）がある。

＜地方公共団体における公道駐車のナンバープレート番号に関連する説明責任とガバナンス＞

CNIL は，2017 年 11 月 14 日，地方公共団体におけるナンバープレート番号の監視について説明責任と良きガバナンスに関する勧告を発出した[102]。2014 年 Mapam 法により，各自治体において公道における違法駐車の監視と罰金を科すことが認められるようになった。情報処理の特定された目的に関する情報収集の合理性や必要性の原則から，幅広く読み取るシステムを避けて，ナンバープレートに制限的な読み取り範囲を設定しなければならないこと（ナンバープレートの自動読み取りの禁止），また保存期間は，違法な駐車ではないと確認されたのちまたは一般料金に従う罰金の支払いが済まされたら直ちに削除するか，違法の恐れがある場合には，現場確認においてしか保存が認められないことなどが勧告に示された。

④　本人関与の仕組み

（同意）

同意の形式が指定されているわけではないが，機微データの処理については，データ主体の明示の同意が必要とされる。労働者のメールアドレスを利用してダイレクトマーケティングを行う場合，ビデオ監視および労働者のメールならびにインターネットの監視を行う場合にも明示の労働者の同意が必要となる。

（データ主体の権利）

いかなる自然人も，正当な理由により個人データの処理に異議申立をすることができる（第 38 条）。また，個人はデータ管理者に対し，自らが処理の対象となっているか否かについて確認を得ることができ，要請をすれば個人データのコピーを入手することができる（第 39 条）（デジタル共和国法では，未成年者の「忘れられる権利」が明文化）。さらに，証拠を提供することにより，各人は自らの個人データを訂正し，完全にし，更新し，ブロック（遮断）し，または消去することができる（第 40 条）。

ただし，情報へのアクセスと訂正については，国土の安全，防衛，公共の安全についてはこの限りではない（第 41 条）。

---

[102] CNIL, Réforme du stationnement payant：les recommandations de la CNIL, 14 novembre 2017. https://www.cnil.fr/fr/reforme-du-stationnement-payant-les-recommandations-de-la-cnil

＜クッキーの設定＞

クッキーの設定については電子プライバシー指令を反映する形で 2012 年 4 月 26 日の規則と 2013 年 12 月 5 日の勧告（no. 2013-378）[103]がある。CNIL は，2014 年末にウェブサイトにおけるクッキーの調査を行い，利用者への十分な情報を提供せずに，同意の手続に違反の恐れがある 20 のウェブサイトに通知を行った [104]。また，2016 年には，「オプトイン」が徹底され，同意の撤回とともにクッキーが消去され，新たなクッキーによる追跡が行われているか否かマーケティングを行っているウェブ企業に対しても監視を開始したことを CNIL は公表した [105]。

＜不正確なクレジット情報の訂正・消去＞

2017 年 1 月，クレジット会社が 38 329 人分のクレジット情報が不正確に保存されていたことが明らかになり，CNIL は現地調査を実施の上，これらの不正確なクレジット情報の訂正・削除を行うよう警告を発した [106]。

＜ポストバカロレアシステムにおけるアルゴリズムの決定＞

教育システムにおける名簿や個人情報ファイルが多いため，届け出制度が定められている [107]。その中には高等教育機関事前登録システム（ポストバカロレアシステム）について，高校，志望校，家庭状況の 3 つの基準に基づき，完全に自動化されたプログラムによって判断が下され，人間の介入なしにアルゴリズムのみにより志願者への入学の合否に影響を及ぼす決定を下すこととされていた。

CNIL は，2017 年 8 月 30 日付決定において，このシステムが個人データの自動処理により個人の行動を評価し法的効果をもたらしており，かつ，自らのアイデンティティに関して質問し異議申立を行う権利を侵害しており，1978 年法第 10 条，同法第 39 条 1 項 5 号に違反するため認められない旨，CNIL から高等教育省に対する勧告を公表した [108]。

高等教育省における APB プラットフォームが変更され，新たなシステムのためのプラットフォームを作成したこと（Parcours up），アルゴリズムについて出願者への情報提供を行うこと，さらに個人の救済への対応が図られるようになったこと，の改善が行われたため，

---

[103] CNIL, Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978
[104] CNIL, Cookies et autres traceurs : premier bilan des contrôles, 30 juin 2015.
[105] CNIL, Cookies: CNIL extends monitoring beyond website publishers, 27 July 2016.
[106] CNIL, Délibération de la formation restreinte SAN - 2017-001 du 26 janvier 2017 prononçant un avertissement public à l'encontre de la société CARREFOUR BANQUE.
[107] CNIL, Questions-réponses sur Base élèves 1er degré, 30 septembre 2010
https://www.cnil.fr/fr/questions-reponses-sur-base-eleves-1er-degre
[108] CNIL, Décision n°2017-053 du 30 août 2017
https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000035647959&fastReqId=1454859097&fastPos=1

2018 年 1 月 18 日，CNIL は 1978 年法に基づく勧告手続を終了することを公表した[109]。

＜WhatsApp から Facebook への個人データの移転＞

2016 年 8 月，ソーシャルメディア WhatsApp は Facebook に買収され，これにより WhatsApp は利用者の行動分析をもとに個人データを移転することを決め，利用規約の改定を行った。2017 年 11 月，CNIL は，この利用規約の改定について，利用者からの有効な同意がないこと，かつ処理の正当な利益がなくデータ処理の適法性がないことを理由に違法であると判断し，調査を開始したが，この調査に WhatsApp が協力しなかった点についても違法であると通知した[110]。今後調査を行い，違法性の有無の判断を行う。

⑤ 救済措置の仕組み

CNIL は，データ保護法に違反した思料した場合に，調査を行い，違反行為への警告などとともに制裁金を科すことができる。

警告（avertissement）は，対審手続を経て発出され，制裁としての性格を有すると規定されている。この警告に基づき，一定の期間内に CNIL は違反行為を止めるよう督促することができ，また緊急の場合には，この期間を 5 日以内に短縮することができる（第 45 条 1 項)。また，個人データ処理が自然人の権利及び自由を侵害するものである場合，CNIL は当事者からの聴聞を行った上で，国務院の命令に基づく緊急手続きに従い次の 3 段階の措置をとることができる。すなわち，①最大で 3 か月間処理の中断を決定すること，②この中断に関する命令を発出すること，及び③最大で 3 か月間処理の停止を決定し，首相に是正措置を取るよう通知することである（第 45 条 2 項)。

CNIL の職員は，午前 6 時から午後 9 時までの間に検査の対象となる個人データ処理が行われた場所，住居，その周辺，設備への立ち入りが認められている。ただし，立入検査への異議申立があった場合，緊急の場合または証拠の隠滅の恐れがある場合を除いて，裁判所の許可が必要となる（第 44 条)。

なお，個人データへのアクセスに関する紛争が生じた場合の立証責任は，データ管理者により思い責任が課されることが規定されている（第 40 条)。

＜Google 検索結果の非表示に関する救済プロセス＞

たとえば，フランスでは検索エンジンに表示される検索結果がプライバシー侵害となる場合，検索事業者が削除に応じないことを理由にデータ主体は CNIL への救済を求める仕組みがある。2016 年，検索エンジンにおける非表示の苦情申し立ては 410 件となっている。

---

109 CNIL, Délibération n° 2018-011 du 18 janvier 2018 portant avis sur un projet d'arrêté autorisant la mise en œuvre d'un traitement de données à caractère personnel dénommé Parcoursup (demande d'avis n° 2134634).

110 CNIL, Décision n°MED-2017-075 du 27 novembre 2017
Décision n° MED-2017- 075 du 27 novembre 2017 mettant en demeure la société WHATSAPP.

CNIL は，2016 年 3 月 10 日，Google に対し，削除の対象を EU のドメインのみに限定していることなどを理由として，100000 ユーロの制裁金を科した[111]。対象となった検索結果における個人データは，ⅰ政治的意見に関わるビデオ，ⅱ宗教的意見に関わる記事，ⅲ起訴されたことに関する記事，ⅳ性犯罪の刑事裁判に関わる記事であり，1978 年法の異議申立権（38 条）及び訂正権（40 条）に基づく訴訟である。これに対し，Google が CNIL の決定に不服申立を行い，裁判所において審理が行われた。国務院は，2017 年 2 月 24 日付けで EU 司法裁判所への判断付託決定を行い，本件は 2017 年 7 月 19 日，EU 司法裁判所に判断を付託された（2018 年 1 月現在係争中）[112]。

EU 司法裁判所に付託された事項は次の 8 点である。

ⅰ　検索エンジンの処理責任者の義務は特殊で，他の処理責任者に適用される処理の禁止は同様に適用されるか。

ⅱ　ⅰが肯定的に回答された場合，その義務が削除請求に従う義務として解すべきか。

ⅲ　その場合，検索エンジンはその義務に関わる禁止例外を主張できるか。

ⅳ　EU 裁判所の先例は，メディアや芸術などのための禁止例外を検索エンジンに適用されないとしたが，リンクされたもの自体がそれに該当する場合に，間接的その主張ができるか。

ⅴ　ⅰが否定的に回答された場合，特に検索エンジンの責任・権限・処理可能範囲を考慮し，その適用の効果が通常とは異なると評価される場合，指令が定めるいかなる義務を負うか。

ⅵ　先例において，適法なコンテンツであっても，削除請求権を認めた。ただし，直ちに違法なコンテンツの場合は，処理責任者に削除義務が生じるか，あるいは請求権の対応において一つの要素として考えるべきか。また，指令の適用範囲外（管轄外）の場合は，その違法性の基準をどのように解すべきか。

ⅶ　ⅰに肯定的・否定的に回答されたことにもかかわらず，特に個人情報が不十分または不正確・実行した情報の場合は，削除請求の対象となるか。

ⅷ　裁判の結果に関する情報を提供することが，処理の権限が限定される情報に該当するか。

＜コネクティドトーイに関する救済プロセス＞

消費者団体が，児童の質問にマイクで回答をすることができる 2 つのインターネット接続された玩具（ロボットと人形）に対して，安全管理が不足していることの警告を発出し，CNIL の委員長はこの警告を基に 2017 年 1 月と 11 月にこの玩具を製造した香港にある企

---

111 CNIL, Right to be delisted: the CNIL Restricted Committee imposes a €100,000 fine on Google, 24 March 2016. https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google

112 Conseil d'Etat, 19 juillet 2017, GOOGLE INC. N° 399922. http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC

業に対して調査を行った。調査結果を基に，CNIL は 2017 年 12 月 4 日，これらの玩具が，ｉ 9 メートル以内にいる者が標準的な Bluetooth を通じてこの玩具に接続できる状態であったことから安全管理措置違反であり，また ii 玩具が個人データの処理について通知を行っていないこと，かつこの企業が EU 域外の第三国に個人データを移転していたことを通知していないことから情報提供の違反である旨通知した。この通知に対する措置が行われない場合，この企業に対して制裁金を科す手続に入ることを公表した [113]。

（情報自由委員 CIL［Correspondants Informatique et Libertés］の設置［GDPR 施行後におけるデータ保護責任者］）

EU データ保護指令の下では，情報自由委員（CIL）の設置が任意であった。しかし，GDPR 第 37 条に基づき，行政機関には，データ保護責任者の設置が義務付けられる [114]。2017 年 7 月下旬時点，地域圏の三分の二，県の半分，大都市の三分の二，都市的なコミュニティの三分の一，都市圏コミュニティの十分の一と基礎自治体（コミューン）の 2%のみが CIL を設置している [115]。

CIL の設置によるメリットは，管理者におけるデータ処理の適法性の確保，情報処理セキュリティ確保，情報処理手続の簡略化，CNIL への連絡役，法令遵守の論証，情報的財産の価値向上につながると説明されてきた。

（認証ラベル）[116]

個人情報処理の際に，個人情報が十分に保護されているか否かを周知すること自体が，個人情報処理の責任者や個人情報の対象である本人にとって有益である。そのため，CNIL は 2011 年から認証ラベルの発行を開始した。認証ラベルは，管理者にとって，競争における優位，信頼性の証明，他のプレイヤーとの差別化，責任ある行動の証明，GDPR の導入後の将来の規制への先取りの対応というメリットがあるとされている。認証ラベルの取得には，CNIL の所定の申請書を提出し，審査を受けて付与される仕組みである。審査には 2 カ月程度要し，申請後発行は 6 か月以内

113 CNIL, Connected toys: CNIL publicly serves formal notice to cease serious breach of privacy because of a lack of security, 4 December 2017. https://www.cnil.fr/en/connected-toys-cnil-publicly-serves-formal-notice-cease-serious-breach-privacy-because-lack-security

114 CNIL, du correspondant informatique et libertes, https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf

115 CNIL, Règlement européen sur la protection des données : comment les collectivités peuvent-elles se préparer ? https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-comment-les-collectivites-peuvent-elles-se-preparer

116 CNIL, Comment obtenir un label CNIL ?, 17 octobre 2017. https://www.cnil.fr/fr/comment-obtenir-un-label-cnil また，CNIL は認証のための内部ガバナンスに関するガイドを公表している。 CNIL, Privacy Seals on Privacy governance Procedure (2015). https://www.cnil.fr/sites/default/files/typo/document/CNIL_Privacy_Seal-Governance-EN.pdf

に行われることとされている。

2017 年現在，ⅰガバナンス・処理・自由の認証ラベル ，ⅱ教育（研修）の認証ラベル ，ⅲデジタル金庫の認証ラベル，ⅳシステム監査の認証ラベルの 4 類型の認証が存在する。なお，2016 年は 97 件の認証ラベルが発行され，13 件中 12 件の認証更新が行われた。

⑥ 罰則

CNIL は，初めての違反の事例については，最大 150,000 ユーロの制裁金を科すことができる。二度目以降の違反については，300,000 ユーロまたは前年度の売上高 5%以内で，最大 300,000 ユーロ（約 4000 万円）の制裁金を科すことができる（第 47 条)。制裁金への不服申立は，2 か月以内に国務院に対して行うことができる（第 46 条)。

さらに，CNIL は刑法（第 226 条 16 項から同条 24 項）で定められたプライバシー侵害について，検察庁へデータ保護法の違反を報告することができる。たとえば，2016 年，CNIL はモバイルアプリで個人に関するオンライン情報，写真，ビデオや噂を収集し「ゴシップ」（たとえば，10 年前に HIV に感染，14 年間アルコール依存症等）として公開していたサイト運営企業に対して，1978 年法第 1 条が規定する人間のアイデンティティへの侵害であり，かつ処理の適法性の根拠がなく違法であるとして，本件を検察庁へ通知した[117]。

行政不服の申立ての仕組みとしては，CNIL による制裁に対して，データ管理者はその報告を受け，意見を提出し，かつ口頭で CNIL の調査委員会に対し意見を表明することができる。また，CNIL の調査委員会は調査に関して寄与し得る者からも聴聞を求めることができる。ただし，データ管理者は審議には参加することができない。制裁を科されたデータ管理者は，事実と法に基づき国務院に対して申立てをすることができる（第 46 条)。

近時の制裁金が科された事例としては次のようなものがある。

150,000ユーロ（2014年）	Google Inc に対して，データ処理の条件や目的に関して利用者への情報提供やクッキーへの事前の同意への違反
50,000 ユーロ（2015 年）	視聴覚補助専門企業の安全管理措置の違反
100,000ユーロ（2016年）	検索エンジンからの非表示違反
30,000 ユーロ（2016 年）	オンライン販売企業のクレジットカード詐欺防止等の安全管理措置違反，クッキーの通知違反など
20,000 ユーロ（2016 年）	デートサイトが性生活，信条，民族的出自等のセンシティブデータの取得に明示同意を取得の違反
15,000 ユーロ（2017 年）	クレジットカード会社の安全管理措置違反，保存期間の違反，退会者のデータ消去の違反など
1000 ユーロ（2017 年）	会社の従業員の監視のためのカメラの運用について CNIL が

[117] CNIL, Décision n° 2016-079 du 26 septembre 2016 mettant en demeure la société W.M.G.

	繰り返し質問を送付したにもかかわらず, 回答せず, 調査に非協力
10,000 ユーロ（2017 年）	歯科医院が保有する医療記録への患者のアクセスを拒否し, CNIL の調査に非協力
40,000 ユーロ（2017 年）	レンタル自動車会社から約 3 万 5000 人の個人データが漏えい
100,000ユーロ（2018年）	オンラインアプリケーション会社から顧客データの数十万件の漏えい

⑦　監督機関の権限（2016 年年次報告書）[118]

（CNIL の組織）

職員数は 2016 年時点で 195 人（女性６３%，男性３７%，平均年齢４１歳）

予算は€16,964,049（約 22.6 億円（2018 年 2 月レート））

組織としては，委員長の下に，事務局長がおり，5 つの局（事業分野の一貫性確保の局，制裁に関する局，技術革新の局，広報・研究の局，総務・財政の局）のほかに EU 及び国際対応の部署がある。

（執行［2016 年］）

命令 82 件，警告 9 件，制裁金 4 件

調査 430 件（オンライン調査 100 件，監視カメラに関する調査 94 件，調査の端緒は，約 60%が CNIL の主導，約 20%がその年のプログラム，約 15%が苦情申立の調査の一環，約 5%が制裁のための調査の一環である）

（相談件数［2016 年］）

CNIL は 7,703 件の苦情を受付け，7,909 件の調査を行ってきた。苦情の内訳として，約 33%がインターネット上における個人データの拡散に関する事項，約 33%が商業目的の利用またはマーケティング利用に関する事項，約 14%が人事情報に関する事項，約 9%が銀行・クレジットカードに関する事項，約 3%が医療・介護に関する事項となっている。行政における公的自由に関する事項は約 4%となっている。

警察, 監視機関等のファイルへの CNIL を通じたアクセス要請は 4,381 件となっている。監査の対象は 8,101 件となっている。監査の内訳は，警察のファイルが 2,167 件，国家憲兵隊のファイルが 2,167 件となっている。

CNIL は，3,078 件の決定を下しており，EU 域外への移転に関する認可が 1,976 件，医

[118] CNIL, 2017 the CNIL in a Nutshell, https://www.cnil.fr/sites/default/files/atoms/files/cnil_en_bref-ven-2017-vd.pdf; CNIL, Rapport d'activité 2016, p.53-73.

療研究または介護に関する認可の 697 件等が含まれる。

（参照条文）
1978 年法（抄）
第 1 条
情報技術はすべての市民の役務のためのものでなければならない。その進展は国際協力の文脈において生ずるものである。それは，人間のアイデンティティ，人権，プライバシーまたは個人並びに公共の自由を侵害するものであってはならない。

第 2 条
本法は，個人データファイリングシステムを含むまたは含む可能性のある個人データの自動処理及び非自動処理に適用されるものとする。ただし，データ管理者が第 5 条における規定された条件を満たしており，もっぱら私的活動の行使のために実施される処理についてはこの限りではない。
個人データは，識別番号並びに一つ若しくは複数の当該自然人の特定の要因を照合することにより，直接的または間接的に識別されたまたは識別することができる自然人に関するいかなる情報を意味する。個人が識別できることを決定するため，データ管理者または他の者が用いまたはアクセスする可能性のあるあらゆる手段が考慮に入れられなければならない。
個人データの処理は，いかなる機械を用いたとしても，特に取得，記録，組織化，保全，適合もしくは改変，復元，参照，利用，送信による開示，拡散またはその他の方法で利用可能にし，配列，結合，ブロック，消去もしくは破壊を含む，当該データのいかなる処理または一連の処理を意味する。
個人データファイリングシステムとは，特定の基準に従いアクセスすることができるいかなる体系化され安定した個人データの集合体を意味する。
個人データ処理のデータ主体は，関連する処理によって対象となるデータの個人を意味する。
（略）

第 5 条
Ⅰ　本法は次の場合の個人データについてのみ適用される。
1　データ管理者がフランス領土に設置されている場合。
2　データ管理者がフランス領土または他の欧州連合加盟国には設定されていないが，フランス領土において処理の手段を用いることができる場合。ただし，フランス領土または欧州連合加盟国のいずれかの国を通じて送信する目的のみに用いられる処理はこの限りではない。

Ⅱ　本条 1 項 2 号にいう処理の目的について，データ管理者は，本法が要求する義務を履行するための代理を行うフランス領土において設置された代理人の任命を CNIL に通知しなければならない。この任命は，データ管理者に対して開始されうるいかなる法的依頼も不可能にするものであってはならない。

第 6 条

処理は，次の条件を満たす個人データに関してのみ行うことができる。

1　データが公正かつ適法に取得され処理されなければならない。

2　データは，特定され，明示され，かつ正当な目的のために取得され，この目的と整合しえない方法で事後的に処理されてはならない。しかし，統計，科学及び歴史に関する目的のための追加のデータ処理は，本章，第 4 章（データ処理に関する形式），第 5 章第 1 節（データ管理者の義務及び個人の権利），第 6 章（医療研究目的のための個人データの処理）及び第 10 章（治療の評価または分析及び防止を目的とした医療の個人データの処理）において規定された原則及び手続を遵守する形で行われ，かつデータ主体に関する決定を行わない限りにおいて，データ収集の当初の目的と整合するものとみなされる。

3　データは，取得され，かつ追加で処理される目的との関連において，適切で，関連性を有し，過度なものであってはならない。

4　データは正確で，完全でかつ必要に応じ最新のものでなければならない。取得され処理された目的との関係において不正確で不完全なデータを消去され訂正されるための適切な措置が講じられなければならない。

5　データが取得され処理される目的で必要な期間を超えてデータ主体の識別が行われる形式で保持されてはならない。

（以下，中略）

第 46 条

第 45 条第 1 項及び第 2 項 1 号に規定された制裁は，調査委員会に所属しない委員の内，委員長から任命された CNIL の構成員の一人により作成された報告書に基づき宣言されるものとする。データ管理者は当該報告を通知され，意見を提出し，また陳述し補助することができる。報告者は調査委員会に対して口頭による意見を提示することができるが，審議には参加することができない。調査委員会は，CNIL の事務局長の要請による職員を含め調査に有用に寄与しうるいかなる者からも聴聞をすることができる。

調査委員会は，決定した制裁を公表することができる。制裁を受けた当事者の費用において指定された雑誌，新聞紙またはその他のメディアにおいて当該公表を命じることができる。CNIL 委員長は，45 条 1 項 2 号の規定に基づき遵守させるため執行部に対して正式な命令を公表するよう指示することができる。委員長が 1 項 3 号において示された条件に基づき非公開の手続を宣言した時，当該非公開手続は正式な遵守命令と同様条件に基づき公

表されなければならない。

第 45 条の適用における調査委員会による決定はデータ管理者に対して通知されなければならない。制裁に対する申立は，事実及び法に基づき国務院に対してなされなければならない。

第４　アイルランド[119]

１　アイルランドの公的部門における個人情報保護制度の概要

（１）背景・経緯

①　背景

アイルランドにおけるプライバシー保護制度の起源については，憲法におけるプライバシー権の存在を背景とし[120]，個人情報保護に関する基本法としての 1988 年データ保護法の成立によって，個人情報及びプライバシー権の保護に係る制度の具体化が図られている。

アイルランド憲法（Constitution of Ireland, 1937; Bunreacht　na hÉireann, 1937）は，基本的人権としてのプライバシー権に関する単一の規定を定めるものではない。しかしながら，プライバシー権は，個人の権利として認められる数多くの権利に現れており，憲法 40 条 3 項（「国は，市民の個人に関する権利を法において尊重し，かつ，実行可能な限りで当該権利を守り擁護することを保障する」）は，プライバシー権の保護においてその中心的な役割を担ってきたということができる[121]。

「欧州人権条約（Convention for the Protection of　Human Rights and Fundamental Freedoms, 1950）」8 条 1 項は，「プライベートと家族生活の尊重の権利（Right to respect for private and family life）」について「何人も，プライベートと家族生活，家庭と通信を尊重される権利を有する（Everyone has the right to respect for his private and family life, his home and his correspondence.）」と規定し，私生活及び家族生活が尊重される権利を保障している。（なお，1988 年データ保護法は欧州人権条約に矛盾することなく解釈運用されなければならないことが 2003 年欧州人権条約に関する法律（European Convention on Human Rights Act, 2003）によって要求されている。）

1981 年に「個人データの自動処理に関する個人の保護のための条約（Convention　for the protection　individuals with regard to automatic processing of personal data done at Strasbourg on the day of January,1981）」が，締結されている。また，法改革委員会は 1988 年に「プライバシーに関する報告書」を公表している。

アイルランドにおいて，上記の条約を実施する必要性から，国内法として 1988 年データ保護法が定められた。同法は，「個人データの自動処理に関する個人の保護のための条約を

---

119 日本語の文献として財団法人行政管理研究センター「アイルランドにおける情報公開制度及び個人情報保護制度の運用実態に関する調査報告書」（http://www.iam.or.jp/data/200901dp_ireland.pdf）がある。

また，本報告書作成にあたっては，Denis Kelleher ”Privacy and Data Protection Law in Ireland (2nd ed.)“(Bloomsbury,2015)によるところが多い。

120 McGee v Attorney General [1974]IR 284,(1975) 109 ILTR 29 は，明確に憲法 41 条(家族生活の保護)が，国家によるプライバシーの侵害から守るものであると明言している。Kelleher によると，憲法におけるプライバシーの権利は，種々の側面(投票の秘密，訴訟のプライバシー，個人の自己決定，住居の不可侵等)に現れるという。

121 40 条 3 項を根拠の中心とするのは，Kennedy and Arnold v Attorney General 事件[1987] IR 587 における Hamilton 意見。上記 Kelleher 8 頁。

実施するため，そして自動的に処理される個人情報の収集，処理，保存，利用及び開示を同条約に基づいて実施するための法律」とされ（前文），附則 1 条は，同条約をそのまま収録している。

1988 年法の詳細は，第 3 で，2003 年改正法と併せて詳細に論じる。

② 経緯

その後，1995 年データ保護指令(「個人データ処理に係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95／46／EC 指令」（以下 EU 指令という）が採択，公表された。これを受けて，2003 年データ保護法が定められ[122]，同年 4 月 30 日に大統領の署名を経て，同年 7 月 1 日から施行された。

さらに，その後，「個人情報の処理及び電子通信部門におけるプライバシーの保護に関する欧州議会及び理事会指令（ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector （Directive on privacy and electronic communications））」（以下「e プライバシー指令」という。）の実施に関して，アイルランドにおいて「欧州共同体における電子通信ネットワーク及びサービス並びにデータ保護及びプライバシーに関する規則（ European Communities (Electronic Communications Networks and Services)(Data Protection and Privacy) Regulations 2003, SI 535/2003)」（以下「2003 年 e プライバシー規則」という。）が定められている。

同規則 3 条 1 項は「これら規則は，アイルランド及び欧州共同体（European Community）に関連する領域における公的な通信ネットワークについて，公的に利用し得る電子通信サービスに関する規定に基づく個人データの処理に適用される」と規定している。

その後，1988 年及び 2003 年個人データ保護法は，法に対する修正及び行政委任立法（statutory instrument）を重ねて，現在に至っている。

（2）年表

1937 年	アイルランド憲法
1950 年	欧州人権条約
1981 年	個人データの自動処理に係る個人の保護に関する欧州評議会条約
1988 年	1988 年データ保護法
1995 年	EU データ保護指令（1998 年施行）
2002 年	e プライバシー指令
2003 年 4 月	2003 年データ保護改正法　成立　7 月 1 日施行

[122] 正式には 1988 年及び 2003 年データ保護法である。2003 年改正法ひとつのものとして解釈され，2003 年データ保護（修正）法とも表記される。以下，本報告書においては，便宜上，「データ保護法」とする。

2016 年	GDPR　成立
2017 年 5 月 12 日	データ保護法案一般枠組の公表

2　GDPR 施行に向けたアイルランドの公的部門に関する法整備等の状況

（1）概要

①　データ保護法一般枠組法案（General Scheme of Data Protection Bill 2017）の公表

Tánaiste（副首相，テナイステ）は，2017 年 5 月 12 日，データ保護一般枠組法案を公表した。この枠組みは，全部で，7 部　95 条からなるものである。具体的には，以下のとおりである[123]。

（1 部－一般的規定）

1 部は，略称，開始時期，定義，規則及び現行法の廃止を取り扱う

具体的な条項としては，1 条　略称，2 条　解釈，3 条　費用，4 条　規則，5 条　廃止から成り立つ。

（2 部－データ保護委員会）

2 部は，GDPR 及び，法執行指令に対しての権限ある監督機関の設立の規定である。

具体的な条項としては，6 条　設立日，7 条　データ保護委員会，8 条　機能，9 条　メンバー，10 条　スタッフ，11 条　メンバー（ヨーロッパ議会），12 条　資金コントロール，13 条　コミッショナーの出席，14 条　情報の無権限開示の禁止，15 条　財産の移転，契約の保全，手続の休止などから成り立つ。

7 条において，データ保護一般枠組法が効力を有する日に，データ保護委員会（An Coimisiún um Cosanta Sonrai）(以下，委員会という)が設立される旨が記載されている。また，8 条 2 項において，GDPR51 条の監督権限及び 57 条・58 条の権限を行う旨が記載されている。

（3 部－GDPR に対する詳細付与規定）

3 部は，GDPR において，裁量にゆだねられている部分を確定し，その他の規定に対して，効果を与える制定法の手続を規定する。

具体的には，16 条　子供の同意，17 条　実質的な公的利益に関する特別のカテゴリの個人データの取扱，18 条　特別のカテゴリの個人データの取扱，19 条　刑事判決及び犯罪に関する個人データの取扱，20 条　データ主体の権利の行使及び管理者の義務の制限，21 条　データ保護オフィサーの使命，22 条　ＥＵ域外への移転の制限，23 条　行政当局と団体に対する行政罰金の賦課，24 条　データ取扱と表現と情報の自由，25 条　公益に関するア

[123] なお，国民議会報告書の 16 頁の解説を参照した。

ーカイブ目的のため，科学的または歴史的調査目的または統計的目的の取扱に関するセーフガード及び特例から成り立つ。

特に留意すべき事項を説明すると以下のとおりである。

17 条は，GDPR 9.2(g)条による特別カテゴリの個人データの取扱について，実質的な公益のために，一定条件のもと，大臣が委員会に諮問の上，規則を定めうることを記している。18 条は，一定条件のもと，医薬品開発のため，従業員の労働能力の評価のため，医学的診断のため，健康/社会的なのケアのためなどの目的のために，特別のカテゴリの個人データが許されうることなどを定めている。

19 条は，GDPR6.1 条などに従い，刑事判決・犯罪等に関する個人データは，不正行為のリスクの評価もしくは予防のため，規制・認証・許諾等の決定のため，不正行為・倫理違反等から生じる損害から公衆を防護するため，民事裁判の提起・防御・執行のため，等の限定された目的にのみ取扱ができることを定めている。

（4 部－法執行指令の実装）

4 部は，犯罪の防止，捜査，探知及び起訴に従事する権限ある当局その他の組織における個人データの取扱に関する法執行指令の規定を取り扱う。6 章から成り立っており，その内容は，以下のとおりである。

1 章（一般規定）

この章は，26 条　解釈，27 条　この部の適用，28 条　個人データの収集，取扱，保管及び利用，29 条　個人データのセキュリティ対策，30 条　データの質，31 条　機微な個人データの取扱から成り立つ。

4 部は，法執行機能を行う場合の公的機関における個人データ保護を取り扱う。データ保護法の廃止に伴って，この機能を行う場合の個人データ保護に伴う制定法を定める効果を有することになる。

なお，26 条において，ほとんどの定義が，GDPR の定義を採用しているが，国家安全保障の定義に関しては，ⅰ1939 年から 1998 年国家法，1976 年刑法，2005 年刑事司法（テロリスト犯罪法）などの法律に定める犯罪の予防，探知，捜査，ⅱ諜報・業務妨害・内政干渉などから国を防衛する行為，ⅲ外国の能力・意図・活動を特定する行為等などと定義しているのが興味深い。

2 章（データ主体の権利）

この章は，32 条　個人の意思決定の自動化に関する制限，33 条　情報への権利，34 条　アクセス権，35 条　取扱の修正，消去または制限の権利，36 条　データ主体とのコミュニケーション，37 条　制限事項，38 条　監督当局による間接的な権利の行使及び検証，39 条　刑事捜査手続におけるデータ主体の権利から成り立つ。

特に留意すべき事項を説明すると以下のとおりである。

32 条は，法執行指令 11 条に対応する規定であり，後述のデータ保護法 6B に匹敵する規定でもある。

33 条は，GDPR13 条に対応し，権限ある当局は，データの取扱に関する種々の情報がデータ主体に対して提供されるようにすべきとする規定である。

34 条は，GDPR14 条に対応するデータ主体のデータに対するアクセス権である。

35 条は，法執行指令 16 条に対応するものである。

36 条は，GDPR14 条に対応するものであって，33 条から 35 条に関してデータ主体に提供する情報や連絡を，簡潔で，わかりやすく，アクセスしやすい形態で，伝えなければならないとするものである。

37 条は，上記 33 条から 35 条に定める権利について，個人の生命・安全または福祉を脅かすとき，犯罪を容易にするとき，国家安全保障を損なうとき，公的・法的な調査・捜査を妨げるとき等については，遅らせたり・制限したりすることができるという規定である。

37 条による制限がなされる場合には，データ主体は，委員会による検証または審査を求めることができる（38 条）。

刑事事件の捜査・手続の過程における裁判上の決定・記録・事件ファイルにおける個人データに関しては，33 条から 35 条に定める権利は，裁判所規則による（39 条）。

3 章（データ管理者及び取扱者の義務）

この章は，40 条　データ管理者の義務，41 条　設計とデフォルトにおけるデータ保護，42 条　処理者，43 条　データ取扱活動の記録，44 条　データのログ作成義務，45 条　委員会との協力，46 条　データ保護影響評価と委員会との事前協議，47 条　取扱のセキュリティ，48 条　個人データの委員会への違反の通知，49 条　個人データ侵害とデータ主体との通信，50 条　データ保護責任者の指定から成り立つ。

4 章（個人データの第三国及び国際機関への移転）

この章は，51 条　個人データの第三国及び国際機関への移転，52 条　適切な保障措置に従った移転，53 条　特別の状況に対する例外，54 条　第三国における受領者への移転から成り立つ。

5 章（救済，責任及び罰則）

この章は，55 条　委員会への苦情申立の権利，56 条　委員会への有効な司法的救済の権利，57 条　データ主体の代理，58 条　賠償の権利から成り立つ。

6 章（独立の監督機関）

この章は，59 条　監督機関，60 条　委員会の職務，61 条　委員会の権限，62 条　相互援助から成り立つ。

59 条は，GDPR41 条に対応するもので，委員会が監督機関であることを定めている。

60 条は，法執行指令 46 条に効力をあたえるものとされ，この部の適用のモニタリングと執行を担当すること，一般の意識を向上させ，取扱に関するリスク・ルール・安全策・権利の理解を促進させること，政府関係機関にアドバイスすることなどが委員会の職務であることを定める。

61 条は，法執行指令 47 条などに対応し，委員会が，調査権限（1 項），是正権限（2 項），助言等の権限（3 項）を有していることを定める。62 条は，法執行指令 50 条に対応し，委員会は，他の監督機関と相互援助をなして，指令の規定を適用するようにしなければならない，他の監督機関からの要求に対応しなければならないとする規定である。

（5 部－データ保護委員会による監督及び執行権の行使）

5 部は，データ保護委員会の監督及び執行権限に関する規定を有している。さらに，それらの権限の行使について「手続的保護策」及び「適正手続」を提案している。捜索令状，調査，制裁，無権限の開示についての犯罪の規定を含んでいる。

1 章（一般）

この章は，63 条　解釈，64 条　通知の送達から成り立つ。

2 章（苦情申立及び執行）

この章は，65 条　データ主体の苦情，66 条　調査及び監査，67 条　権限あるオフィサー，68 条　捜索令状，69 条　情報を要求する権限，70 条　執行する権限，71 条　効果的な司法救済をうける権利，72 条　高等法院に申立がなされうる例外的状況，73 条　報告を求めうる権限から成り立つ。

3 章（調査）

この章は，74 条　調査，75 条　調査権限，76 条　権限あるオフィサーの報告から成り立つ。

4 章（制裁）

この章は，77 条　調査報告書からのアクション，78 条　協調及び一貫のメカニズム，79 条　行政罰に対する異議申立，80 条　巡回裁判所における行政罰に対する決定の確認，81 条　取扱者による無権限での開示，82 条　権限なしに取得した個人データの開示，83 条企業体における経営者による犯罪，84 条　委員会による略式犯罪の提訴，85 条　判決・制裁等の公表から成り立つ。

5 章（雑）

この章は，86 条　法的資料の非開示特権，87 条　推定規定，88 条　専門家証拠，89 条訴訟からの免除から成り立つ。

（6 部－雑則）

この章は，その他のさまざまな規定を含むものである。

具体的には，90 条　司法分野における裁判所に対する監督機関，91 条　司法救済，92 条　裁判所規則，93 条　法的非開示特権，94 条　1934 年中央銀行法における 33 条 AK の改正，95 条　EU 司法裁判所への回付の適用などから成り立つ。

（7 部－67 条における権限あるオフィサーによる口頭審問に適用される規定）

この規定は，上記に関する附則である。

②　精査報告書の公表

同 11 月には，国民議会（Tithe an Oireachtais／Houses of the Oireachtas）の司法及び平等合同委員会において，上記一般枠組法に対する精査報告書が公表されている[124]。同報告書において，重要な論点としては，法案の構造，児童の年齢及びデータ保護，制裁があげられている。

（２）年表

2016 年 4 月 27 日	GDPR の最終文言が公表される
2017 年 5 月 12 日	データ保護一般枠組法案が公表される
2017 年 11 月 23 日	司法及び平等合同委員会による報告書が公表される
2017 年 12 月 22 日	DPC が，「SME のための GDPR ガイダンス」を公表
2018 年 5 月 25 日	GDPR が完全実施

（３）データ保護コミッショナーの対応

GDPR に対するデータ保護コミッショナーの対応は，大きく，ガイダンスと意識向上活動に分けられる。

データ保護コミッショナーは，ガイダンスとして，GDPR and YOU というアニメーションなどを利用するサイトを準備しており，そこで，12 のステップにわけて，対応のためのステップを解く資料，データ保護インパクト評価についての資料，「GDPR にむけての準備－準備チェックリスト」という中小企業宛の資料（テンプレートを含む）を準備している。12 ステップの内容は，以下のとおりである。

---

124 「前立法における検討報告書（Report on pre-legislative scrutiny of the General Scheme of the Data　Protection Bill 2017）」
https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_justice_and_equality/reports/2017/2017-11-23_report-on-pre-legislative-scrutiny-of-the-general-scheme-of-the-data-protection-bill-2017_en.pdf

① 意識をもつ（Becoming Aware）
② 説明可能になる（Becoming Accountable）
③ スタッフ及びサービス利用者と連絡（Communicating with Staff and Service Users）
④ 個人プライバシー権（Personal Privacy Rights）
⑤ アクセス要求がどのように変わったか？（How will Access Requests change?）
⑥ 「法的根拠」の意味するもの（What we mean when we talk about a 'Legal Basis'）
⑦ データの取り扱い根拠としての顧客同意の利用（Using Customer Consent as grounds to process data）
⑧ 児童のデータの取扱（Processing Children's Data）
⑨ データ侵害の報告（Reporting Data Breaches）
⑩ データ保護インパクト評価及びデータ保護バイ・デザイン／デフォルト（Data Protection Impact Assessments（DPIA） and Data Protection by Design and Default）
⑪ データ保護オフィサー（Data Protection Officers）
⑫ 国際組織及び GDPR（International Organisations and the GDPR）

意識向上活動は，GDPR 意識向上活動 2017（GDPR Awareness Raising Activities 2017）といい，具体的には，会議等における講演活動，ブログ・メディア（ツイッター・WEB ページも含む）活動，29 条委員会への貢献，多様な継続的な意識向上活動などによって成り立っている。

3 GDPR 施行前の公的部門に関する個人情報保護制度の運用実態等

（1）概要

① 公的部門を規律する法律

アイルランドにおけるデータ保護に関する基本的な法律は，1988 年データ保護法(25/1988)であり，2003 年データ保護法(6/2003)によって，改正されている。1988 年及び 2003 年データ保護法称されることもある。なお，現行の法律は，2017 年 7 月 26 日の改正まで踏まえたものが公表されている [125]。

同法の構成は，序（1 条），個人データに関する個人のプライバシーの保護（2 条－8 条），データ保護コミッショナー（9 条－15 条），登録（16 条－20 条），その他（21 条－35 条），附則 1（自動取扱に関するストラスブルグ条約），附則 2（データ保護コミッショナー），附則 3（公的機関及びその他の団体・人）から成り立っている。

なお，公的機関に対しては，1988 年法 16 条（1）（a）において，データ取扱の登録に関

[125] http://www.lawreform.ie/_fileupload/RevisedActs/WithAnnotations/EN_ACT_1988_0025.PDF

する規定(データ管理者/データ処理者がコミッショナーに登録を行わなければならないとする制度)が適用されると定められ，さらに，附則 3 において，公的機関とは具体的に，政府，政府の大臣，司法長官，会計監査長官，オンブズマン等をいうと定められていた。しかし，同附則は 2003 年データ保護法によって廃止され，代わりに，情報を公に提供するために登録される場合やデータ管理者が利益のためではない組織である場合に適用されると定められるようになった[126]。

② 公的部門を監督する機関

監督する機関は，データ保護コミッショナー（An Coimisineir Cosanta Sonrai/Data Protection Commissioner）である。法的には，1988 年 7 月 13 日に通過した 1988 年データ保護法にもとづいて, 1989 年 4 月 19 日から効力を有している。データ保護法は 9 条(1)において，Coimisinéir Cosanta Sonraí というコミッショナーを置くものとしており，同（1C）において，EU データ保護指令の目的において，監督機関となるとされている。具体的な組織構成，権限等については，2（5）以降において論じる。

（2）各項目の分析

① 目的及び適用対象機関

1988 年データ保護法は，個人データの処理に関して公的部門と民間部門を分けて規定しておらず, 同法が適用されるデータについては「処理されうる状態にある情報」(information in a form in which it can be processed)（1 条 1 項）と定義づけるにとどまる。また，個人データ処理の実施機関であるデータ管理者（data controller）について「個人データ及びその利用を管理する個人ないし複数の者」（1 条 1 項）と規定している。さらに，データ登録の規定は,「公的機関, その他の団体及び個人のデータ管理者に適用される」(16 条 1 項(a))としている。

② 保護対象データの範囲

1988 年データ保護法は，上述のように「データ」については，あいまいな定め方であったが，2003 年データ保護法の改正によって，「データとは，自動処理データ（automated data）及びマニュアルデータ（manual data）をいう」（1 条 1 項）と改正された。2003 年法は，データ保護をマニュアルデータまで拡張した[127]。ここでいう「自動処理データ」は，「入力された指示にもとづいて自動的に作業をなす装置によって処理された情報又は当該装置によって取り扱われるべき情報をいう」とし，また，マニュアルデータについては,「関連ファイリングシステム（relevant filing system）の一部として記録されている情報，又は関連ファイリングシステムの一部を形成する意図のもとに記録された情報をいう」と規定

[126] 具体的な限定列挙から，性質からの広範囲な定義に変わったということになる。
[127] Kelleher 135 頁

している。

また，「個人データ」については，「そのデータから，又はデータコントローラーが保有する他の情報に関連するデータから，識別されうる生存する個人（a living individual）に関連するデータ」と規定している。

③　データ取扱根拠／データ保護に関する原則と公的機関

（データ取扱の法的根拠）

データ取扱にあたっては，法によって定められた合法的な根拠にもとづく取扱が求められることになる。この点に関する一般的な原則は，データ保護法 2 条による。

同条は，「個人データの公正な取得及び取扱」，「正確な個人データの確保」，「目的に適った個人データの取扱」及び「個人データに係る安全手段の確保」という 4 つの原則を採用している。

これらの例外としてデータ保護法 2A 条は，データの取扱が許容される場合を例示している。すなわち，

個人データは，データ管理者によって，データ管理者が本法 2 条に適合し，少なくても，以下の一つの条件に合致しない限り，取り扱われないものとする

（a）個人データの処理は，データ主体が当該データ取扱に同意した場合，または，データ主体が身体的，精神的及び年齢の理由によりその同意の性質及び効果を正しく認識できない，又は認識できそうにない場合には，当該データ主体の親，保護者等による同意がなされ，その同意が法によって禁止されていない場合であること

（b）取扱が，

（ⅰ）データ主体が当事者である契約の実施のためにデータ取扱が必要な場合

（ⅱ）データ主体の依頼により，契約に入る前の事前処理のために，データ取扱が必要とされる場合

（ⅲ）契約によって課せられる義務のほか，データコントローラーが従わなければならない法的義務の実施のために，データ取扱が必要な場合

（ⅳ）データ主体の健康に対する危害又はその他の損害を避けるためにデータ取扱が必要な場合。又は，2A 条 1 項（a）に係るデータ主体の同意又はその他の者の同意の要求がそれらの者の利益に損害を与えるような場合において，それらの者の重大な利益を保護するためにデータ取扱が必要な場合

（略）

（c）取扱が，

（ⅰ）司法の実施のためにデータ取扱が必要な場合

（ⅱ）法律によって与えられた，又は法律に基づく職務の実施のために，データ取扱が必要な場合

（ⅲ）政府又は大臣の職務の実施のためにデータ取扱が必要な場合

（iv）公益目的のために実施されるその他の公益に係る職務の実施のために，データ取扱が必要な場合

とされている。

公的な機関における取扱を考える場合には，同条（c）の規律は，参考になる。

一般的には，公的機関については，法律によって与えられた，又は法律に基づく職務があるため，その実施のために，データ取扱が必要な場合については，当然にデータ取扱が許容される（上述の（c）（ii））。また，政府又は大臣の職務の実施のためにデータ取扱が必要な場合についても，データの取扱が許容されている（上述の（c）（iii））。この場合について，アイルランドにおいて，公的機関における情報共有の問題が議論されている。データ保護コミッショナーは，社会保護省の苦情申立事例（Case Study 8/2002）において，「当該事例においては，個人データは政府機関において共有され得るものであり，かつ，共有されるべきものである。･･･それぞれの政府各部門はそれぞれの権利を持ったデータ管理者であって，政府は全般的なデータ管理者ではなく，そこには社会福祉に関する法律及びその他の法律に基づく個人データの移動に係る構造が必然的に存在している」と述べ，政府各部門における共有について法的な根拠が必要なことが明らかにされている。

この問題は，欧州司法裁判所においても，Bara and others 対 Preşedintele Casei Naţionale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate and Agenția Națională de Administrare Fiscală （ANAF）[128]事件として争われている。この事件は，ルーマニアの自営業者が，個人データが国税当局から，国家健康保険に移転されることが適法かどうかを争った事件である。これに関して，欧州司法裁判所は，2015 年 10 月に，個人データ保護指令の 10 条における公正な個人データの取扱の規定は，データ主体に対して，事前に，他の公的部門に対して個人データを移転すると伝えておくことを求めていると判断した。さらに，欧州司法裁判所は，同 11 条（1）の公正なデータ取扱の規定は，受領した機関のデータ管理者がデータ主体に対して，その名称，目的，その他必要な情報を伝えることを求めているとした。

そして，これらの事件を基に，データ保護コミッショナーは，公的部門におけるデータ共有についての短いガイダンスを公表している [129]。

その内容は，Bara and others 事件やその他の判決が，個人の権利を強化する傾向があることを踏まえ，公的機関はデータ共有を行う際，データ主体に，データの取扱いを連絡することが重要であるとするものである。データ保護コミッショナーは，さらに，個人がデータの取扱についてどのように考えているのか，個人データの利用が，公共サービスの効率性とどう関連するのか，誰が，個人データにアクセスしうるのか，誰と，どのように共有されるのか，といった事情について本人に情報が提供されるべきであると考えている。この見地か

[128] Case C 201/14 Judgement of the European Court of Justice dated 1st October 2015 concerning a data arrangement between two public bodies

[129] ”Data Sharing in the Public Sector”（https://www.dataprotection.ie/docs/Data-Sharing-in-the-Public-Sector/m/1217.htm）

ら，個人データの取扱に際しては，相当の注意をもって取り扱われるべきであり，個人データは，相当な理由なしにアクセスされたり，利用されたりしない権利を有するという。そして具体的には，公的機関は，1　正当化理由とその表示，2　明確な法的根拠，3　透明性（法，推奨事項，連絡方法，連絡者），4　認可，5　データ最小化，6　データアクセス及びセキュリティ，7　データ維持，8　ガバナンス，9　利用者とのコミュニケーションについて配慮したベストプライクティスを採用するべきとしている。

④　本人関与の仕組み

データ主体の権利として，個人データの保有目的及び保有者を知らされる権利（3 条），個人データの存在を確認する権利，アクセスの権利（4 条），個人データの訂正及び削除に関する権利（6 条）がある。

本人関与の仕組みとの関係では，公的機関の保有する個人データに対しての本人のアクセス制限の規定があり。データ保護法 5 条 1 項で，アクセス権が制限される場合を列挙している。公的な処理に関する場合は，以下のとおりである。

（a）犯罪の予防，発見又は捜査の目的のために保有されている個人データ

（b）（a）に関する目的のために取得された情報を構成する個人データ

（c）同法 4 条の適用により，刑務所，留置所，軍事刑務所，聖パトリック施設（Saint Patrick's Institution）における安全又は規律の維持が損なわれる可能性のある個人データ

（d）財政的損失から公衆を保護するために，法務大臣によって発せられた命令に基づいた職務の実施に係る目的を維持するための個人データ

（e）同法 4 条の適用が，国家の国際関係の保護の利益に反することになる場合の個人データ

（f）ないし（g）　略

（gg）職務を遂行する目的のために，データ保護コミッショナー又は情報コミッショナーが保有する個人データ

⑤　監督機関の権限と監督機関による救済

（データ保護コミッショナーの組織）

データ保護コミッショナーの組織等については，データ保護法の 9 条の附則 2（Second Schedule）が定めている。同附則は，組織体（合議制の機関）であること，その機能の行使において独立であることを定め（同 1 条），政府によって任命されること（2 条（1）），任期は，5 年を超えてはならないこと（3 条），その他の事項などを定めている。

その使命は，ガイダンス，監督及び執行を通じたコンプライアンスによってデータプライバシ権を保護することである。戦略陳述書[130]において，その使命，バリュー等が示されている。

[130] https://dataprotection.ie/documents/strategy17.pdf

なお，データ保護コミッショナーの組織図は，付録として添付した。

上級管理チーム（Senior Management Committee (SMC)）は，チーフコミッショナーである Helen Dixon[131]と 4 名のコミッショナー補からなる。現在のスタッフ数は，およそ 100 名であり，2013 年が 30 名ほどであったのに比較して，急速に増大している。また，予算も 750 万ユーロ（10 億 1250 万円相当 -約 1 ユーロ＝135 円で計算）であり，ここ数年，急速に増大している。

（執行及び権限）

データ保護コミッショナーは，データ保護法に違反する者に対して，文書でもって，期間内に該当する規定に適合するよう求めることができる（同 10 条（2））。また，その機能を実現するために必要であり，もしくは，実際的である場合には，特定事項に関して情報を提供するよう求めることができる（情報通知，同 12 条（1））。情報通知に対する不履行もしくは虚偽の事項の提供は，犯罪である（同（5））。その他，法に違反する個人データの国外への移動の禁止（11 条 7 項）(このような禁止の通知を禁止通知と呼ぶことがある)，データ処理及び登録申請に係る事前調査（12A 条 1 項及び 2 項），企業及び団体等による個人データの取扱に関する実務規範（codes of practice）の策定を促進させる権限（13 条）などの権限がある。

なお，データ保護コミッショナーの通知に対して納得のいかない当事者（データ管理者／取扱者）は，データ保護法 26 条 1 項にもとづいて，巡回裁判所（Circuit Court）に異議を申し立てることができる（なお，データ保護指令 28 条（3））。

⑥　救済措置の仕組み

（監督機関による救済）

データ主体の権利についての救済は，監督機関に専属的に帰属すると解されている。例えば，Farrell v Bank of Ireland 事件においては，ソリシタ（事務弁護士）が，本人訴訟として，データ保護法に基づく書類の提供を強制する命令を裁判所に直接求めたという事案であるが，最高裁判所は，データ保護法に執行のための手段を定められているため，裁判所が，それ以外の命令を行う権限を有していないと判断している。

データ保護についての権利侵害を受けたとき，データ主体は，データ保護コミッショナーに対して，苦情申立を行う。苦情申立が行われた際には，データ保護コミッショナーは，その申立てがとるに足らない（frivolous），濫用である（vexatious）と判断されない限りは，調査しなければならない（同法 10 条（1）（b））。

---

131 データ保護コミッショナーのホームページによると，応用言語学，経済及び公共政策等の学問を修めた後，10 年ほど IT 関係の企業に勤務。その後，労働企業革新省の上級サービスを勤めた後，2009 年よりアイルランド企業登録官を勤めた。2014 年 9 月よりデータ保護コミッショナー。
https://www.dataprotection.ie/docs/Helen-Dixon/1507.htm

（裁判所の関与）

個人データ保護に関しては，ⅰ以下に説明する刑事制裁によって，データ保護法の履行が執行される場合，ⅱ損害賠償によって執行される場合については，裁判所が関与する。

ⅰ　刑事制裁

データ保護法は，刑事罰となる行為を定めている。具体的には，以下のとおりである。

（a）第三者に対して就職，雇用または，サービスの規定に関して，アクセス要求を行うこと（法 4 条（13））

（b）執行通知における要求事項に対して遵守することを怠る，または，拒絶すること（法 10 条（9））

（c）禁止通知に含まれる禁止事項を遵守することを怠ること（同 11 条（15））

（d）情報提供通知において 要求された情報を提供することを怠る，もしくは，拒絶すること，または，意図的に，虚偽の情報を提供すること（同 12 条（5））

（e）データ保護法の 12A 条（6）に違反して取扱をすること（同 12A 条（7））

（f）データ管理者の観点から，登録の手続をなさずに個人データを保持すること（同 19 条（6））

（g）登録の手続に際して虚偽もしくは誤解を招く情報を提供すること（同 20 条（2））

（h）従前のデータ管理者の権限を用いてデータ取扱者が，開示すること（同 21 条（2））

（i）従前のデータ管理者の権限を用いて個人データにアクセスすること（同 22 条（1））

（j）データ保護コミッショナーの官吏を妨害し，または，（調査から）隠蔽すること（同 24 条（6））

（k）データ保護コミッショナーまたは，そのスタッフが，機密情報を漏洩すること（同附則 2，パラ 10（2））

データ保護法のもとでの罰金刑は，略式言い渡しで，2500 ユーロから，4000 ユーロであり，起訴事件で，10 万ユーロである。

ⅱ　損害賠償

アイルランドにおいて，データ保護法違反は，同時にプライバシー侵害をもたらすものと考えられている。しかしながら，裁判所は，憲法上のプライバシー侵害を根拠とした損害賠償については，否定的な判断を行う場合が多い（LO'K v.LH ほか）。一方，裁判所が，2003 年ヨーロッパ人権条約法 8 条(1)のもとの権利を侵害していると認定して，損害賠償を認めた事件がある（Pullen v. Dublin City Council，Sciacca v. Italy）。

データ保護法違反を根拠とする損害賠償については，データ保護法 7 条（データ主体に対しての注意義務を負うとする）に基づく，データ取扱者等の注意義務が争点となる。

この点について，最高裁判所は，Kelly v Board of Governors of St. Lawrence's Hospital

事件において，データの取扱者等は，「合理的な人間が予測すべき損害を与えることのないように合理的な注意を払う義務を負う」と述べている。

データ保護法 7 条の違反でもって直ちに損害賠償請求が認められるのかという点が争いになった興味深い事案として，Collins v FBD Insurance がある。原告は，配管工で，バンが盗まれたとして，保険を申請したところ，保険会社である被告は，原告の情報を調査し，原告が，従前に盗品を購入していたことを知り，支払いを拒絶した。原告は，被告に対して，個人データに対するアクセス要求を行ったが，被告は，これに 40 日以内に応えなかったという事案である。この事案において，データ保護コミッショナーは，40 日以内に答えなかったことが，データ主体のアクセス権を侵害するとし，また，保険の申請に関して調査を行ったことがセキュリティ原則を侵害するとした。原告は，この判断をもとに，この二つと刑事判決に関するデータの不適切な取扱による損害賠償を求めた。巡回裁判所は，1 万 5000 ユーロの損害賠償を認めたが，高等法院は，損害が認められるためには，実際に損害を被っていることを明らかにしなければならないとして巡回裁判所の判断を覆し，原告が損害を被ったという事実を証明できていないとして，損害賠償を認めなかった。

⑦　公的機関における実務規範

データ保護法 13 条は，データ保護コミッショナーが，事業者団体や組織が実務規範を準備して個人データ保護に備えるのを支援すると定めている（同（1））。そして，コミッショナーは，それを認証することができる（2）。

この規定に従って，教育実務省(Department of Education and Skills)[132]と保健省(Department of Health)[133]は，個人データ取扱に関する実務規範を公表し[134]，データ保護コミッショナーが，これを認証している[135]。

以下，保健省の実務規範を概観する。同規範は，データ保護コミッショナーから，2014 年 8 月に第 3 版の認証を受けている。同実務規範は，14 のパートから成り立っている。データは，市民のものであることが述べられ，権利は，データ保護法の神聖なものであることが述べられている(巻頭)。部門 3「制定法枠組み」では，1963 国家秘密法の枠組み，データ保護法，1997 年及び 2003 年情報自由法などが述べられ，部門 7「個人データの保有例」では，求人様式，登録様式，免許，健康専門員の履歴書などが紹介されている。部門 8「ルールと義務」では，ルールと義務としてデータ保護法の原則がルールとしてすべての個人データに適用されている旨が明らかにされ，9　「データ保護ルール」では，そのルールが具体的に論じられている。特に，ルール 3 は，個人データの開示であるが，具体的な例外に該当する事例が記載されている。具体的には，開示が許容される場合として，データ主体，また

---

132 https://www.education.ie/en/The-Department/Data-protection/pub_data_protection_code_of_practice.pdf
133 http://health.gov.ie/wp-content/uploads/2015/08/Data-Protection-Code-of-Practice.pdf
134 データ保護コミッショナーのホームページによれば，8 団体が実務規範の認証を受けている(https://www.dataprotection.ie/docs/Self_Regulation_and_Codes_of_Practice/m/98.htm)。
135 しかしながら，公的機関において実務規範を作成することが義務づけられているわけではない。

は，データ主体の代理である場合，データ主体の求めに応じる場合／同意がある場合，データ主体が，データが開示される個人／組織に気づいている場合，法または裁判所命令にもとづく場合，などと明らかにされている。

⑧　監督機関の活動の実態

監督機関の活動についての実態は，以下のとおりである（主として，2016 年年間活動報告[136]による）。

（相談件数等）

2016 年の苦情申立件数は，電子メールによるもの 15335 件，電話によるもの 16774 件，郵便によるもの 1150 件である。

調査された案件は，1479 件である。そのうち，本人によるデータアクセスの件が 56%に及んでいる。

「忘れられる権利」については，26 件の苦情申立を受理し，うち，6 件は認容され，15 件が棄却，5 件が現在調査中である。

セキュリティ侵害案件については，有効に記録されたのは，2224 件である。

また，相談は，1170 件で，2015 年の 860 件からきわめて増加している。50 件以上の監査及び調査を行っており，政府機関に対する詳細な監査も行っている。

また，データ保護の啓発・意識向上もデータ保護コミッショナーの重要な仕事の役割であり，2016 年 10 月には，ツイッターのアカウントを開設する他，年間 60 回以上の講演活動を行っている。

（2016 年におけるデータ保護コミッショナーの活動）

2016 年特別調査ユニットが設立された。この調査ユニットは，苦情申立に対する調査とは別に，みずからの判断で調査を行う。

2016 年，特別調査ユニットは，私立探偵セクター（代表的な案件は，Cowley 私立探偵の件で 61 件の違反の嫌疑があった。知り合いから社会保護省のデータを取得して，保険会社に開示した。また，それ以外に，乗用車追跡システムを尾行担当者の自動車に付着させて利用し，情報を取得した案件），手術決済システム（Surgical Symphysiotomy Payment Scheme 手術を行った場合に，その申込み書類等が，手術が終了した以降に裁断されているかを，特別調査ユニットが確認した結果，データ保護違反はなかったことが判明した），病院セクター（病院において，患者のセンシティブデータが一般からアクセス可能な場所でどのように管理されているかを調査する準備を完了，2017 年以降の調査の準備である）を調査した。

多国籍技術企業における監督も重要な問題であるとされている。年間報告書においては，

[136] https://www.dataprotection.ie/documents/annualreports/AnnualReport16.pdf

WhatsApp の問題(2014 年に，WhatsApp と Facebook が合併した際，WhatsApp のユーザーデータを FaceBook のユーザーデータと共有し，マッチングされるように利用条件を改訂したことについて，ユーザー（この件の当事者のデータは，Facebook アイルランドが保有）の同意を取得したかを調査した)や，データ保護コミッショナーが，Facebook と利用条件，利用ポリシ，製品アップデートについて意見交換を頻繁に行った経緯，また，LinkedIn との交渉（アカウントセッティングやクッキーバナーの導入に際して，有意義な意見交換を行ったこと，特にアカウントセッティングにおいては，個人データに関する設定をレイアウトと様式の点から，アクセスしやすくするようにしたこと）の経緯などが報告されている。

（具体的な公的機関の関係するケーススタディ）

年間活動報告書（2013 年から 2016 年の 4 年間）では，公的機関が関係するケーススタディとして，以下の事案が紹介されている。

・2016-8　データ処理者による個人データの第三者への開示

アイルランド郵政事業が，亡くなった配偶者との共同預金口座明細を，アイルランド国債管理庁（NTMA）に勝手に開示したとして，個人データの本人が，データ保護コミッショナーに対して苦情申立をしたものである。アイルランド郵政事業は，ミスにより開示してしまったとして謝罪の連絡を行ったが，開示を行った経緯についての詳細な説明がなかったために調査が行われたものである。調査の結果，アイルランド郵政事業が，データ処理者であって，アイルランド国債管理庁（NTMA）がデータ管理者であると考えられた。結局，アイルランド国債管理庁（NTMA）が第三者であるアイルランド郵政事業により処理させるということが明確になされておらず，データ保護法違反とされた。

・2015-6　国家組織の個人データの過度な取扱

国家組織（名称不詳）において，管理職が，従業員が自ら記載しているタイムシートとオフィス等へ入退室を管理するセキュリティカードの比較を行うとして，セキュリティのカードへのアクセスを求めたことに対して，従業員がその正当性を争った事案である。

セキュリティカードは，建物やセキュリティゾーンへの入退室の管理のみに利用されて，時間管理のためには，使われないことになっていた。この事案において，データ保護コミッショナーは，このセキュリティカードのデータは，当初の目的以外に利用されたということになると判断した。

・2015-8　社会保障省における個人情報の第三者への開示

雇用関係審判所の聴聞において，疾病手当の情報に関して申立人の指名，住所，社会保障番号，生年月日，銀行詳細が明らかにされた。省からは，この開示が誤りであったとして謝罪がなされたが，非常に迷惑を受けたとして，個人データの本人が苦情申し立てを行った事案である。データ保護コミッショナーは，この開示が誤りであった以上，その後の取扱は，当初の目的に違反する行為になるとの判断を示した。

・2014-9　農業省による過剰なデータ収集

農業省が，動物病気法の遵守という目的のために，馬の所有者に対して，口座番号の提出を求めたことに対し，馬の所有者が，飼育地の登録は別としても，銀行口座は不要であると，データコミッショナーに苦情申し立てを行った事件。データ保護コミッショナーが，データ保護法の 2（1）(c)（iii）は，個人データは，その収集目的に関して適切で，関連があって，収集目的に必要な範囲を超えないように収集されなければならないというのは，必要な時に収集することができるという意味であって，必要になるかもしれないという意味ではないということを指摘した結果，口座番号の提出は行われなくなった。

付録１　データ保護法２条

データ保護法２条は，以下のように定める。

データ管理者は，データの保有に関して，以下の規定に適合するものとする

(a) 個人データ，又は，場合によっては，個人データを構成している情報は，公正に取得／公正に取扱われなければならない。

(b) 個人データは正確かつ完全なものでなければならない。そして個人データは，必要に応じて，最新の状態に保たれなければならない。

(c) 個人データは，

（ｉ）十分かつ明確な，そして合法的な目的のためにのみ取得されなければならない

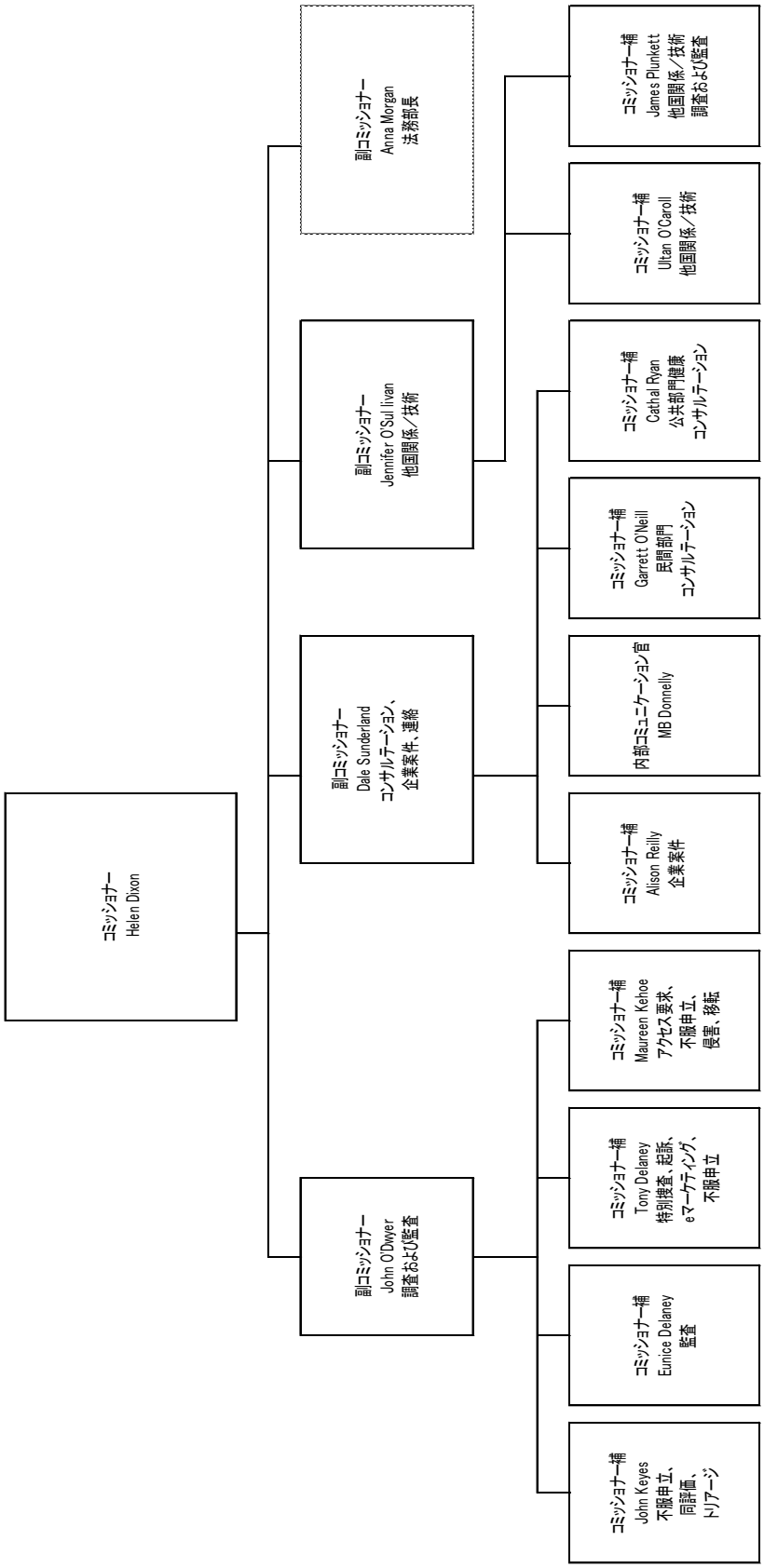
（ii）個人データは，当該目的に矛盾して処理されてはならない

（iii）個人データは，当該個人データが収集された目的又は処理される目的に関して妥当かつ関連するものでなければならず，当該目的を超えるものであってはならない

（iv）個人データは，当該目的のために必要な期間を超えて保有されてはならない

(d) 個人データに対する権限のないアクセス，あるいは権限のない個人データの改編，開示又は破壊に対して，とりわけネットワークを通してのデータ移動を含むデータ取扱の場合には，適切な安全手段が確保されなければならない。さらに，その他の違法な形態のデータ取扱に対しても，適切な安全手段が確保されなければならない。

付録 2　組織図


コミッショナー
Helen Dixon
副コミッショナー
John O'Dwyer
調査および監査
副コミッショナー
Dale Sunderland
コンサルテーション、
企業案件、連絡
副コミッショナー
Jennifer O'Sul livan
他国関係／技術
副コミッショナー
Anna Morgan
法務部長
コミッショナー補
John Keyes
不服申立、
同評価、
トリアージ
コミッショナー補
Eunice Delaney
監査
コミッショナー補
Tony Delaney
特別捜査、起訴、
eマーケティング、
不服申立
コミッショナー補
Maureen Kehoe
アクセス要求、
不服申立、
侵害、移転
コミッショナー補
Alison Reilly
企業案件
内部コミュニケーション官
MB Donnelly
コミッショナー補
Garrett O'Neill
民間部門
コンサルテーション
コミッショナー補
Cathal Ryan
公共部門健康
コンサルテーション
コミッショナー補
Ultan O'Caroll
他国関係／技術
コミッショナー補
James Plunkett
他国関係／技術
調査および監査

第５　イタリア

１　イタリアの公的部門における個人情報保護制度の概要

（１）背景・経緯

イタリア憲法（1948 年施行）は，それ自体，明示的にプライバシーの権利を定めているものではない。しかしながら，同 2 条は「共和国は，個人として，またその個性が発展する社会組織において，人間の不可侵の権利を承認し保障する。また共和国は，政治的，経済的及び社会的な連帯の絶対的な義務の履行を求める。」と定めている。この規定は，「基本的な原則（Principi Fondamentali）」と名付けられており，この不可侵の人間の権利に該当すると考えられる場合，同条に基づき憲法上保障されていると解されている。

また，同 3 条は「すべての市民は等しく社会的な尊厳を有し，性別，人種，言語，宗教，政治的見解，人格及び社会的条件の違いにかかわらず，法の前に平等である。共和国の義務は，市民の自由及び平等を事実上制限し，人間的な人格の発展とわが国（Paese）における政治的，経済的及び社会的組織におけるあらゆる労働への効果的な参画を妨げる社会的及び経済的秩序の障害を除去することである。」と定めている。プライバシーが保護されなければ，この 3 条の平等の規定の趣旨が実現されないとも考えられている。

プライバシー保護の趣旨は，他にも憲法 13 条（不可侵の権利），14 条（家庭の不可侵性），15 条（通信の自由及び秘密），21 条（表現の自由）などにも含まれているとされている[137]。

また，ヨーロッパは，世界人権宣言（1948），人権に関するヨーロッパ条約（1950），基本権憲章などにより，プライバシーに関する保護規定を発展させてきた。これらの国際法の規定が，直接的に，裁判規範性を有しているものと考えられており，それによって，法的な保護がなされてきたと考えられる[138]。

EU 指令を国内法化した「個人データの取扱に関する個人及びその他の主体の保護に関する法（no. 675/1996）（Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ）（1996 年 12 月 31 日議会通過。1997 年 5 月 8 日施行）がイタリアにおいてプライバシー保護について定めた初の法律である。それまでは，個人データ保護のために有効な制定法も法的ツールもほとんど存在しなかった[139]。

同法は，1 章　一般原則（PRINCIPI GENERALI），2 章　取扱者の義務（OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO），3 章　個人データの取扱（TRATTAMENTO DEI DATI PERSONALI），4 章　特別なデータの取扱（TRATTAMENTO DI DATI PARTICOLARI），5 章　特別枠組に従う取扱（TRATTAMENTI SOGGETTI A REGIME

---

137 以上について，Francesco Modafferi ”Lezioni Dirrritto Alla Protezione Dei　Dati Personali，alla reiserva tezza e all’identita peronale” lulu（2015）85 頁以下

138 国際法の規定の国内法的な効力については，国により異なっており，イタリアは，国際法が自力執行であることを前提としている意味で，かかるプライバシーの保護規定の中で，国内の効力を考える意味が強いものといえる。

139 例外として，労働法（law 300/1970）がある。

SPECIALE），6 章　司法手続における保護（TUTELA AMMINISTRATIVA E GIURISDIZIONALE），7 章　個人データ保護官（GARANTE PER LA PROTEZIONE DEI DATI PERSONALI），8 章　制裁（SANZIONI），9 章　経過及び最終・廃止規定（DISPOSIZIONI TRANSITORIE E FINALI ED ABROGAZIONI），10 章　財政的手当及び施行（COPERTURA FINANZIARIA ED ENTRATA IN VIGORE）からなる。公的機関に関する定めとして，4 条　公的部門における特別の取扱，27 条　公的主体による取扱があるのが注目される。

その後，2001 年法番号 127（データ保護法延期法），2002 年電気通信プライバシー指令，2003 年法番号 14（ヨーロッパ共同体法）などへの対応などから，プライバシー保護に関する規定を一つの法典にまとめることとなり，2003 年個人データ保護法典（Codice in Materia di Protezione dei Dati Personal）が定められるに至った。この詳細は，第 3 で分析する。

（2）年表

1948 年	イタリア憲法
1996 年 12 月 31 日	個人データの取扱に関する個人及びその他の主体の保護に関する法（no. 675/1996） 成立
1997 年 5 月 8 日	同　施行
2001 年 3 月 24 日	個人データの取扱に関して法による権限行使の期限を延期する法
2002 年	電気通信プライバシー指令
2003 年	ヨーロッパ共同体法
2003 年 6 月 30 日	個人データ保護法典　成立

2　イタリアにおける GDPR のための対応について

（1）GDPR のための対応について

イタリアにおける公的部門での GDPR 対応について，政府／議会における対応と監督機関（情報コミッショナー）における対応とにわけて概観する。

（2）政府／議会における対応について

2018 年 1 月末現在，イタリア政府において，GDPR に対応する法制定の動きは存在しない。

また，特定の分野に関する GDPR への対応としては，議会において，予算法 101 条 2 項に基づく，予算措置がなされている。

（3）データ保護官における GDPR 対応について

イタリアのデータ保護官（Grante per protezione dei dati personali）は，そのホームページにおいて，GDPR－情報シート（Regolamento europeo in materia di protezione dei dati personali - Pagina informativa）という GDPR 対応のため情報サイトを準備している[140]。

当該サイトでは，EU の個人データ保護規則に関連する情報ページや犯罪防止等における個人データの処理に関する指令のいわゆるデータ保護パッケージのページ[141]，GDPR の行政罰（administrative fines）の適用と前提・データ侵害通知・自動的意思決定・データ保護インパクト評価に関して，それぞれ 29 条委員会ガイドラインへのリンク，監督機関概念・データポータビリティの権利・データ保護オフィサーの紹介とそれぞれの 29 条委員会ガイドラインへのリンク，GDPR のテキストが準備されている。これらは，基本的に EU の制度の簡単な解説もしくは，29 条委員会のガイドラインに対するリンクを準備するものである。

また，イタリア独自の解説として「個人データ保護の欧州の規則についての新しいガイド（Guida al nuovo Regolamento Europeo in Materia Protezione Dei Dati Personali ）」，「EU 規則－公的行政当局のためのプライバシ保護イニシアチブ（Regolamento Ue: al via l'iniziativa del Garante privacy per le Pubbliche amministrazioni)」，「ヨーロッパデータ保護規則枠組みの適用についてのガイド（Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali)」が公開されている。

また，2017 年 12 月 15 日には，公的機関におけるデータプライバシーオフィサーについての FAQ（Nuove Faq sul Responsabile della Protezione dei dati （RPD）in ambito pubblico）が公表されている。

（個人データ保護の欧州の規則についての新しいガイド）

このガイドは，全部で，15 ページからなり，GDPR のポイントを簡易に解説している。具体的な項目は，市民のさらなる保護（Cittadini più　garantiti)，処理における明確かつ完全な情報（Informazioni più chiare e complete sul trattamento)，同意（オンラインにおける保護の手段）（Consenso, strumento di garanzia anche on line)，自動的データ処理における管理権限の制限（Limiti alla possibilità per il titolare di adottare decisioni solo sulla base di un trattamento automatizzato di dati)，忘れられる権利についてのさらなる保護と自由（Più tutele e libertà con il diritto all'oblio)，データポータビリティ／より開かれたデジタル市場へのデータ移転の自由（Portabilità dei dati: liberi di trasferire i propri dati in un mercato digitale più aperto alla concorrenza)，ＥＵ域外に対するデータの移転の厳

140 http://www.garanteprivacy.it/web/guest/regolamentoue

141 いわゆるデータ保護パッケージとは，2012 年 1 月に欧州委員会が公表した GDPR 及び法執行指令の総体をいう。

格な保護（Garanzie rigorose per il trasferimento dei dati al di fuori dell Ue），個人データ侵害（データ侵害）事案についての報告義務（Obbligo di comunicare i casi di violazione dei dati personali (data breach)），企業・事業に対するイノベーション（Le novità per le imprese e gli enti），すべての EU 諸国に対する単一のルールのセット（Un unico insieme di norme per tutti gli Stati dell Unione europea），責任ある人々にとってのもっとも効果のあるリスク・ベースのアプローチ（Approccio basato sulla valutazione del rischio che premia i soggetti più responsabili），自己規制システムの奨励による保護の強化と単純化（Semplificazioni per i soggetti che offrono maggiori garanzie e promuovono sistemi di autoregolamentazione）である。

（ヨーロッパデータ保護規則枠組みの適用についてのガイド）

前記「個人データ保護の欧州の規則についての新しいガイド」が GDPR の説明であるのに対して，これはイタリアの個人データ保護庁が，具体的にイタリアにおける GDPR の執行に際してのガイドラインを明らかにしたものである。

2017 年 4 月 28 日に，個人データ保護庁は，GDPR 対応のガイドライン群を明らかにした。

具体的には，処理の適法性の基礎，情報，関連当事者の権利，データ管理者・データ処理者・処理担当者，データ処理者における処理及び説明責任のリスクをもとにしたアプローチ手法，第三国に対するデータ移転と国際組織について解説している。

このガイドは，企業と公的機関が，5 月 25 日の完全実施を視野にいれて留意すべきことを示しており，特に，推奨事項では，各国の立法府による介入が許されない事項についての対応策が明らかにされている。また，主たる改正事項について，解説がされるとともに，示唆されている事項については，より明確なアイディアとともに到達しうるアプローチが記されている。当該内容については，推奨事項のある事項についてのみ記載を抜き出している。

（EU 規則－公的行政当局のためのプライバシー保護イニシアチブ［Regolamento Ue: al via l'iniziativa del Garante privacy per le Pubbliche amministrazioni］）

このイニシアチブは，公共の問題に関して新しい規則を適用させる過程において，適正な情報を提供し，明確化の必要性／既に実装されたアクションの情報を収集し，調査結果／既になされた影響を共有することを目的とする[142]。具体的には，2017 年 6 月の会合，11 月 7 日のローマ，12 月 4 日のミラノ，2018 年 1 月 15 日のバーリ（Bari）で会合が開催されている。

142 この目標を達成するために，公的部門は，下記の優先して取り組むべき事項があり，それらの支援のために，上述の一連の会合で，ガイドラインの提供，規則の実施の支援などが行われる。以上について，http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6487400

データ保護庁のホームページでは，公的部門（Pubbliche amministrazioni）おいて GDPR に対応する際，優先して取り組むべき事項が公表されている。具体的には，（1）データ保護責任者の指名（37 条ないし 39 条）（2）取扱行為の登録の実施（30 条ほか）（3）個人データ侵害の通知（データ侵害ともいう，33 条及び 34 条）である。

（公的部門におけるデータ保護オフィサー（RPD）の FAQ）

データ保護オフィサーについては，29 条グループがガイドラインを公表しているが，この FAQ は，29 条グループのガイドラインに付加されるものとして公表されているものである。質問項目は，1　主体的要求事項，2　資格，3　認証，4　指名の公式行為，5　事務所の必要性，6　複数指名の可否，7　追加業務の可否である。

主体的要求事項について，GDPR は，「公的機関」または「公的団体」の定義を置いていないが，29 条委員会では，定義は国内法によるとされることから，イタリアでは，データ保護法典の 18 条ないし 22 条の範疇に該当するデータ主体が「公的機関」または「公的団体」に該当すると考えられる。従って，公的機能を行使するとしても，それらの範疇に該当しない民間企業については，規則の適用があるとはされない。しかしながら，FAQ では，そうした民間企業に対しても，データ保護オフィサーの設置を強く推奨している。FAQ はデータ保護オフィサーについて，特定の資格が求められるとはしていないが，担当する仕事によって評価されること，組織内において指示を受けてはならず，独立性をもった対応を行うこと，トップの経営層に連絡できる人材であること，管理職または，高度な専門職になること，などを定めている。

（4）年表

2017 年 4 月 28 日	ヨーロッパデータ保護規則枠組みの適用についてのガイド
同 10 月 19 日	EU 規則－公的行政当局のためのプライバシー保護官による第 2 ラウンド会合の通知
同 12 月 4 日	同ミラノ会合
同 12 月 18 日	データ保護オフィサーFAQ　公表

3　GDPR 適用前の公的部門に関する個人情報保護制度の運用実態等

（1）概要

①　公的部門の個人情報保護の法的枠組と議論動向

イタリアにおいて，公的部門に対する個人データの保護に関する特別法は存在せず，個人データの取扱はデータ保護法に関する一般的な法である個人データ保護法典（CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI）（Legislative Decree no. 196 of 30 June 2003）[143]のもと，公的部線，民間部門区別なく規制される。

もっとも，この個人データ保護法典は，個別のセクターごとの条文も存在している。全体の構造は，1 部（一般規定），2 部（特定セクター），3 部（救済及び制裁）と附則 A 及び B に分かれている。この構造は，

（1 部－一般規定）

タイトル 1　一般原則（1 条－6 条）
タイトル 2　データ主体の権利（7 条－10 条）
タイトル 3　一般データ取扱規定（11 条－27 条）
タイトル 4　取扱作業をなす組織（28 条－30 条）
タイトル 5　データ及びシステムセキュリティ（31 条－36 条）
タイトル 6　特定行為の遂行（37 条－41 条）
タイトル 7　越境データ流通（42 条－45 条）

（2 部－特定セクターに適用される規定）

タイトル 1　司法セクターにおける処理（46 条－52 条）
タイトル 2　警察における取扱業務（53 条－57 条）
タイトル 3　国家防衛及び安全（58 条）
タイトル 4　公的部門における処理（59 条－74 条）
タイトル 5　ヘルスケア産業におけるデータ処理（75 条－94 条）
タイトル 6　教育（95 条－96 条）
タイトル 7　歴史，統計，科学目的の取扱（97 条－110 条）
タイトル 8　職業及び社会安全問題（111 条－116 条）
タイトル 9　銀行，金融及び保険システム（117 条－120 条）
タイトル 10　電気通信（121 条－134 条）
タイトル 11　自営専門職及び私立探偵（135 条）
タイトル 12　報道・文芸・芸術表現（136 条－139 条）
タイトル 13　ダイレクト・マーケッティング（140 条）

---

143 英語訳は，http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf

（3 部－救済及び制裁）

タイトル 1　行政的及び司法的救済

タイトル 2　監督機関

タイトル 3　罰則

タイトル 4　改正，廃止，経過及び最終規定

（附則 A－行為規範）

（附則 B－最低限のセキュリティ手法における技術仕様）

公的機関における個人データの保護について，データ保護官が公的機関に対して，ガイドラインを公表しているのが注目される[144]。2007 年 4 月には，「地方公共団体が文書を公表し，伝達するための個人データ取扱に関するガイドライン」[145]，同 7 月には，「公的機関における労働者の個人データの取扱に関するガイドライン（Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico）」が公表されている[146]。

また，Web の利用が進んだことに対応して，2011 年には，「公的行政機関における個人データ：Web ベースの通信に関する公的機関による取扱のガイドライン(Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico）)」[147]が，2014 年 5 月には，「行政文書に含まれる個人データに関する取扱と，公的機関による Web の公表と透明性に関するガイドライン(Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati)」が公表されている[148]。

---

144 http://qualitapa.gov.it/it/relazioni-con-i-cittadini/comunicare-e-informare/privacy-e-tutela-dei-dati-personali/

145 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1407101

146 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1693793

147 英語版ハイライトは，http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1803707
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1793203
データ保護官が，公共行政機関の透明性を拡張することを目指し，公的記録へのアクセスを実現することを目的とした近時の立法に留意し，組織において，記録を公表し，共有する場合のガイドラインである。
個人データの公表について，法的根拠のある場合，公共目的から厳格な必要性のある場合，透明性を求める規制改革に基づく場合，関係者の求めによる場合に分けて，留意すべき事項が議論されている。

148 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436
このガイドラインは，EU 指令，データ保護法典，情報公開・透明性・拡散の再構成に関する立法命令，上記 2011 年ガイドラインなどに留意した公共機関の有する情報の公表及び透明性に関するガイドラインである。
上記透明性立法による公表の際に検討すべき事項，公共機関において他の目的によって公表する場合に検討すべき事項についてそれぞれ検討がなされている。

② 公的部門を監督する機関（担当省庁）

公的部門を監督する機関（L'Autorità）は，個人データ保護官（Garante per la protezione dei dati personali）であり，データ保護法典 3 部　救済及び制裁のタイトル 2 に定められている。タイトル 2 は，1 章　個人データ保護官（Garante per la protezione dei dati personali）　2 章　データ保護局（L'Ufficio del Garante）　3 章　聴取及びコントロール（Accertamenti e controlli）からなる。

データ保護法典 153 条 1 項は，保護官は，自律的に，独立して，決定及び評価を行うことを定めている。データ保護官は 4 名からなり，2 名は代議院，2 名は元老院から選任される（同 2 項）。

現在（2016 年報告による）のデータ保護局の人員構成は，執行役員 15 名，官吏（officials）73 名，運営（operating）24 名の合計 113 名（その他　派遣 8 名）である。

具体的な組織図は，付録に添付する。

また，個人データ保護の機関という趣旨とは異なるが，公的機能省(Dipartimento della Funzione Pubblica)[149]のもとに PAQ（公的機関の質-Pubblica Amministrazione di Qualità）の名前で，種々のイニシアチブが展開されており，個人データ保護に関するベストプラクティス[150]も提供されている。

（2）各項目の分析

① 適用対象機関

データ保護法典は民間部門，公的部門双方を適用対象とするが，2 部に特定のセクターごとに適用される規定を個別においている。

また，1 部タイトル 3　データ取扱の一般規則（Titolo III-Regole generali per il trattamento dei dati）の 2 章（Capo II）でも，公的部門において付随して適用される規則（Regole ulteriori per i soggetti pubblici）（18 条－22 条）が置かれている。

（18 条－公的団体によってすべての取扱業務について適用される原則［Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici］）

同条は，この章の規定が，営利の公的団体以外のすべてに適用されること（1 項），個人

149 公的機能省とは，国際的ヨーロッパのガイドラインに基づいて，行政機関が，公的サービスの業務と質を向上させるのを実行するための取り組みを促進することを目的とする行政機関である。http://www.qualitapa.gov.it/　。公的機能省が，展開しているものとして，ベストプラクティスの普及以外に，ノウハウの定義，CAF モデルに基づいた自己評価の支援，ベンチマーキングももとにした業績評価などがある(http://qualitapa.gov.it/chi-siamo/)。

150 PAQ における公的機関の個人データの取扱に関する記載としては，以下の 2 つがある。
http://qualitapa.gov.it/it/relazioni-con-i-cittadini/comunicare-e-informare/privacy-e-tutela-dei-dati-personali/
http://qualitapa.gov.it/it/relazioni-con-i-cittadini/comunicare-e-informare/privacy-e-tutela-dei-dati-personali/trattamento-dati-personali-dei-lavoratori-delle-pa/
また，公的機関における自己評価のモデルを提供している。

データを機構の目的を行うのに必要な限りでのみ取り扱うこと（2 項），取扱に関しては，公的団体は，この法典において定められているデータ取扱の条件とされる事項及び限界とされる事項に限定され，法及び規則と，データの特性の配慮によって限定されること（3 項）などについて触れている。

（19 条－機微及び司法データ以外のデータの処理に適用される原則［Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari］）

機微かつ司法データ以外については，18 条（2）項の規定に従って取り扱うことができること，公的団体が他の公的団体と連絡を行うことは，法または規則によって定められていれば許容されること（2 項），他の民間団体と連絡を行うことは，法または規則において許容される場合のみ許容されること（3 項）について触れている。

（20 条－機微データの処理に適用される原則［Principi applicabili al trattamento di dati sensibili］）

公的団体による機微データの取扱は，法によってデータの範囲が明確に認められている場合であり，実質的に公益が実現されるカテゴリである場合に認められること（1 項），法が，実質的な公益を追求することを述べているが，機微データに関するカテゴリや実行される取扱方法が示されていない場合には，常に，データの範囲と取扱が，特定され，公になっている場合のみ認められること（2 項），もし，取扱が明確に法によって明らかになっていない場合には，データ保護官に対して，実質的な公益を行う取扱であるかを否かの決定を求めることができること（3 項）などが定められている。

（21 条－司法データに適用される原則［Principi applicabili al trattamento di dati giudiziari］）

公的部門における司法データの取扱については，法もしくはデータ保護官の命令によって，目的／データの範囲／取扱の手法が特定されている場合に限って，許容されること（1 項），組織犯罪防止のため特定の場合も同様であること（1 項の 2）などが定められている。

（22 条－機微及び司法データに適用される原則［Principi applicabili al trattamento di dati sensibili e giudiziari］）

公的部門における機微な司法データについては，データ主体の権利，基本的な自由及び尊厳についての侵害を防止する対応策に従って取り扱うこと（1 項），データ主体に対して 13 条（データ主体に対する情報）に定めるデータの取扱に関する情報を伝える際には，機微な司法データを処理する根拠として，関連する義務，または求められる事項に明確に言及すること（2 項）などが定められている。

（2 部［特定のセクターのデータ保護］と公的部門）

2 部における特定のセクターのデータ保護のうち，司法セクターの処理，警察の処理，国家安全，その他の公的部門における処理に関する規定を簡単に紹介すると以下のようになる。

タイトル 1　司法セクターにおける処理（46 条－52 条）

タイトル 2　警察における取扱業務（53 条－57 条）

タイトル 3　国家防衛及び安全（58 条）

タイトル 4　公的部門における処理（59 条－74 条）

このタイトル 4 においては，行政記録に対するアクセスについて，1990 年 8 月 7 日法によって規定されていること（59 条），健康状況・性生活に関するデータが保護されるべきこと（60 条）が定められている。また，データ保護官が，実務規範を構築するのを促進すること（61 条）が定められている。誕生，死亡，婚姻，人口センサスの登録等については，20 条（センシティブデータに適用される原則），21 条（司法データの取扱に適用される原則）に基づいて公共の利益によるものと見なされること（62 条），64 条以下は，実質的に公共の利益があると考えられる類型であって，具体的には，市民権，移民，外国人の状況（64 条），政治的権利や選挙の投票の秘密・陪審団の構成かどうかなどの特定の団体の行動の開示（65 条），課税・関税の事案（66 条），監査等の事案（67 条），認可・認証（68 条）などの場合である。

②　保護対象データ

データ保護法典 4 条 1 項 b）は，個人データについて「個人データ（dato personale)」は，自然人に関連する，個人識別番号を含む他の情報を参照することによって，個人を識別し，または，識別しうる情報すべてをいうと定義している。また，「取扱（trattamento)」について，取扱とは，電気的，自動的な手段の助けがあるとないとに関わらず，収集，記録，整理，保管，聴取，精緻化，変更，選択，検察，比較，利用，接続，ブロック，通信，拡散，消去及び廃棄の処理，もしくは，そのセットを意味するものであって，データ保管所に含まれているかを問わないと定義されている。従って，イタリアにおいては，マニュアルで保管されているデータについても保護の対象となる。

③　目的外利用の状況（目的外利用の根拠規定，件数等）

データ保護法典は，一般論として，11 条 1 項（データ取扱の様式及びデータの質）において，個人データの取扱については，

「特定の，明確で適法な目的のために収集され，記録されること，更に実際に取り扱われる際には，その目的と矛盾しない方法によること」（b）

「収集され，または，取り扱われるとした目的に関連すること／その目的で取扱を完了すること／その目的を超過しないことと」（d）

としている。しかしながら，公的部門においては，一般に 18 条（公的団体によってすべての取扱業務について適用される原則）の 2 項において明らかなように，公的部門の目的を行うのに必要な限りでのみ取り扱うこととされる一方で，具体的な取扱に関しては，公的団体は，この法典において定められているデータ取扱の条件とされる事項及び限界とされる事項に限定され，法及び規則と，データの特性の配慮によって限定されること（3 項）となっている。なお，機微／司法データについて，それぞれ特別の定めがあることについては，上述したところである。

イタリアにおいては，このように公的部門における個人データ取扱についての特別の原則が，他の国に比較して明確になっている。

目的外利用についての運用実態等については，データ保護官の年間報告書において，特段のデータは存在しない。

④　本人関与の仕組み（開示，訂正，利用停止請求）と運用実態（請求件数等）

本人関与の仕組みについての一般的な規定は，データ保護法典 1 部タイトル 2　データ主体の権利（Diritti dell'interessato）において記載されている

同タイトルは，7 条　個人データへのアクセス権その他の権利（Diritto di accesso ai dati personali ed altri diritti），8 条　権利の行使（Esercizio dei diritti），9 条　権利行使のメカニズム（Modalità di esercizio），10 条　データ主体への対応（Riscontro all'interessato）について述べている。

個人データへのアクセス権及びその他の権利（7 条）において，個人データの処理がなされているか確認する権利があること（1 項），個人データをどのような経路で取得したか，取扱の目的及び方法，取扱のロジック（自動処理において，どのような手順・解法で取り扱うか等），データ管理者・データ取扱者・代表者の氏名，伝達された組織・責任者・取扱者を知る権利があること（2 項），データのアップデート・修正・統合を求めること，不適法に取り扱われている場合の消去・匿名化・ブロックを求めること，それらの場合の証明書を取得すること（3 項），法律の定めに基づいた異議を求めうる権利，広告を直接に送付する・直接に販売する・宣伝・広告を送付するために個人データを取り扱うことに異議を求めうる権利を有すること（4 項）が定められている。

ただし，これらの権利は，通貨・金融政策・決済システム・ブローカー・信用・金融市場及びその安定性のコントロールの目的のために法で明示的に求められている場合（8 条 2 項 d）やマネーロンダリングに関する場合，暴力行為の被害者の場合，議会の調査権の場合，公衆電気通信サービスの司法前手続き調査の場合，司法手続きの場合，53 条（警察活動）の場合において，制限されている。

（公的部門における本人関与の実態）

データ保護官の 2016 年報告書においては，この様なデータは存在しない。

⑤　執行における特別事情／救済措置の仕組み（第三者機関，訴訟等）とその運用自体（件数等）

（救済措置の仕組み（第三者機関，訴訟等）とその運用実態）

行政的及び司法的救済は，更に，1 章　データ主体がデータ保護官において利用可能な救済　と 2 章　司法的救済に分かれている。前者は，一般的原則（Principi generali141 条），行政的救済（Tutela amministrativa 142 条－），非司法的救済（Tutela alternativa a quella giurisdizionale 145 条－）に分かれている。後者については，権限があることが述べられている（152 条）以外は，2011 年立法命令 150 号の 10 条によって論じられている（同項 2 号）。

具体的には，労働関係の手続の規定によること，データ管理者の居所に管轄があること，申請人が初回欠席の際には，却下の判断がなされることなどである。

（データ保護官において利用可能な救済）

一般的原則（141 条）において，データ主体は，データ保護官に対して（1）142 条に基づいて個人データの処理について関連する事項についての詳細な請求（reclamo circostanziato）（2）データ保護官が上述の規定を確認できるような報告（3）7 条に関した特定の権利を（以下の司法的救済に代替する保護措置の規定に従った形式で）主張する要求，をそれぞれ申し立てることができるとされている。

（救済の手続的事項）

詳細な要求の記載事項（同 142 条），請求の取扱（143 条），報告（144 条）などが定められている。請求の取扱においては，個人データの取扱を暫定的に，自動的に停止したり，禁止したりすること，法で定められている取扱に必要な手段をとることを明示すること，個人データの取扱を停止し，または，禁止することを求めることができること，公共の利益に反する場合には，団体・カテゴリの個人データの取扱を禁止することができることが述べられている。

（司法的救済に代替する保護措置）

データ保護法典 145 条は，司法的救済との選択的保護(Tutela alternativa a quella giurisdizionale)として，同法典 7 条の権利は，裁判を提起することによっても，また，データ保護官に請求を申し出ることによっても，行使することができると論じている。データ保護官に請求を申し出る場合の記載事項，添付書類等については，147 条で規定されている。

データ保護事務局は，請求を受け取ってから 3 日間以内に，データ管理者に連絡し，データ管理者が，その請求が認められない，あるいは，根拠がないという場合以外は，10 日以内に，自発的に請求に従う旨を請求者及び保護官事務局に連絡する。事案によって，データ

保護官は，暫定的に部分的・もしくは全面的なデータの利用停止や，取扱の終了を命じることもできる。必要な情報を収集した場合には，データ保護官は，理由とともにデータ管理者に対して，期限を定めて違法な取扱をやめる，またはデータ主体の権利を執行する旨の救済を命じることができるとされている。

（司法的救済）

データ保護官の判断について，データ管理者／データ主体は，裁判所に異議を申し立てることができる（151 条）。

また，152 条は，データ保護法典に関する争いが，裁判所の権限によって判断されることを明らかにしている。

（民事責任の問題）

司法的救済については，民事的な責任の問題と刑事的な責任の問題がある。

民事的な責任の問題については，データ保護法典 15 条が，「個人データの取扱の結果として他人に損害を与えたものは，民法 2050 条に従って損害を賠償する義務を負う」と定めている。また，データ保護法 11 条違反による財産的損害でない場合においても同様である（同 15 条 2 項）。民法 2050 条（危険な活動の行使に対する責任）は，「その性質上または使用された手段の性質によって，危険な活動を行う上で他人に害を与える者は，損害を回避するための適切な措置をすべて講じていないと判明した場合には，補償の責任を負う。」と定めている。

民法 2050 条における「損害を回避するための適切な措置」をめぐり，データ管理者が果たすべき責任については，データ管理者等が，損害を防止する可能で適切な手段を取ったことの証明責任を負うという立場と，説明責任までは含まないという立場がある。また，民法 2050 条が，財産的損害がない場合において適用されるとしても，信頼関係違反があったことのみをもって，損害が発生したとは解することはできず，実際に損害があったことの証明がなされなければならないという最高裁判決がある（26972/2008）。

（行政規範違反への罰及び刑事罰）

タイトル 3 は，1 章　行政規範違反（Violazioni amministrative）及び 2 章　刑事罰（Illeciti penali）から成り立っている。

（行政規範違反への罰）

行政規範違反は，データ主体に対する情報の不提供／不適切な提供（161 条　Omessa o inidonea informativa all'interessato），その余の不遵守（162 条，Altre fattispecie），通信データ保持違反（162 条の 2，Sanzioni in materia di conservazione dei dati di traffico），公衆電気通信プロバイダーに対する罰（162 条の 3，Sanzioni nei confronti di fornitori di

servizi di comunicazione elettronica accessibili al pubblico)，通知送付の懈怠もしくは不十分な送付（163 条，Omessa o incompleta notificazione)，データ保護官に対する情報提供／部署提出の懈怠（164 条，Omessa informazione o esibizione al Garante)，軽度な案件等（164 条の 2，Casi di minore gravità e ipotesi aggravate)，データ保護官による公表（165 条，Pubblicazione del provvedimento del Garante)，実際の手続（166 条，Procedimento di applicazione）に分けて論じられている。

（刑事罰）

刑事的な責任について，データ保護法典は，種々の行為に対して刑事罰をもって，これを禁止している。具体的には，以下の表のとおりである。

section		構成要件	処罰
167 条 1 項	違法なデータ取扱	自己の利益または第三者を害する目的で，18 条，19，23，123，126 及び 130 条または 129 条までの規定に違反すること	損害が発生した場合，懲役 6-18 月
			通信，または，拡散された場合は，懲役 2-24 月
167 条 2 項		自己の利益または第三者を害する目的で，17 条，20，21，22(8)&(11)，25，26，27 及び 45 条の規定に違反すること	損害が発生した場合，懲役 1-3 年
168 条	データ保護官に対する不誠実な宣言・通知	32 条の 2 の通知，37 条の通知，データ保護官への/調査における連絡，記録，文書，陳述書において，不実の情報，状況を宣言/証言/偽造された記録・書類を提出すること	懲役 6 月-3 年
169 条	セキュリティ手段	関連する義務違反において 33 条に定める最低限のセキュリティ手段を採用するのを怠ること	禁固（arresto）2 年まで
170 条	データ保護官の定める規定の不遵守	26 条（2），90，150（1）（2），143（1）c）に従ってなされるデータ保護官の規定を遵守するのを怠ること	懲役 3 月-2 年

171 条	その他の犯罪	113 条（1）及び 114 条による規定違反	1970 年 5 月 20 日法 300 の 38 条

実際の判決の状況については，2016 年報告書では，刑事事件として 58 件の違反が司法当局に対して送致されている。その内訳は，

・最低限のセキュリティ採用違反（169 条）が 35 件

・5 件が，労働法（n. 300/1970（Workers' Statute））違反。法典 171 条違反

・5 件が違法なデータ取扱（167 条 1 項及び 2 項）

・2 件が，保護官の規定に対する適合懈怠（170 条）

・5 件が，その他の刑事処罰（171 条）

である。

⑥　監督機関の権限及び活動

（データ保護官の活動）

データ保護官の業務は，同 154 条によって，法と規則の遵守を確認すること，苦情申立に対する受領，対応，各規定を遵守するように管理者・責任者に対して命令を行うこと等と定められている。

データ保護法典 157 条は，データ保護官が，データ管理者，データ処理者，データ主体等に対して，情報を提供し，書類を提出することを要求する権限があることを定めている。また，同 158 条は，保存されたデータやファイリングシステムへのアクセス，取扱のなされている現場の監査，法規の遵守のために調査する命令の権限を定めている（それらの手続は，159 条）。

なお，公的部門（2 部のパート 1 ないし 3）については，データ保護官の指定する代理人によって実行されうることが明らかにされている（160 条）。

（データ保護官の活動の状況）

2016 年の年間報告書によれば，データ保護官は 4633 件の質問・苦情申立及び報告に対して回答を行っている。分野としては，電話営業，消費者信用，ビデオ監視，公共サービスの営業権，信用修復，ジャーナリズム，地方社会，健康・社会援助サービスなどである。また，277 の異議申立（appeals）対しての判断を行っており，主として，出版（テレビを含む），銀行・金融会社，公的・民間雇用主，信用情報システム，公共サービスの営業権者などからのものである。

異議申立は，個人データ保護のための最低限度のセキュリティも採用していないということを理由にしたものが多いが，データ保護官は 53 件について，司法当局に対して，告発を行っている

行政的違反の件数は，増加しており，2016 年は，2339 件（2015 年比で 38%増加）。その

うちの相当部分が，データ侵害事案においての通知の電話の不履行及び電気通信オペレーターの不足の案件である。また，それ以外には，同意なしの違法な取扱，取扱に際して提供される情報が省略され，不適切であること，電話・電気通信のトラフィックデータの過度の利用，セキュリティ手段の不十分さ，保護官への書類の不備，監督機関の規定への不適合などがある。

行政罰の課せられた額の合計は，330 万ユーロ弱（約 4 億 3800 万円）に及び，その内訳は，以下のとおりである（単位ユーロ）。

略式の手続きによる支払	2,324,440
差止命令による支払	432,976
169 条のセキュリティ手段懈怠による支払	150,000
その他の制裁活動による支払	382,480
合計	3,289,896

査察件数は 282 件である。民間企業では，自動車シェアの会社（ウーバー事件），Web 及び電話マーケティング，遺伝子検査会社，派遣労働代理業，PC／携帯電話のデータ復旧及び技術支援会社，オンラインゲーム会社等に対して査察が行われている。

公共部門，特に地方自治体政府で明らかとなった主な問題は，1）顧客に関するデータ侵害に関するもの，2）大量のデータ収集に関する主体の同意の欠如，または 3）最低限のセキュリティ対策の欠如，4）個人データ保護官への通知義務違反等である。

⑦　ケーススタディ

（公的部門における問題の具体例）

具体的な例は，公的な機関における機微なデータの取扱，公的データベースの監視，公的機関における透明性，民間のアクセス，公的データ漏洩，個人的文書及び電子文書，学校教育，税金，公共領域におけるビデオ監視，地域公共団体における取扱，社会保障・支援制度，司法活動である。

このうち，地域公共団体における取扱において取り扱われている事例の中には，公共団体における事実調査のためのグーグルフォームの利用の問題（地方自治体が，交通量の測定のため，データを氏名，年齢，電子メールをグーグルフォームで収集した案件について，データ保護法典 13 条に違反するとされた事案。調査対象になったあと，自治体は，データを消去した）などがある。

付録１　ヨーロッパデータ保護規則枠組みの適用についてのガイド

「ヨーロッパデータ保護規則枠組みの適用についてのガイド」について，イタリアにおける推奨事項として記載されている事項は，以下のとおりである。

１　適法性の基礎（Fondamenti di liceità del trattamento）

推奨事項としては，前文 47 において，利益衡量が提供されていること，また，29 条委員会によって WP217 が公表されていること，イタリアデータ保護庁が文書でこの基礎を明らかにしていることがあげられている。

２　情報（informative）

データ管理者は，一定の範囲の情報について，同意とその条件案の過程と同様に，準拠することを検証しなければならない。データ保護官がかねて明らかにしてきたことである [151] が，GDPR は，明確に，「階層的」情報（informativa “stratificata”）という概念を支持している。これは，ビデオ監視システムを利用していることをアイコン（簡単な絵柄での表示）を使用するなどして周知するように，データの利用等について，より分かりやすく，簡潔に，かつたくさんの人に伝達するという考え方である。また，データ主体に提供される情報については，データ主体により直接に収集される場合でなければ，1 カ月を超えない範囲で，データ管理者等により提供されなければならない(データ保護法典 13 条 4 文との相違)。

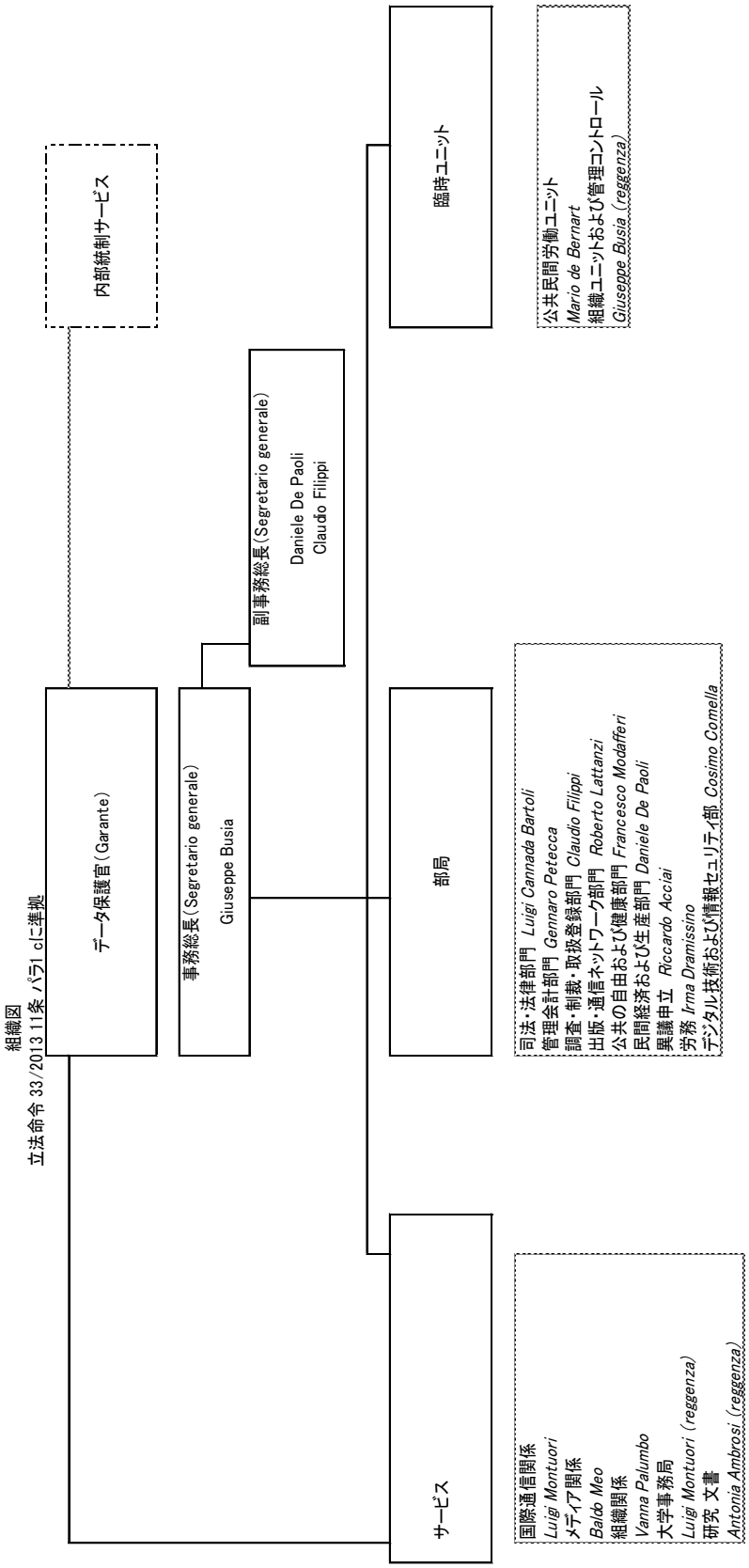
データ主体に提供される情報の態様としては，GDPR 前文 58 項でふれられているように，簡明，明確，アクセスが容易で，シンプルであることなどが求められており，文書(電子的様式)で提供されることが望ましいとされる。アイコンとともになされる場合には，説明が付されるべきであり，アイコンは，EU 域内で同一であるように定める。データ管理者が多数の関係者に対して情報を伝える必要があり，それが必要以上の労力を要すると考える場合には，保護官は，どのようにしてそのような労力を要する業務に対応するかについてのコメント [152]を公表している。

---

[151] ビデオ監視システムについて(2010 年 8 月) http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680
信用機関における指紋認証システムについて（2005 年 10 月）
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675

[152] 関連する当事者への情報-明らかに過剰な手法が必要とされる場合(1998 年 10 月)
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39624
ビジネス行為におけるデータ処理の開示
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3864423

付録 2　組織図


組織図
立法命令 33/2013 11条 パラ1 cに準拠
データ保護官（Garante）
内部統制サービス
事務総長（Segretario generale）
Giuseppe Busia
副事務総長（Segretario generale）
Daniele De Paoli
Claudio Filippi
部局
臨時ユニット
公共民間労働ユニット
Mario de Bernart
組織ユニットおよび管理コントロール
Giuseppe Busia（reggenza）
司法・法律部門 Luigi Cannada Bartoli
管理会計部門 Gennaro Petecca
調査・制裁・取扱登録部門 Claudio Filippi
出版・通信ネットワーク部門 Roberto Lattanzi
公共の自由および健康部門 Francesco Modafferi
民間経済および生産部門 Daniele De Paoli
異議申立 Riccardo Acciai
労務 Irma Dramissino
デジタル技術および情報セュリティ部 Cosimo Comella
サービス
国際通信関係
Luigi Montuori
メディア関係
Baldo Meo
組織関係
Vanna Palumbo
大学事務局
Luigi Montuori（reggenza）
研究 文書
Antonia Ambrosi（reggenza）

第６　ポーランド

１　ポーランドの公的部門における個人情報保護制度の概要

（１）背景・経過

ポーランド共和国憲法（1997 年 4 月 2 日）は，47 条で人格権，自己決定権を保護しており，51 条で個人情報保護の権利等を保護している。憲法の直後に成立している 1997 年 8 月 29 日のデータ保護法（PDPA）がポーランドでのデータ保護に関する一次的な法律である。野党第一党であった自由同盟が 1996 年 8 月に議員提案の形で個人データ保護法案（Druk nr 1928）を提出，10 月に政府も同名の法案（Druk nr 1890）を提出し，11 月から議会審査が開始された。両法案は関連委員会により一本化され，下院で可決，上院での修正を経て，1997 年 8 月末に，国会の圧倒的多数の賛成により最終的に成立したとされる（後掲・小森田論文による）。その後，逐次の改正を経ている。

憲法レベルでの個人情報保護の権利の記述には，1993 年の欧州人権条約（ECHR. European Convention on the Protection of Human Rights）加盟及び，1995 年 EU データ保護指令の影響が見て取れる。なお，ポーランドが欧州連合に加盟したのは 2004 年 5 月 1 日である。

（２）年表

1997 年 4 月 2 日	ポーランド共和国憲法制定
1997 年 8 月 29 日	データ保護法（PDPA）成立
2004 年 5 月 1 日	欧州連合加盟
2017 年 9 月 14 日	デジタル化省（Minister of Digitalization）から欧州一般データ保護規則実施のための新データ保護法草案公表

２　ポーランドにおける GDPR のための対応について

（１）GDPR のための対応について

ポーランドにおいては，GDPR の完全適用である 2018 年 5 月 25 日に向けて，実施法案の検討及びデータ保護機関（GIODO）によるガイドラインの公表が行われている[153]。

（２）政府における対応について

①　法案の概要

2017 年 9 月 14 日に，デジタル化省（Minister of Digitalization）から欧州一般データ保護規則実施のための新データ保護法草案（a draft of the new Personal Data Protection Act

[153] ポーランド法についての情報はポーランド語によるものが大半であり，詳細を検討するためには膨大なポーランド語による文書の翻訳または現地でのヒアリングが必要となるため，ここでは英語による文献，情報を中心に情報を整理し，必要に応じてポーランド語による文献，情報は英語または日本語に自動翻訳することで大意を紹介するに留める。

“implementing” EU General Data Protection Regulation，以下「実施法案」という。）が公表され，2017 年 10 月 13 日までパブリックコメント手続に付された [154]。

実施法案は 130 以上の法令を改正するものであって，ポーランドの法案の中でもここ数年で最も大規模な改正を行うものであるとされている [155]。データ保護法の改正事項は，ⅰデータ保護機関の組織，ⅱ行政調査手続，ⅲ民事責任（GDPR79 条，82 条），ⅳ課徴金，ⅴ刑事罰（GDPR84 条），ⅵ認証メカニズム（GDPR42 条），ⅶ13 歳未満の子に対するサービスの提供に関する特則（GDPR8 条），ⅷDPO の設置に関する経過規定に及び，これ以外に労働法，電気通信法，電子サービス法，決済サービス法，銀行法等において改正がなされるとされている [156]。

以下では，データ保護法の改正事項の内，公的部門への影響があり得る点を概観する。

② データ保護機関の組織

ポーランドのデータ保護機関は”The Bureau of the Inspector General for the Protection of Personal Data” (GIODO)（個人データ保護検査官局）であったが，新たに“Office for Personal Data Protection”（個人データ保護事務局）とされ（略称は”GIODO”のまま），”President”（事務局長）が置かれることになる。また，諮問機関として“Council for the Protection of Personal Data”（個人データ保護評議会）が置かれ，答申等を行うこととなる。

③ 行政調査手続

個人データ保護に関する社会組織（いわゆる Privacy Advocate に相当するものであると思われる）によって手続の開始が請求されたり，手続に参加することを認めたりすることがありうる他，調査に係る書類が外国語で記載されている場合には，すべて，調査対象のコストによって，ポーランド語に翻訳を提出する義務が定められた。

行政調査は計画的なもの，突発的（ad hoc）なものいずれも認められるが，30 日以上に渡ることはできない。行政調査の結果，データ保護法違反が判明した場合，GIODO 事務局

---

[154] 原文は，https://legislacja.rcl.gov.pl/docs//2/12302951/12457700/12457701/dokument308369.pdf（ポーランド語）。2018 年 1 月 15 日には，デジタル関係省によって，パブリックコメントの結果概要に関するカンファレンスが開催された。Magdalena Gad-Nowak, ”Poland’s Draft GDPR Implementation Law – Where Are We At?”, https://www.ceelegalblog.com/2018/01/1178/, (January 29, 2018). 同記事によれば，2018 年 4 月には議会を通過し，成立するのではないかとされている。

[155] Onetrust, “Poland Publishes New Draft Data Protection Acts “Implementing” the GDPR”, https://onetrust.com/poland-publishes-new-draft-data-protection-acts-implementing-gdpr/, (September 26, 2017) 米国の CBPR における AA（アカウンタビリティ・エージェント）である Onetrust（旧 TRUSTe）による記事である。

[156] 前掲 Onetrust。その他，実施法案の内容については Marcin Lewoszewski, “Poland's draft GDPR implementation law”, https://iapp.org/news/a/polands-draft-gdpr-implementation-law/, Ewelina Witek, “The Polish Draft of the New Personal Data Protection Act - Announced!”, https://www.lexology.com/library/detail.aspx?g=8c1f13ee-d757-4ec9-a209-76dd39a24b22 (September 18, 2017)を参照している。

長は適切な手続きを採らなければならず，作為または不作為が刑事罰に該当すると考えた場合には法執行機関（捜査機関）への告発義務を有する。

④　民事責任

個人データ保護法（及び GDPR）に基づく権利が侵害された者は，侵害者に侵害状態を取り除くために必要な措置を講じることを要求することができる。これは，民事上の司法救済を要求する GDPR79 条及び 82 条に対応したものであると考えられる。地方裁判所（sądokręgowy）が管轄権を有する（訴額に拘わらない）。

上記訴訟が提起された場合，地方裁判所は，訴訟の提起を GIODO 事務局長に通知する義務がある。当該侵害に関して GIODO の手続または行政裁判所[157]の手続が係属している場合，事務局長は裁判所に通知する義務があり，裁判所は手続を中止することができる。民事訴訟と，GIODO による手続（及びその後の行政訴訟）の調整のための規定であると考えられる。

⑤　課徴金

GIODO は，GDPR 上の課徴金を課す権限を有する。ただし，公的機関に対しては規則に規定されているものの 400 分の 1 に過ぎない最高 10 万 PLN の課徴金しか課すことができず，この点は GIODO からの批判の対象となっている（後述）。

課徴金は，不服申立ての期限の満了日から 14 日以内に，または行政裁判所の判決が最終的かつ拘束力を持つ日から 14 日以内に支払われる。合理的な請求があった場合，事務局長は課徴金の支払いを延期したり，分割払いにしたりできる。

⑥　罰則

GDPR84 条に基づいた罰則が定められており，行政調査妨害に関して，軽罪の訴訟手続に従って罰金が科せられるとしている。さらに，特別類型の個人データ（GDPR9 条，旧センシティブデータ）について法的根拠無く取り扱った場合は，刑事訴訟法の下で最大 1 年間の自由制限刑または自由刑が科せられるとしている。

⑦　13 歳未満の子に対するサービスの提供に関する特則

ポーランド領土内から，13 歳未満の子供に直接提供される電子サービスについては，法定代理人の事前の同意がある場合か，当該子供によってなされた同意について直ちに法定代理人の確認がなされた以後にのみ提供が可能である。

---

157 ポーランドは普通裁判系統と行政裁判系統が分かれており，行政裁判所の一審は県行政裁判所である。在ポーランド日本大使館による「ポーランドの裁判制度」（http://www.pl.emb-japan.go.jp/relations/documents/saibanseido.pdf）参照。

（3）データ保護機関（GIODO）における GDPR 対応について

前述の通り，GIODO は多くのガイドラインを提供している他，実施法案への意見を公表している。

① ガイドライン

GIODO は以下の通り多くのガイドラインを提供している。Q&A 形式のものもあれば，文書形式のものもある [158]。以下のリストは Taylor Wessing 法律事務所による 2017 年 10 月段階における整理であり [159], 公表日は何れも 2017 年におけるものである。なお, GIODO は，2018 年 5 月 25 日以降，データ管理者が遵守すべきセキュリティに関し，ベスト・プラクティスを記述することによって, GDPR を補完する行動規範を公表するとしている [160]。

GDPR 対応を含む DPO の設置に関するガイダンス（Guidance on DPO appointment, including GDPR updates (Polish, 08/17)）
GDPR 対応を含む DPO 一般に関するガイダンス（Guidance on DPOs generally, including GDPR updates (Polish, 08/17)）
GDPR における侵害通知に関するガイダンス（Guidance on breach reporting obligations under the GDPR (Polish, 06/17)）
GDPR におけるプロファイリングに関するガイダンス（Guidance on profiling under the GDPR (06/17)）
GDPR における子どものデータに関するガイダンス（Guidance on children's data under the GDPR (Polish, 06/17)）
GDPR におけるデータ処理の委託に関するガイダンス（Guidance on outsourcing data processing under the GDPR (Polish, 06/17)）
GDPR に関する事業者向け一般ガイダンス（General guidance for businesses on the GDPR (Polish, 06/17)）
GDPR におけるデータ主体の権利に関するガイダンス（Guidance on data subjects' rights under the GDPR (Polish, 06/17)）
GDPR における同意についてのガイダンス（Guidance on consent under the GDPR (Polish, 06/17)）
GDPR におけるデータセキュリティに関するガイダンス（Guidance on data security under the GDPR (Polish, 06/17)）
データ処理に関する文書化についてのガイダンス（Guidance on the documentation of data

158 すべてポーランド語によるものであり，題名以外は確認が取れていない。
159 “GDPR Guidance - EU Regulators”, https://united-kingdom.taylorwessing.com/globaldatahub/article-GDPR-guidance-table.html
160 Thanos Rammos and Jürgen Pölzl, “Regulator guidance on the GDPR - What are other EU Member States doing?”, https://www.lexology.com/library/detail.aspx?g=4834d0d6-fcf6-4dcf-b400-fc89416dc51a

processing (Polish, 06/17))
プライバシーバイデザインに関するガイダンス（Guidance on privacy by design (Polish, 06/17))
DPIAs（データ保護影響評価）に関するガイダンス（Guidance on DPIAs (Polish, 06/17))
GDPR における説明責任についてのガイダンス（Guidance on accountability under the GDPR (Polish, 05/17))
GDPR と現在のポーランド法の主たる変更点に関するガイダンス（Guidance on key changes between the GDPR and the existing domestic legislation (Polish, 05/17))

② 実施法案に対する意見

GIODO は実施法案に対して 140 頁を超える意見を提出している[161]。

その内容は，ⅰ監督機関の独立性を害する，ⅱ子どもの個人データの取扱いについて 13 歳への引き下げは適切ではない，ⅲ行政機関への課徴金が著しく低額，ⅳ分野別規制の変更，との各項目に渡るものである。ⅰに関しては，GIODO 事務局長の任命から議会の関与を排除しており，監督機関の独立性（特に，2014 年 4 月 8 日の C-288/12 - 欧州委員会対ハンガリー判決）に反するとしている。また，ⅱ子どもの個人データの取扱いについては，個人データの取扱いに同意を与えることができるラインを 13 歳以上に引き下げたことを批判している。ⅲ行政機関への課徴金が著しく低額である点については，10 万ユーロでは抑圧的機能または予防的機能のいずれも満たさないリスクがあるとしている。更に，④に関しては，統計法，労働法，銀行法等の規制の変更について，個人データの保護を低下させるものであるとしている。

3 GDPR 適用前の公的部門に関する個人情報保護制度の運用実態等

（1）公的部門の個人情報保護の法的枠組と議論動向

ポーランド共和国憲法（1997 年 4 月 2 日）は，47 条で人格権，自己決定権を保護しており，51 条で個人情報保護の権利等を保護している。

憲法 47 条[162]
何人も，個人生活，家族生活，尊厳や名誉の法的保護を求める権利及び自らの個人生活を決定する権利を有する。

[161] http://www.giodo.gov.pl/pl/1520280/10202（ポーランド語）。データ保護法（PDPA）12 条 5 項に基づき，GIODO が個人データの保護に関する法案や規則に対して意見を述べる権限を有していることを根拠としているものと思われる。同条項には拘束力の点は定められておらず，現時点で GIODO の意見を取り入れていない論点についても報道されているところからは（前掲注 2・Gad-Nowak），拘束力があるものではないようである。

[162] 仮訳は在ポーランド日本大使館によるもの。http://www.pl.emb-japan.go.jp/seiji/documents/kenpou.pdf

憲法 51 条
1. 何人も法律に基づかなければ自らに関する情報の公開を強制されない。
2. 公権力は，民主的法治国家において不可欠なものを除き，市民に関するその他の情報を取得，収集し，閲覧に供してはならない。
3. 何人も自らに係わる公的文書及び資料を閲覧する権利を有する。
4. 何人も虚偽もしくは不完全な情報，または違法に収集された情報の訂正もしくは削除を要求する権利を有する。
5. 情報の収集及び閲覧の原則及び手続は，法律で定める。

1997 年 8 月 29 日のデータ保護法（PDPA）がポーランドでのデータ保護に関する一次的な法律であり [163]，最終改正は 2016 年 6 月 1 日である。欧州人権条約（ECHR. European Convention on the Protection of Human Rights）には 1993 年に，欧州評議会第 108 条約には 2002 年に加盟している。PDPA に基づく行政命令が 8 本定められている。

具体的には，ⅰデータファイリングシステムのデータ保護機関への登録に関する，The Regulation of 11 December 2008 by the Minister of Internal Affairs and Administration on specimen of a notification of a data filing system to registration by the Inspector General for Personal Data Protection，ⅱデータ保護機関に関する，Regulation by the President of the Republic of Poland of 10 October 2011 as regards granting the statutes to the Bureau of the Inspector General for Personal Data Protection，ⅲ安全管理措置基準に関する，The Regulation of 29 April 2004 by the Minister of Internal Affairs and Administration as regards personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing，ⅳデータ保護機関の調査員の ID カードに関する The Regulation of 22 April 2004 by the Minister of Internal Affairs and Administration As regards specimen of personal authorisations and service identity cards of the inspectors employed in the Bureau of the Inspector General for Personal Data Protection，ⅴデータ保護機関に関する，The Regulation of 19th November 2015 by the President of the Republic of Poland amending the regulation on granting the status to the Bureau of the Inspector General for Personal Data Protection，ⅵデータ保護オフィサーによるデータファイリング方法に関する，The Regulation of 11th May 2015 by the Minister of Administration and Digitalisation on the manner of keeping the data filing register by the data protection officer，ⅶデータ保護オフィサーの職責に関する，The Regulation of 11th May 2015 by the Minister of Administration and Digitalisation on the manner of

[163] 特別法が制定されている場合にはデータ保護法に優先して適用される。このような例として，精神的健康の保護についての法律（1994 年），非公開情報保護法（1999 年），銀行法（1997 年）が挙げられている（小森田明夫「ポーランド（個人情報保護法制の国際比較―民間部門を中心として）」比較法研究 64 巻（2002 年）58-67 頁）。

fulfilment of tasks by data protection officer in order to ensure that data protection provisions are applied，viiiデータ保護オフィサーの任命と解任に関する，The Regulation of 10th December 2014 by the Minister of Administration and Digitalisation on data protection officer appointment and dismissal patterns である。

データ保護機関については，実施法案で名称の変更がなされることとなっており，また，任命権者等について議論がある点は前述のとおりである。

（2）適用対象

公的部門に関していえば，PDPA は，国家行政機関（state authorities），地方自治体の機関（territorial self-government authorities）に，国家または地方自治体の組織単位で適用される（PDPA3 条 1 項）。また，公的業務を行う非国家的主体[164]にも適用される（PDPA3 条 2 項 1 号。同 2 号は民間事業者等の定義）。

「管理者」の定義は 3 条に定める適用対象であって，個人データの取扱いの目的と手段を決定するもの，となっている（PDPA7 条 4 号）。

（3）目的外利用の状況（目的外利用の根拠規定，件数等）

① 目的外利用禁止の根拠規定

目的外利用の禁止に関しては，「データは，特定の正当な目的のために収集され，以下の第 2 項の規定に従い，意図された目的と適合しない方法で処理されない」（PDPA23 条 1 項 2 号）とされ，原則として禁止される。

PDPA23 条 2 項は例外を定めており，「データ収集時に意図された目的以外の目的でのデータの処理は，データ対象の権利と自由に違反しないことを条件に許可され」るとされ，「科学的，教訓的，歴史的または統計的研究のために用いる場合」（2 項 1 号），「第 23 条及び第 25 条の規定による場合」（2 項 2 号）が認められている。

このうち，23 条は，個人データの取扱いの原則に関する条項であり，公的機関との関係では，法令に基づく場合（23 条 1 項 2 号），公的機関がその権限を行使する際に必要な場合（23 条 1 項 4 号）などが関係する。また，24 条及び 25 条（利用目的の通知，24 条は直接取得，25 条は間接取得）との関係で公的機関と関連する場合としては，統計調査，世論調査等や 3 条 1 項（国家行政機関等）及び 3 条 1 項 2 号（公的業務を行う非国家的主体）のデータ管理者が法令上の根拠に基づいてデータを処理する場合が通知を不要とする場合として認められている（25 条 2 項 3 号及び 5 号）[165]。

---

[164] 公共調達法の対象である「エネルギー，水道，運送部門などの公的企業」などが該当するものと考えられる（公共調達法の内容につき，独立行政法人日本貿易振興機構（ジェトロ）「＜ポーランド法務情報＞ポーランド・公共入札ガイドライン」（2012 年 2 月）2 頁。

[165] なお，その他の例外条項としては，法令に基づく場合（24 条 2 項 1 号及び 25 条 2 項 1 号）及びデータ主体が既に利用目的についての情報を得ている場合（24 条 2 項 2 号及び 25 条 2 項 6 号）が認められている。

② 目的外利用禁止に関する執行件数等

公的部門における目的外利用に関する統計はみられないが，データ保護法の侵害に関しての異議申立て全体の統計としては，2012 年度の集計で，行政機関に対して 88 件，裁判所，検察庁，警察等に対して 44 件が，2013 年度の集計で，行政機関に対して 126 件，裁判所，検察庁，警察等に対して 56 件が確認されている[166]。

（4）本人関与の仕組み（開示，訂正，利用停止請求）と運用実態（請求件数等）

① 本人関与の仕組みについての一般的規定

PDPA32 条から 35 条が「第 4 章　データ主体の権利」を定めており，32 条 1 項は，「データ主体は，ファイルシステムに含まれる個人データの処理を制御する権利があり，特に以下の権利がある」として，各権利を列挙している。その内容は，システムが存在するかどうか及び，管理者の名称，住所等を知得する権利（1 号），システムに含まれるデータの利用目的，範囲，処理手段に関する情報を入手する権利（2 号），いつから個人データが処理されるのか及び，データの内容について分かりやすい形式で本人に通信を受ける権利（3 号），管理者が，国，貿易または職業上の機密として秘密を保持することを義務付けられていない限り，個人データの出所に関する情報を入手する権利（4 号），データが開示されている方法，特にデータの受信者または受信者カテゴリに関する情報を取得する権利[167]（5 号），第 26a 条第 2 項にいう決定を下す前提条件についての情報を取得する権利（5a 号），データが完全でなかったり，古かったり，正しくなかったり，法違反によって収集されたか，既に目的との関係で不要である場合に，完全にし，アップデートし，修正し，利用を一時的にまたは永続的に停止し，若しくは消去させる権利（6 号），第 23 条第 1 項第 4 号または第 5 号に規定する場合には，本人の特定の状況に応じて，書面によってデータの取扱いの阻止を要求する権利（7 号，管理者の対応義務について 35 条），第 23 条第 1 項第 4 号または第 5 号に規定する場合に，管理者がマーケティングのためにデータを処理したり，他の管理者にデータを転送することを拒否したりする権利（8 号），第 26a 条第 1 項に違反して解決された個々の事案を管理者に再検討するよう要求する権利（9 号）である。第 1 号から第 5 号の権利は 6 ヶ月に 1 回しか行使できない（5 項）。

データ主体の請求があった場合，管理者は，本人の権利及び，PDPA32 条 1 項 1 号ないし 5 号の情報について，書面で提供しなければならない（PDPA33 条 1 項 2 項）。

② 公的部門における本人関与の制限

公的部門に関係する本人関与の制限規定として以下のものが挙げられる。

---

166 European Commission Justice and Consumers “Sixteenth Report of the Article 29 Working Party on Data Protection Covering the year 2012” Adopted on 25 November 2014.p.90., European Commission Justice and Consumers “Seventeenth Report of the Article 29 Working Party on Data Protection Covering the year 2013” Published on 1 December 2016.p.96.

167 日本法的にいえば，第三者提供の方法及び提供先について知る権利ということになろうか。

まず，データの取扱いが科学的，教訓的，歴史的，統計的または記録目的のためのものであって，個人データの取扱いに関してデータ主体に通知することについて「不平等な努力」を伴う場合[168]，管理者は，通知を省略することができる（PDPA32 条 4 項)。

また，PDPA34 条がデータ主体の権利行使の制限について定めており，特に公的部門に関しては，機密情報の開示にあたる場合（1 号)，国防，安全保障，個人の生命または身体，公共の安全及び公的命令への脅威にあたる場合（2 号)，国の重要な経済的または財務的な利益への脅威にあたる場合（3 号）が該当する（4 号はデータ主体または第三者の重要な権利侵害に該当する場合)。

③ 公的部門における本人関与の実態

公的部門における本人関与に関する統計はみられないが，データ保護法の侵害に関しての異議申立て全体の統計としては，2012 年度及び 2013 年度の集計[169]で，それぞれ行政機関の取扱いに対して 88 件，裁判所，検察庁，警察等の取扱いに対して 44 件（2012 年度)，行政機関の取扱いに対して 126 件，裁判所，検察庁，警察等の取扱いに対して 56 件（2013 年度）が確認されている。

（5）執行における特別事情／救済措置の仕組み（第三者機関，訴訟等）とその運用実態（件数等）

① 執行

GIODO の検査官は一定の要件の元に検査を行うことができ（PDPA14 条及び 15 条)，検査後は検査結果通知書を管理者に交付する（16 条 1 項)。検査の結果，データ保護法違反が判明した場合，検査官は検査官長に対して PDPA18 条 1 項所定の是正措置を求め，検査官長は必要と判断した場合，是正措置を行う。

その内容としては，過失の是正（1 号)，個人データの修正，更新，訂正，開示，または開示しないこと（2 号)，収集された個人データを保護する追加措置の適用（3 号)，第三国への個人データの提供の中断（4 号)，データの保護措置またはデータの第三者への移転（5 号)，個人データを消去（6 号）等である（例示列挙)。

公的部門における執行に関する統計はみられないが，データ保護法の侵害に関しての異議申立て全体の統計としては，行政機関の取扱いに対して 88 件，裁判所，検察庁，警察等の取扱いに対して 44 件 (2012 年度)，行政機関の取扱いに対して 126 件，裁判所，検察庁，警察等の取扱いに対して 56 件（2013 年度）が確認されている。

---

168 「不平等な努力」を伴うとは，日本法でいえば「本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。」（個人情報保護法 16 条 3 項 4 号）に近いニュアンスの要件と考えられる。

169 前掲注 166

② 司法的救済，責任および制裁

データ主体は管理者のデータ保護法違反に対しては民事裁判所に民事訴訟を起こすことができるが，民法によるものであって，「個人の利益」が侵害されたことを主張立証する必要がある。通常の民事手続であり，データ保護法違反があったからといって民事責任が自動的に認められるものではない[170]。

データ主体は GIODO に申立てをすることによって，PDPA18 条 1 項の措置を求めることもできるが，必ず認められるわけではない[171]。

（6）公的部門の個人データ保護の法執行における刑事罰の位置づけ

① 刑事罰概観

PDPA49 条ないし 54a 条（8 章　制裁）が，刑事罰を定めている。罰金，自由制限刑または自由刑が定められており，その内容は以下のとおりである。

許されないデータ処理　罰金または 2 年以下[172]の自由制限刑，自由刑（49 条 1 項）
許されないセンシティブデータの処理　罰金または 3 年以下の自由制限刑，自由刑（49 条 2 項）
許可されていない開示　罰金または 2 年以下の自由制限刑，自由刑（51 条 1 項）
過失による開示　罰金または 1 年以下の自由制限刑，自由刑（51 条 2 項）
データの持ち出し，破損等（故意過失を問わない）　罰金または 1 年以下の自由制限刑，自由刑（52 条）
ファイリングシステムの未登録　罰金または 1 年以下の自由制限刑，自由刑（53 条）
データ主体への未通知　罰金または 1 年以下の自由制限刑，自由刑（54 条）
検査妨害　罰金または 2 年以下の自由制限刑，自由刑（54a 条）

罰金は自然人の場合 1 件で最大 1 万 PLN（ポーランドズロチ，1PLN≒30 円），最大 5 万 PLN。法人の場合，1 件で最大 5 万 PLN，最大 20 万 PLN とされている[173]。

② 公共部門と刑事罰

公共部門であっても刑事罰の除外規定はなく，ポーランド刑法の一般規定に委ねられるものと考えられるが，上記刑事罰規定は”a person”に科せられるとされている。

---

170 Arwid Mednis and Gerard Karp, “Data Protection & Privacy Poland” September 2017, https://gettingthedealthrough.com/area/52/jurisdiction/39/data-protection-privacy-2018-poland/
171 前掲注 18。
172 自由制限刑及び自由刑の短期は 1 月である（ポーランド刑法 34 条 1 項，37 条。山中敬一・葛原力三監訳「ポーランドの 1997 年新刑法典（翻訳）（一）」関西大学法学論集 50 巻 2 号（2000 年 6 月）127-169 頁）。
173 Olesinski I Wspolnicy Sp. K. “Personal data protection in Poland”.

（7）公的部門における個人データの保護に関する著名判決例

① 情報公開法と PDPA の関係に関する 2001 年 12 月 6 日最高行政裁判所判決

2001 年 12 月 6 日の最高行政裁判所判決は，個人データを含む行政記録の非公開を支持した。ある郡において，建築計画が，郡職員として建築許可を出しているのと同一人物によって作成されているという疑惑の追求のため，週刊誌編集部が建築許可に関する文書の閲覧を郡長に請求したところ，PDPA 上の個人データを含むとしてこれを認めず，最高行政裁判所でも許可しない決定が支持されたもの。1996 年最高裁判決は，プレスに，情報源にアクセスする権利を認めているが，PDPA の制定によって状況は変化し，個別的事件記録へのアクセスは制限されるとしたもの[174]。

② 2013 年 3 月 14 日最高行政裁判所判決（I OSK 620/12）

最高行政裁判所は，上記の判決において，PDPA23 条 2 号の処理の必要性（processing is necessary for the purpose of exercise of rights and duties resulting from a legal provision）を検討するにあたり，コミューン評議会には，その決議を公式のオンライン出版として公表する義務があるものの，この義務を履行するために，個人データを開示する必要はなかった，公的情報をオンライン出版に掲載する目的が，決議内容を含むコミューン評議会の公的活動の透明性であるのであれば，個人のデータを消去しても義務は達成されるとして，GIODO 及び一審裁判所の判断を支持した。

[174] 前掲注 163

第７　英国

１　英国の公的部門における個人情報保護制度の概要

（１）背景・経緯

①　背景

ウォーレン・ブランダイスが，「プライヴァシーの権利」の論考[175]で，その考察の基礎としたにもかかわらず，英国におけるコモンロー（慣習法）は，そもそも，プライバシーという概念を有していなかった。プライバシー権は，コモンロー上のトレスパス（不法侵入），ニューサンス（生活妨害），コンフィデンシャリティ（信任違反），名誉棄損などの観点から論じられていたにすぎなかった。

②　経緯

こうした中，1960 年代に入ると一般的なプライバシー権を創設しようという動きが出てきた。1961 年に貴族院に提出されたマンクロフト卿の「プライバシー権法案」をはじめとする三つの法案が，議員立法の形で議会に提出された（いずれも不成立）。また，1971 年には，政府は，ケネス・ヤンガー[176]を委員長とするプライバシーに関する委員会を発足させ，1975 年には，ヤンガー報告書[177]が公表された。この報告書は，コンピューターが個人データを取り扱う場合における 10 の原則をまとめたものだが，プライバシー権の立法化を勧告するには至らなかった。結局，1975 年に政府は白書を出して，「個人情報をコンピューターで取り扱っている者を，自分たちのシステムがプライバシーに対して十分な保護を行っていると判断を行う唯一の裁判官とさせ続けることはできない」として，データ保護局の法制化を認めることになった。このデータ保護局の構成等についてリンドップ卿[178]を議長とするデータ保護委員会が構成され，1978 年には，リンドップ委員会報告書においてデータ保護法の立法提案が行われたが，この提案は，採用されなかった。その後，1981 年には「個人データの自動処理に関する個人の保護のための条約（Convention for the protection individuals with regard to automatic processing of personal data done at Strasbourg on the day of January,1981）」が締結され，1984 年のデータ保護法 1984(以下，84 年法という)の制定のきっかけとなった。

そして，1995 年の EU 指令（「個人データ処理に係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95／46／E C 指令」（以下，EU 指令という）への対応として，英国は，1998 年にデータ保護法 1998（以下，98 年法とい

---

175 ブランダイス＝ウォーレン，外間　寛訳「プライヴァシーの権利」（戒能通孝，伊藤正己編「プライヴァシー研究」所収）（日本評論社，1962）9 頁

176 ケネス・ヤンガー卿(Sir Kenneth Younger)(1908-1976) 英国の労働党議員及びバリスター。諜報機関勤務のあと，政界入り。1959 年に政界を引退すると法律の改正等に従事する。

177 https://www.jstor.org/stable/1093890?seq=1#page_scan_tab_contents

178 ノーマン・リンドップ卿(Sir Norman Lindop)(1921-2014) 英国の教育管理者，化学者から，大学での教鞭をとるとともに管理も行い，1976 年から 1978 年に内務省データ保護の委員会の長を勤める。

う）を制定した。（2000 年 3 月）。英国では，個人データを取り扱う場合には，人権法（Human Rights Act 1998），情報の自由法（Freedom of Information Act 2000），調査権限法（Investigatory Powers Act2016），雇用法一般に留意しなければならないとされている[179]。特に，人権法は，ヨーロッパ議会の「人権及び基本的自由条約」の国内法化である。同条約の 8 条 1 項（「すべての者は，プライベートな生活，家族の生活，家庭及び通信を尊敬してもらう権利を有する」）は，個人データへのアクセスを含むと解されている。

その後，「個人情報の処理及び電子通信部門におけるプライバシーの保護に関する欧州議会及び理事会指令（ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)」（以下「e プライバシー指令」という。）の実施に関して，英国では，2003 年プライバシー及び電子通信（EU 指令）規則（PECR）（Privacy and Electronic Communications （EU Directive） Regulations 2003（PECR））が定められている。

（2）年表

	コモンローによる一般的保護
1950 年	欧州人権条約
1961 年	プライバシー権法案等　提出
1971 年	ヤンガー委員会成立
1975 年	ヤンガー報告書公表／政府による白書
1981 年	個人データの自動処理に係る個人の保護に関する欧州評議会条約
1984 年	1984 年データ保護法
1995 年	EU データ保護指令（1998 年施行）
1998 年	1998 年データ保護法
2000 年	1998 年データ保護法施行
2002 年	e プライバシー指令
2003 年	2003 年プライバシー及び電子通信（EU 指令）規則（PECR）
2016 年	GDPR　成立
2017 年 9 月 14 日	データ保護法案 2017 の公表

2　英国における GDPR のための対応について

（1）GDPR のための対応について

英国政府は，2017 年 8 月，GDPR に対応するよう 98 年データ保護法を改正する意図があることを明らかにするとともに[180]，法案の内容を明らかにした。英国において GDPR 対

[179] Peter Carey　”Data Protection”(4th ed)Oxford University press（2105）
[180] http://www.wired.co.uk/article/uk-data-protection-act-GDPR-data-privacy

応のための一般の関心は，きわめて高いものがある。以下，具体的に，英国における公的部門での GDPR 対応について，政府における対応と監督機関（情報コミッショナー）における対応とに分けて概観する。

（２）政府における対応について

①　概要

デジタル・文化・メディア及びスポーツ省は，2017 年 4 月 17 日に「GDPR 例外に関するコメント募集（Call for views on the General Data Protection　Regulation derogations）」を公開した。このコメント募集は，GDPR は，（それ自体が，規則であって，柔軟性に乏しいとはいうものの）特定の規定が適用される場合の例外規定について英国が裁量を行使しうることになることから，具体的に例外規定についての意見を求めるものである。ここで，英国政府は，事業に対して，不必要な負担を課さないように EU と交渉を行った旨の見解を明らかにしている。

このパブリックコメントは，回答方法・背景のあとに諮問項目が掲載されている。もっとも，この諮問項目自体は，テーマ 1　監督機関，テーマ 2　制裁，テーマ 3　コンプライアンスの顕示，テーマ 4　データ保護オフィサー，テーマ 5　保管及び調査，テーマ 6　第三国移転，テーマ 7　機微個人データ及び例外，テーマ 8　刑事制裁，テーマ 9　権利及び救済，テーマ 10　オンラインサービスについての子供の個人データ，テーマ 11　メディアにおける表現の自由，テーマ 12　データ取扱，テーマ 13　制約，テーマ 14　教会及び信仰集団に関するルールに大きくわけて，関連する条文のみが記載されている。このパブリックコメント募集に対しては，324 の応募があった。これらの意見は公開されている[181][182]。これらの意見のうち組織からの意見は 170 であり，うち，公的機関からの意見は，スコットランド裁判所，国立記録所（スコットランド，北アイルランド），地方公共団体（エセックス郡，リーズ市，サルフォード市，シェフィールド市）である。これらの意見については，特筆すべき意見は見当たらなかった。同 8 月 7 日には，同省からデータ保護法案の制定趣旨（statement of intent）が明らかにされている。9 月 14 日には，データ保護法案の条文が公表されている[183]。詳細については，以下のとおりである。

---

https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law

[181] General Data Protection Regulation - call for views responses（https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views）

[182] また，2017 年 5 月には，「GDPR のもとで，個人データ権の定量化の調査及び分析（Research and analysis to quantify the benefits arising from personal data rights under the GDPR）」という報告が公開されている。この報告は，GDPR の改正によって充実する情報主体の権利について，消費者は，それらが，採用されることについて，5－10 パーセントの価格に匹敵するものと考えていること，また，高額な罰金の存在が非常に高く評価されていることを述べている。

[183] 2018 年 3 月 8 日現在（庶民院　第二読会）（https://services.parliament.uk/bills/2017-19/dataprotection.html）

② データ保護法案

同法案は，7 部（194 条）と，18 の附則（Schedule）から成り立っている[184]。

法案の骨子は，(1) データ保護法 1998 の制裁強化を代表とする全般的／現代的枠組み，(2) GDPR 準拠の一般データ保護の新しい標準，データに対するコントロール，データの移転及び消去に関する新しい権利，(3) 世界をリードする研究，金融サービス，報道，法的サービスを継続しうるような例外規定の維持，(4) 刑事司法機関・国家安全組織において，被害者・証人・容疑者の権利を保持しながら，英国が直面する国際的な脅威に対して対抗しうるような枠組み，である。その中で，法案の主たる要素が個別の項目に分けて触れられている。具体的には，以下のとおりである。

（一般データ取扱［General data processing］）

データ保護法案の第 2 部は，一般のデータ取扱として，官民を通じたすべての一般的なデータ取扱に関して GDPR 標準を実装する規定を述べる。これには，英国の文脈において GDPR で使用される定義を明確にすること，センシティブな健康，社会福祉，教育データが，継続的に機密保持されたままで取扱を続けられ，保護の状況を維持することができるように確保すること，国家の安全の目的を含み，強力な公共政策の正当性がある場合において，データのアクセスと削除の権利に適切な制限を設けて，現在行われている特定の取扱を継続できるようにすること，オンラインでデータを取扱するのに親の同意が必要ない年齢を 13 歳に設定すること，などが含まれている。

なお，個人データ保護法案 7 条は，「公的機関（public authority）」及び「公的組織（public body）」の定義を有している（参考資料 1）。

（法執行機関における取扱［Law enforcement processing］）

データ保護法案の第 3 部は，法執行の目的のために，警察，検察，その他の刑事司法機関による個人データの取扱について別個定めをおいて規定している。

なお，この部分は，法執行指令（The Law Enforcement Directive（Directive EU2016/680））を英国法に国内法化するのに際して，データ保護法と単一の制定法で定めたという性格を有している。

具体的な構成としては，1 章が適用範囲及び定義（29 条ないし 33 条），2 章が原則（34 条ないし 42 条），3 章がデータ主体の権利（43 条ないし 54 条），4 章が管理者及び処理者（55 条ないし 71 条），5 章が第三国に対する移転（72 条ないし 78 条），6 章がその他（79 条ないし 81 条）である。

（情報サービスにおける取扱［Intelligence services processing］）

---

184 これは，発表当時の案の条文の数である。現時点では，208 条，附則 18 条である。なお，以下，便宜上，2017 年データ保護法案の条番号は，提案時点での条文の番号を用いる。

データ保護法案の第 4 部は，国家情報機関のサービスに関してなされる個人データの取扱に関して規制するものである。これらの規定は，新しく出現しつつある国家安全保障上の脅威に対して情報(諜報)コミュニティが引き続き取り組むことができるよう，適切な取扱のための手段を含むものとしており，最新の国際基準[185]への適合性を確保することが述べられている。国家安全に関連する事項は，GDPR の範囲外であるが，データ保護法に含まれて記述されている。

具体的な構成としては，1 章が適用範囲及び定義（82 条ないし 84 条），2 章が原則（85 条ないし 91 条），3 章がデータ主体の権利（92 条ないし 100 条），4 章が管理者及び処理者（101 条ないし 108 条），5 章が第三国に対する移転（109 条），6 章が例外（110 条ないし 113 条）となっている。

（規則及び執行［Regulation and enforcement］）

データ保護法案の 5 部は，情報コミッショナー，6 部は執行を定める。データ保護法を継続して規制し実施する情報コミッショナーの追加権限を定めるものであって，具体的には，最も重大なデータ侵害の場合，データ管理者及び処理者に対してより高い行政罰金を課し，最も深刻な違反に対して最大 17 百万ポンド（2000 万ユーロ）または全世界売上高の 4%を課す権限をコミッショナーに許容する，データ管理者または処理者が，データ主体のアクセス要求による開示を防止する目的でレコードを変更する犯罪に対して刑事訴訟を提起する権限を情報コミッショナーに付与する，という内容が含まれている。

③　保護強化点

保護強化点については，プライバシーインパクト評価（PIA）及びデータ保護オフィサーに関する準備がある。英国において，PIA は，個人情報の悪用によって個人への危害を軽減することができ，個人データを取扱するためのより効率的で効果的なプロセスを設計するのに役立つとされ，情報コミッショナーは，実務規範を公表している。今回，データ保護法案に関し，GDPR は，そのまま効力を有するとされている。データ保護法案においては，3 部 法執行取扱 4 章 管理者及び取扱者の 69 条において，法執行に関する個人データの取扱については，司法手続において取り扱う場合以外においては，データ保護オフィサーを指名しなければならないと明らかにされている。また，それ以外の場合における取扱については，データ保護法附則 6 条の 30 によって，データ保護に関するその他の国内法の定めに違反しないかぎりと修正された上で，効力を有し，一定の場合には，データ保護オフィサーを設ける必要があるとされている。

[185] 欧州委員会の「個人データの自動的取扱に関する個人の保護条約」（欧州評議会条約 108 号）をさす。

④　公的機関等に関連する例外規定の適用

一般的な処理において，若干の除外規定がある。

データ保護法案 24 条は，情報自由法公的機関（FOI public sector）[186]によって保持されているマニュアルの非構造的データに関して GDPR が適用されないものとしている（参考資料 1)。また，データ保護法案 26 条（1）は，国家安全及び防衛を理由として，それらの領域に GDPR(5 条(1)(a)，6 条，9 条等)の適用が除外されることについて規定している（参考資料 1）また，同 28 条は，GDPR9 及び 32 条（9 条は，特別カテゴリの個人データの取扱の禁止，32 条は，取扱の安全)が，国家安全の防衛のため，または，防衛目的のためには，適用されない旨を述べている（参考資料 1)。

（3）情報コミッショナーにおける GDPR 対応について

①　概要及び対応の局面

情報コミッショナー（ICO）においては，GDPR の適用について，「データ保護改革（Data protection reform)」として，専門的な解説を公表している。現時点までに，ICO は，「GDPR の概要（Overview of the General Data Protection Regulation (GDPR))」，「GDPR に備える，現在なすべき 12 のステップ（Preparing for the GDPR: 12 steps to take now)」，「GDPR 準備チェックリスト(Getting ready for the GDPR checklist)」「プライバシー通知，透明性及びコントロール（Privacy notices, transparency and control)」（プライバシー通知実務規範)，同意ガイドライン・パブリックコメント案，プロファイリング・パブリックコメント案，ビッグデータ分析（バージョン 2)，を明らかにしている。

また，政府のデータ保護法案 2017 に対して，情報コミッショナーが，”Data Protection Bill, House of Lords second reading – Information Commissioner’s briefing”[187]という書面を明らかにしている。

保護法案の中には，公的部門に対する特別の規定というものはないが，ICO の組織ごとに対する情報提供の一環として「地方公共団体のための GDPR 侵害報告の秘訣（GDPR personal data breach reporting tips for local government)」が公表されており注目に値する [188]。

②　地方公共団体のための GDPR 対応

情報コミッショナーは，2017 年 3 月に地域公共団体について，情報ガバナンス調査（Local

---

[186] データ保護法案 21 条(5)は，情報自由法公的機関について，2000 年情報自由法に定義されている公的機関，または，2002 年情報自由法(スコットランド)に規定されているスコットランドの公的機関と定義している。2000 年情報自由法は，その 3 条において，同法附則 1 条にさだめる組織すべて，もしくは，同法 5 条によって指定される組織を公的機関というとしている。なお，同法附則 1 条は，公的機関として，すべての政府機関，庶民院，貴族院，北アイルランド議会，ウェールズ議会，軍隊などをあげている。

[187] https://ico.org.uk/media/about-the-ico/documents/2172484/dp-bill-commissioner-briefing-lords-second-reading.pdf

[188] https://ico.org.uk/media/for-organisations/documents/2173111/gdpr-breach-reporting-tips-for-local-government.pdf

Government Information Governance survey results）を公表している[189]。この調査においては，GDPR に関しての重要なポイントが明らかになっている。

また，情報コミッショナーは，地方公共団体に対してのガイダンスを公表している。これらのガイダンスについては後述する。

（4）年表

2017 年 4 月 17 日	GDPR 例外に関するコメント募集（Call for views on the General Data Protection　Regulation derogations）　公表
5 月 25 日	情報コミッショナー　改革に備えるように演説
8 月 7 日	データ保護法案の制定趣旨（statement of intent）
9 月 14 日	データ保護法案公表
同日	情報コミッショナー　データ保護法案へのコメントを公表

3　GDPR 適用前の公的部門に関する個人情報保護制度の運用実態等

（1）概要

①　公的部門を規律する法律

EU のデータ保護指令は民間部門と公的部門を区別しておらず公的部門の特殊性は，その国内法において個別に定められる。具体的に個別に定められている事項のうち検討に値する事項としては，適用対象，目的外利用の状況，本人関与の仕組み，執行・救済，刑事罰の状況，注目すべき司法判断などがある。

②　公的部門における個人情報保護を監督する機関

情報コミッショナー[190]は，独立した監督機関であり，国内的にも国際的にも重要な役割を果たしている。情報の適正な取扱を促進し，データ管理者における行動指針を推進している。なお，従来はデータ・コミッショナーという名称であったが，現在では，英国における情報の自由法における監督業務をも行うために情報コミッショナーという名称に変更になっている。

EU 指令における監督機関の権限はすでに，英国においては 1984 年データ保護法によってデータ保護登録局が有していたものである。データ保護登録局は，1998 年データ保護法によって，データ保護コミッショナーと名前を変えて存在し続けることになった。具体的な任務としては，

ｉ　データ管理者によるよい実務慣行を促進すること，特に，データ管理職に法の要求

189 https://ico.org.uk/media/2013721/local-government-information-governance-survey-results-20170320.pdf
190 http://www.dataprotection.gov.uk

の遵守を促進すること，

ii　法及びその働きの情報を広めること

iii　適当なガイダンスのための行動規範の制定

iv　要求されるデータ管理局の登録簿を維持すること

v　法令のもとで犯された犯罪に関し人を告訴すること

などが挙げられている。

情報コミッショナー事務局の組織構成は，添付の付録 1 のとおりである。

また，情報コミッショナーにおいては，公的部門，特に地方公共団体におけるデータ保護に対して情報提供のホームページを準備[191]して，豊富な情報を提供している。提供されている具体的なガイドラインとしては，

地方公共団体情報共有及びデータ保護チェックリスト[192]

地方公共団体から議員に対する個人情報開示[193]

公的機関被傭者に関する個人データ請求－情報の自由法環境情報規則[194]

個人情報（40 条及び規則 13）－情報の自由法環境情報規則[195]

などがある。

（2）各項目の分析

①　適用対象機関

98 年データ保護法は，民間部門であると公共部門であるとを問わず適用がなされる。

②　保護対象データの範囲

適用対象について，98 年データ保護法は，「(略) (c) 関連するファイルシステムの部分または，それを構成する意図をもって記録される」情報と定義している。従って，データ保護法はマニュアルデータにも適用される。また，同(e)において，公的機関(public authority)によって保持されている場合には，いわゆる非構造的なデータについても，データ保護法の適用対象となるとされている（後述)。

③　目的外利用の状況（目的外利用の根拠規定，件数等）

英国法においては，目的外利用の原則禁止は，個人データ取扱の第 2 原則の中に含まれるものと解されている。具体的には，「個人データは，1 つまたは 2 つ以上の特定された合法的な目的に限り取得されるものであり，かかる目的に矛盾する方法により処理されない。」

---

191 https://ico.org.uk/for-organisations/local-government/

192 https://ico.org.uk/media/for-organisations/documents/2664/leadership-data-protection-checklist.pdf

193 https://ico.org.uk/media/for-organisations/documents/1432066/disclosure-of-personal-information-by-local-authorities-to-councillors.pdf

194 https://ico.org.uk/media/for-organisations/documents/1187/section_40_requests_for_personal_data_about_employees.pdf

195 https://ico.org.uk/media/for-organisations/documents/1213/personal-information-section-40-and-regulation-13-foia-and-eir-guidance.pdf

（98 年データ保護法　別表 1　第 2 原則）とされている。第 2 原則におけるデータの取扱の目的については，データ主体に対する「適時の通知」ないしはコミッショナーに対する通知によって特定されることになる。

データの目的外での使用及び開示についての特別の規定は存在しないが，相当するのは，この第 2 原則である。というのは，目的外での使用及び開示の適法性は，個人データの目的外での利用目的が，第 2 原則のいう「合法的な目的」に該当し，データの取得された目的と両立しうるか否かという点により判断されるからである。そして，上記 EU 指令 7 条，13 条の規定で触れられている適用除外については，個別の規定によって定められている。具体的には，98 年データ保護法附則 2 のパラ 5 が，この個別の規定に該当する。同規定は「裁判の実現，議会の機能行使，政府機関の機能，公的性質の機能の実現のため，に処理される場合には，合法的な目的のために処理される」ものとしている。結局，公共部門における個人データの目的外利用の可否は，公共部門において個人データが，「合法的な目的」のために取り扱われているのかという問題に帰着することになる。

英国においては，地方自治体における情報共有について労働年金省から「Guidance for local authorities on the use of social security data」が公開されており（2014 年 4 月）[196]，具体的な問題についてのガイダンスが示されている。このガイダンスは，この「合法的な目的のための処理」が，実際にどのように法的な枠組みのもとでなされているのかについての理解を助けてくれる。

同ガイダンスによれば，個人情報の利用と共有について，公共団体が有している権限を規制する法源は単一ではなく，公共団体の活動を定める法（行政法），1998 年人権法及びヨーロッパ人権条約，コモンローの信任義務違反の不法行為，1998 年個人情報保護法，ヨーロッパ法によって定まるとしている（ガイダンス 4 頁）。

行政法において，社会保障についての主たる制定法は，1992 年社会保障管理法（Social Security Admin Act，SSAA 法）と 2012 年社会福祉改革法（Welfare Reform Act，WRA 法）である。SSAA 法 7B 条は，社会保障情報を住宅福祉のために利用することを認めている。また，これら以外にも，1999 年福祉改革及び年金法，2002 年税金信用法，2005 年教育法などが根拠となる。

また，これらのような明確な行政法上の根拠がない場合においては，同意を取得することが，データ共有の合法的な根拠となる。

労働年金省と地方自治体における情報共有については，公共サービスネットワーク（PSN）によってなされており（2013 年より），住宅福祉及び労働年金福祉のために地方公共団体が社会保障データを利用できる。具体的には，介護手当，死別手当，障害者手当などがそれで

196 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307156/data-sharing-guide-april-14.pdf
なお，この点に関連するガイダンスとして，労働年金省と地方公共団体との労働年金省覚書，地方公共団体情報システムガイドがある。

ある。また，地方税減額スキーム，住宅サポート，福祉上限のためなどに利用することが可能である。

なお，調査の限りでは，公的機関における目的外利用の件数というデータは見当たらなかった。

④　本人関与の仕組み（開示，訂正，利用停止請求）と運用実態（請求件数等）

（本人関与の仕組みについての一般的規定）

84 年データ保護法には情報のコピーを得る権利，誤りを訂正し損害賠償を得る付随的な権利が規定されている。

さらに，98 年データ保護法では，与えられるべき情報の範囲が拡大された。それに伴い，保管されている情報へのアクセスを意味する「主体アクセス」という用語が拡張され，「主体情報」という用語が用いられるようになった。この主体アクセスは，具体的には，「主体のアクセス権」「処理の停止権」「ダイレクト･マーケッティング停止権」「自動的意思決定に関する権利」「損害賠償権」「訂正･停止･消去･破棄請求権」「コミッショナーに対する法律違反評価請求権」を含んでいる。

これらについて，簡単に論じると以下のとおりである。

「主体のアクセス権」[197]

これは，データ主体に関して，個人データが取り扱われている場合には（その取扱の確認についても返答の義務がある），そのデータ取扱の性質(目的，開示される人ないしはカテゴリー，情報源，自動的な手段で取り扱われるときの取扱の論理構造，データ自体を構成する情報に関して，その内容を明らかにさするように求めることができるという権利である。98 年法では，アクセスを請求しているデータ主体に対しては，それらのデータの源(どのような経緯で取得したかという情報)についてもデータ管理者が利用しうるすべての情報が与えられなくてはないとされている。データ管理者は，要求が書面でなされたときに限り，返答する義務がある（第 7 条（2））。ただし，「国家安全」「第三者のデータ」「犯罪捜査及び徴収目的」「健康･社会保障データ」「規制についての行動」「調査，歴史，統計」「その他の例外」などの例外があり，これらの場合には，そもそもこれらの規定の適用がなかったり，返答する義務がなかったりする。

「データ主体の異議申立権」

異議申立権①－ダイレクト･マーケッティング停止権

ダイレクトマーケティングとは，「手段の如何を問わず，広告またはマーケッティングの資料を特定の個人に対して伝達すること」をいうが，データ主体は，この目的のための取扱を停止等することを求めることができる（98 年データ保護法 11 条（1））。公的部門との関

[197] 前出　Carey　（2015）166 頁

係が薄いため，詳細は省略する。

異議申立権②－取扱の停止権

データ保護指令 14 条は，データ主体の権利として，データの取扱を停止することができる旨を規定している（参考資料 2)。英国においては，98 年データ保護法 10 条（1）項により，ダイレクトマーケティング以外の取扱に関しては，データ主体は，損害や抑圧を引き起こす可能性があるということを理由にして取扱の停止を要求することができるとしている。

EU 指令はフランスの立法例に見られる規定を採用し，仕事における評価，クレジットの信用力，信頼性等に関して，個人にとって不利な決定をする際には，自動的なデータ取扱のみに基づき行われてはならないという規定を設け，自動的なデータ取扱の問題点を指摘している（データ保護指令 15 条「自動取扱による個人に関する決定」)。98 年法も，データ主体は，データ管理者に対し，個人に重要な影響を与える決定については，自動的なデータ取扱によって行わないようにすることを，書面によって要求できるとしている（98 年データ保護法 12 条 1 項)。もし，こうした個人に重要な影響を与える決定が，自動的なデータ取扱によってなされた場合，データ管理者は，個人に対して，自動的なデータ取扱によって決定がなされたことをできる限り早急に伝えなければならず，また，データ主体は，通知を受け取った後に，書面によって，自動的なデータ取扱以外の根拠に基づく判断を求めることができる（同条 2 項)。

98 年法は，上記の一般ルールに対する例外として，データ主体と契約を締結するどうかを決定する場合や契約を遂行したりする場合に際して，決定が主体にとって望ましいものであるときや，その適切な利益を保護するための手段が取られる場合については，1 項の規定が効力を有しないことを定めている（同条（6）項，(7）項)。データ管理者が自動的意思決定の禁止について違反したと認められる場合には，データ主体はデータ管理者がその意思決定を見直し，または自動的なデータ取扱以外を根拠とする新しい決定を出すことを裁判所に要求することができる。裁判所は，データ主体からの要求に応じ，データ管理者に対し，かかる命令を行う。(同条（8）項)。

（公的部門における拡張の規定）

非構造的な個人データは，通常，個人データとされていないが，公的機関によって保持された場合においては個人データとして扱われ，公的部門に対するアクセス権が拡張されている。これは，2000 年情報の自由法によって，1998 年データ保護法 1 条（1）に定義（e）が加えられたことによるものである（参考資料 3)。これにより，非構造的データについても，データ主体がデータを特定した場合には，アクセスにかかるコストが適切な限度を超過しないかぎり，要求に応える（返答及び開示）必要があることとなっている（以下，9A 条（2)。参考資料 3)。

（公的部門における本人関与の制限）

上記 EU 指令 13 条の規定が定める例外は，実際の法律の中にも規定されている（IV 部）。主体のアクセス権を例にとると，「国家安全」（28 条）「第三者のデータ」（7 条(4)），「犯罪捜査及び徴収目的」（29 条），「健康･社会福祉事業」（30 条）「規制についての行動」（31 条）「調査，歴史，統計」（33 条），「立法により公衆が利用可能となる情報」（34 条）「その他の例外」（35 条ないし 39 条），などについての例外規定が存在する（参考資料 3）。

（公的部門における本人関与の実態）

公的部門におけるデータ主体のデータへのアクセスの実態について，統一的なデータは，存在していない。

⑤　執行における特別事情／救済措置の仕組み（第三者機関，訴訟等）とその運用自体（件数等）

（執行）

一般論

データ保護指令 28 条の監督機関の定めに対応して，1998 年データ保護法の 6 条（1）は，1984 年法におけるデータ保護登録官事務局としていた部局が，データ保護コミッショナー（制定当時）として存在することで継続するものとされている（参考資料 3）。なお，本条項は，2000 年情報自由法等の制定に伴い，若干の改正がなされている（参考資料 3）

法律違反評価請求権（Request for assessment）

98 年法の 42 条は，コミッショナーに直接取扱によって影響を受ける当事者からの評価要求を受領した場合に，その取扱はデータ保護法に従っているかを評価する義務を課している。評価がなされた事実は，申立人に通知され，評価の結果や処置についても開示されることとなる。

情報通知（Information notices.）

98 年法 43 条は，コミッショナーは，データ管理者に対して，情報通知，すなわち調査の対象に関する特定の情報を限られた時間内にコミッショナーに対して供給すべきことを要求する権限を認めている（参考資料 3）。この権限は，情報通知といわれる。データ管理者が，この情報通知に対応することを怠った場合には犯罪行為となり，意図的にもしくは重大なる不注意で虚偽の情報を対応した場合についても同様である。

執行通知（enforcement notices）

98 年法の下においては，執行通知が定められている（同法 40 条。参考資料 3）。コミッショナーは，データ管理者においてデータ保護原則違反がなされたときに，その違反条項を

特定し，状況を改善するための手段を特定して記載した執行通知を送達する。データ管理者が，この通知を順守しない場合には犯罪を構成することになる（執行通知に対する不遵守（同法 47 条（1））。データ管理者はこの通知に不満がある場合には，データ保護審判所に意味を申し立てることができ，この申し立てが認められれば通知の効力は停止されることになる。

金銭的制裁通知（Monetary Penalty Notices）[198]

2010 年 4 月から，情報コミッショナーには，データ保護原則の重大な違反に対して金銭的制裁を科す権限が与えられた。その根拠条文は，データ保護法 55A 条である（参考資料 3）。

強制監査／政府機関における拡張

98 年データ保護法は，その 41A 条において，評価通知（assessment notice）を定めている（参考資料 3）。これは，データ管理者が，政府機関等の場合（(2) 参照）に，強制的にコミッショナーの監査を認めさせるものである。

居所への立入及び捜索令状

98 年法の 50 条及び附則 9 条は，コミッショナーに対し，巡回判事に対して居所への立入及び捜索令状を求めることができるとしている（参考資料 3）。添付の令状が，コミッショナーもしくはそのスタッフに対し，用具の検査・検証，捜査及びテストを可能とし，そこで見つかったいかなる書類及び物に対する閲覧または押収の権能を与えているのである（同（3）項）。

（司法的救済，責任及び制裁）

損害賠償権

98 年データ保護法は，損害を被ったデータ主体は算定可能な経済的損失の形態をとった損害は証明され，さらに関連する心理的圧迫についても損害賠償が認められる（同法 13 条（1）項及び（2）項）としている。なお，心理的圧迫に対して，どの程度の損害賠償が認められるかという点については，ケースによるとされている。一般的な場合では，£5,000 から£10,000 が，感情に対する損傷を与えた評価として認められている。すべての事案について，データ管理者は法律違反を避けるための合理的な注意がとられたという抗弁をなすことができる（同（3）項）。

---

198 金銭的制裁とは，情報コミッショナーは司法手続を経ずに科し得る金銭的制裁であり，刑罰としての罰金とは区別される民事的制裁である。（消費者庁「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」におけるイギリスの章（加藤隆之）の説明による。
(http://www.caa.go.jp/planning/kojin/h22report1.pdf)

訂正･停止･消去･破棄請求権

データ保護指令 32 条（2）の規定に対応して，98 年データ保護法 14 条（1）は，個人データの訂正・停止・消去・破棄に関する請求権を規定する（参考資料 3)。また，この規定に関して，98 年データ保護法は，84 年法を拡張している。98 年データ保護法により裁判所は，データが不正確であり，訂正，停止，消去または破棄[199]がなされるべきであると決定した際には，通知を行うのが合理的であると考えられる場合は，データ管理者が，データがすでに開示されたすべての第三者に対して，その変更の詳細を通知すべきであると命令することができるようになった（同条（5）項)。

公的部門における個人データ保護に関して, 興味深い事件として, Robertson 事件（Brian Reid Beetson Robertson v Wakefield Metropolitan Council,Secretary of State for the Home Department [2001] EWHC Admin 915)事件がある。この事件は，電子選挙人登録局の事務員が，電子選挙人名簿（electoral registration）を，そのコピーを要求した組織すべてに渡していたという事件である。

Representsation of the People Act1983 のもとの規則においては，組織が電子選挙人登録局に対して要求した場合には，登録情報のコピーを販売しなければならなかった。実際は，登録情報が，営利組織によって信用参照目的やダイレクトマーケティング目的に利用されていた。Robertson 氏が，営利組織に売却されうるという事項について同意しているということに異議を唱え，電子的登録から自らの情報を削除するように申し出て，この申出が認められたという事件である[200]。

（3）公的部門の個人データ保護の法執行における刑事罰の位置づけ

① 刑事罰概観

98 年データ保護法は，「個人データの不法な取得等（unlawful obtaining etc. of personal data)」を行った個人に対する処罰規定がある（同法 55 条（1))。また，個人データの売却（申出を含む）行為（同 55 条（4)），主体アクセスの強要行為（同 56 条)，コミッショナーにおける開示（同 59 条（1)），令状の執行に対する妨害を行う・助力を怠ること（別表 9 パラ 12）などが刑事罰によって禁止されている。また，情報コミッショナーによる法の執行を妨害する行為，具体的には，執行通知に対する不遵守（同法 47 条（1)），情報通知・特別情報通知に対する虚偽の陳述（同 47 条（2））も刑事罰の対象となる。

これらの罪の法定刑は，略式起訴による有罪判決の場合は「法定最高額（the statutory maximum)」を超えない罰金であり，正式起訴による有罪判決の場合は罰金額の上限がない（60 条（2）項)。1991 年刑事司法法（Criminal Justice Act 1991）917 条によると，略式起訴による有罪判決の場合の「法定最高額」は 5000 ポンドである。そして，55 条違反の罪を犯した者に対して拘禁刑を科す旨の命令を主務大臣が発布することが可能である。

---

199 条文においては，訂正（rectify)，停止（block)，消去（erase）または破棄（destroy）になる。
200 前出 Carey （2015）91 頁

② 公共部門と刑事罰

上記刑事罰に該当する行為は，個人のみならず，組織（会社・地方公共団体）によっても犯されうる。中央政府については，官僚が，起訴されることになるが，部門自体は，起訴を免れる（同 63 条）。

（4）監督機関の組織と執行

① 情報コミッショナーにおける公的部門に対する執行の状況

情報コミッショナーにおける年次報告書[201]及び情報コミッショナーのホームページにおける具体的な執行の事例報告によれば，データ保護に関する懸念[202]は，全体で，18,300 件ほど寄せられており，うち，300 件は，検索エンジンに対する，いわゆる忘れられる権利に関するものであって，3 分の 1 は，検索結果の消去を求めている。また，600 件が，家庭用監視カメラが近所に対して問題，いやがらせを引き起こしているという案件である。データ管理者に対して行動がとられなかったのが 33.4%，データ管理者の行動が求められたのが 20.3%，懸念が提起されたのが 15.8%となっている。また，部門ごとを見ると，一般企業は 13%，ヘルスケア関連が 10%，金融関係 10%，地方公共団体が 10%，中央政府が 5%，警察・刑事が 5%，教育が 4%，電気通信 4%，インターネット 4%となっている。

② 公的部門に対する執行の具体例

公的部門に対する執行の具体例として，興味深い事案は以下のとおりである。

（司法大臣［Secretary of State for Justice］事件（2017 年 12 月））[203]

情報コミッショナーが司法大臣に対して，個人データの主体的アクセス要求に対する内部のシステム，手続及びポリシーが，データ保護規定を遵守するものとは考えられないと認定し，2018 年 10 月 31 日までにデータ保護規定を遵守するよう命じた事案である。

（Nilesh Morar 事件（2017 年 9 月））

Nilesh Morar は，Nuneaton マジストレイト裁判所において，個人データを違法に取得した罪で起訴された。被告は，当時は，レスター市役所で働いており，成人ソーシャルケア部門の利用者であるという機微な情報を含む 349 人の個人データを彼の個人アドレスに，データ管理者である雇用主の同意なしに送付した。 Morar 被告人は，データ保護法 55 条のもとでの犯罪に有罪を認め，160 ポンド（日本円にして約 2 万 5000 円）の罰金，訴追費用 364.08 ポンド，被害者サーチャージ 20 ポンドを支払うように命じられた。

---

201 ”Information Commissioner’s Annual Report and Financial Statements 2016/17 ” https://ico.org.uk/media/about-the-ico/documents/2014449/ico053-annual-report-201617-s12-aw-web-version.pdf

202 以下は，2016-2017 報告書による（19 ページ以下）。

203 https://ico.org.uk/media/action-weve-taken/enforcement-notices/2172935/secretary-of-state-for-justice-en-20171221.pdf

（Nottinghamshire 郡（2017 年 8 月））[204]

Nottinghamshire 郡は，個人情報を 5 年間もネットにおいてアクセスしうる状態においていたとして 70,000 ポンド（約 1091 万円）を支払うように命じられた事件。

（ロンドン・イズリントン自治区（同））[205]

イズリントン自治区は，駐車チケットシステムで，駐車違反や交通犯罪のチケットを発券しており，ユーザーは，自動車登録番号とチケットナンバーを入することにより，ログオンして CCTV の画像やビデオを閲覧でき，また，URL を操作することで，ユーザーが交通犯罪について異議がある場合に，当局に送付する書類をみることができた。システム設計上の瑕疵から，8 万 9000 人の情報が，第三者もアクセスできる状態になっており，安全な状態にしていなかったとして，情報コミッショナー事務局に 7 万ポンド（約 1091 万円）を支払うように命じられた。

（５）公的部門における個人データの保護に関する著名判決例

公的部門における個人データの保護に関して，裁判所で扱われた著名な事件は，以下のとおりである。

（R. v Brown［1996］2WLR203）[206]

債権回収会社を経営する友人を助けるために，警察官 Brown が，警察のコンピュータデータベースに貯蔵されている情報をコンピュータ・スクリーンに呼び出すよう同僚に依頼したところ，警察官は，1984 年法所定の，登録簿に記載された目的を超える個人データの使用の罪で告発されたというものである。

（R. v Rooney [2006]　EWCA Crim1841）

被告人 Jacqueline Mary Rooney は警察職員（スタフォードシャー警察の労務管理部門に勤務）であり，姉妹が他の職員と別れたことから，その職員の個人データにアクセスして情報をその姉妹（第三者）に開示したとして有罪になった事案である[207]。

---

[204] https://ico.org.uk/media/action-weve-taken/mpns/2014734/mpn-nottinghamshire-county-council-20170831.pdf
[205] https://ico.org.uk/media/action-weve-taken/mpns/2014671/mpn-london-islington-20170807.pdf
[206] https://www.ato.gov.au/law/view/document?DocID=JUD/*1996*1AC543/00001
[207] Carey p.251

参考資料－条文

1　2017 年データ保護法案

7 条（「公的機関（public authority）」及び「公的組織（public body）」の意味）

⑴　GDPR の目的のため，以下（及び以下のみは）連合王国の法のもと「公的機関」及び「公的組織」は，

（a）2000 年情報自由法によって定義される公的機関

（b）2002 年情報自由（スコットランド）法によって定義されるスコットランド公的機関

（c）（2）項及び（3）項に従って，規則に基づいて Secretary of State によって特定された組織

⑵　⑴項に該当する機関もしくは団体は，公的利益を遂行するもしくは公的権限を行使する場合にのみ「公的機関」または「公的組織」となる。

⑶　Secretary of State は，規則によって，(1)(a) or (b) に記載されている者を GDPR の適用に関して，「公的機関」または「公的組織」ではないとすることができる。

⑷　（略）

24 条（情報自由法公共機関によって保持されている非構造的データ）

⑴　適用 GDPR 及び⑵によって掲載されている規定は，この章の規定が，21 条⑵（情報自由法公共機関によって保持されている非構造的データ）によって適用されるものには，適用されない

⑵　規定とは

（a）　適用 GDPR の 2 章（原則）―

（ｉ）　5 条⑴（a）から（c）（e）及び（f）（正確性原則以外の取扱に関する原則）

（ii）　6 条（適法性）

（iii）　7 条（同意の条件）

（iv）　8 条⑴及び⑵（児童の同意）

（ｖ）　9 条（特別のカテゴリーの取扱）

（vi）　10 条（刑事判決に関するデータ）

（vii）　11 条⑵（っしきべつせいを要求しない取扱）

（b）　適用 GDPR の 3 章（データ主体の権利）

（ｉ）13 条⑴ないし⑶（データ主体から収集した個人データ，提供される情報）

（ii）14 条⑴ないし⑷（データ主体以外から収集される個人データ，提供される情報）

（iii）20 条（データポータビリティの権利）

（ⅳ）21 条⑴（取扱の異議）

(c)　適用 GDPR の 5 章,44 条ないし 49 条（個人データの第三国もしくは国際機関に対する移転）

(d)　本法 170 条，171 条（附則１ 7 のパラグラフ 1⑵参照).

⑶　適用 GDPR の本条⑷項の規定は，この章の規定が，21 条⑵によって，以下に定める指名，退去，支払，懲戒，superannuation その他個人的な関係について適用されるものには，適用されない

(a)　軍隊における従事

(b)　クラウンもしくは公共機関のもとでの公務・労務

(c)　（略）

⑷　規定とは，

(a)　Ⅱ章及びⅢ章の残りの規定（原則及びデータ主体の権利）

(b)　Ⅳ章（管理者及び処理者）

(c)　Ⅸ章（特定の処理状況）

⑸　管理者は，以下の場合においては，この章の規定が，21 条⑵によって，適用される個人データに関して適用 GDPR の 15 条⑴ないし⑶に準拠する義務はない。

(a)　当該条項にもとづく要求が，個人データの記載を含まない場合，または，

(b)　管理者が，適合るためのコストが個人データに関して，適切な最高額を超えてしまう限りの場合

26 条　国家安全及び防衛による除外（National security and defence exemption）

⑴　適用 GDPR または⑵項における本法の規定は，以下の場合において本章が適用される個人データについて適用されない

(a)　国家安全を維持する目的のために除外されることが必要とされる場合

または

(b) 防衛目的のために除外されることが必要とされる場合

28 条　国家安全及び防衛：9 条ないし 32 条の適用の改変（National security and defence: modifications to Articles 9 and 32 of the applied GDPR）

⑴　適用 GDPR の 9 条⑴（特別カテゴリの個人データ取扱の禁止）は，以下の取扱がなされる場合において，本章が適用される個人データの取扱を禁止するものではない

(a)　国家安全を維持する／防衛目的のための場合

及び

(b)　データ主体の権利と自由に対して適切な安全策が取られる場合

⑵　適用 GDPR の 32 条（取扱の安全）は，以下の場合において，データ管理者／処理者が個人データを取り扱う個人データに関する限りにおいて適用されない

(a)　国家安全を維持する目的の場合

(b)　防衛目的の場合.

⑶　適用 GDPR の 32 条が適用されない場合において，管理者または処理者は，個人データの取扱から生じるリスクに対して適切なセキュリティ手段を実装しなければならない

⑷　⑶項の目的のために，個人データがすべてまたは一部において自動的手段で取り扱われる場合には，管理者または取扱者は，リスクの評価ののちに，以下を配慮した手段を採用しなければならない

(a)　取扱に利用するシステムに対する無権限の取扱もしくは無権限の干渉を廃除する手段

(b)　行われる取扱の詳細を精確にとり行うことを確かにする手段

(c)　取扱の機能が適切になされるシステムで，中断があったときには，回復がなされうることを確かにする手段

(d)　利用されているシステムが取扱の不具合が起きたとしても，保存されている個人データが破壊されないのを確かにする手段

2　EU データ保護指令

14 条

第 7 条（e）及び（f）に規定された場合には，国内法に別段の規定がある場合を除き，いつでも自己に関するデータの取扱いに対して，自己の特定の状況に関連するやむにやまれない正当な理由を根拠として，異議申立てを行うことができること。適法な異議申立てがあった場合には，管理者によって始められた取扱いに，当該データを含むことはできない。

3　1998 年データ保護法

1 条　基本的解釈規定（Basic interpretative provisions）

⑴　本法において，文脈が特段に求めることがない限り，「データ」とは，以下の情報をいう

(a) ないし (d)　　省略

(e)　公的機関によって保持されているものであって，(a) ないし (d) パラグラフに該当しない情報

6 条（コミッショナー及び審判所）－制定時のオリジナル文言

⑴　1984 年データ保護法 3 条⑴（a）によってデータ保護登録官事務局として設立された事務局は，本法の目的のためにデータ保護コミッショナー事務局として存続するものと

し，本法において，データ保護コミッショナーは，「コミッショナー」とされる。

6 条（コミッショナー）－現行法

⑴　本法及び 2000 年情報の自由法の目的のために情報コミッショナー（本法において「情報コミッショナー」とされる）として知られる官吏をおく。

9A 条　公的機関に保持されている非構造的個人データ（Unstructured personal data held by public authorities.）

⑴　本条において，「非構造的個人データ」とは，1 条⑴における「データ」の定義のパラグラフ（e）に該当するものであって，個人もしくは，そのクライテリアを参照することによって構造化されている個人に関する情報のセットもしくは，その一部とされているもの以外のすべての個人データをいう。

⑵　公的機関は，データの記載とともになされた要求でないかぎり，非構造的データに関して 7 条⑴を遵守する義務はない。

⑶　請求において，データ主体が記載されていたとしても，公的機関は，適切な限度を超えたデータに関するものとなる限りにおいて非構造的データに関して７条（１）を遵守する義務はない

⑷　⑶条は，データが，7 条⑴パラグラフ（a）を遵守するのにかかると考えられるコストが，適切な限界を超過しない限り，公的機関は非構造的データに関して同パラグラフの義務から免れるものではない

12 条　自動的意思決定に関する権利（Rights in relation to automated decision-taking）.

⑴　人は，いつでも，データ管理者に対する書面による通知で，同人に対して，その人に対して重要な影響を与える決定が，データ管理者によって，もしくは，そのために，個人データの自動的な取扱のみをもって，なされないことを求める権利がある。その人は，たとえば，労働における仕事ぶり，信用，信頼性，または，行為などの彼に関する事項の評価のための個人データの情報主体である。

⑵　⑴項のもとでの通知がなされずに⑴で論じられる取扱にもとづく個人に重要な影響を与える意思決定がなされる場合，

（a）　データ管理者は，かかる根拠において決定がなされたということを可及的速やかに通知しなければならず，かつ，

（b）　個人が，データ管理者から，通知を受領した２１日以内に，データ管理者に対して書面でもって，当該根拠にもとづく決定を再考する，もしくは，新たな決定をなす，ことを求める権利を有する

⑶　以下略

なお，申請人にかかる個人データが不正確であるという申請を認める場合には，裁判所は，データ管理者に対して，それらのデータ及びそのデータ管理者の管理するデータであって裁判所が，不正確なデータに基づいていると認識する他の個人データすべてに対して訂正・停止・消去・破棄を命じることができるとされている（同⑻項の趣旨）。

28 条　国家安全（National security）

⑴　個人データは，国家安全の維持のために除外が必要とされる場合には，以下の規定の適用を除外される

（a）　データ保護原則

（b）　Ⅱ部，Ⅲ部，Ⅴ部

（c）　54A 条及び 55 条

29 条　犯罪捜査及び徴収目的（Crime and taxation）

⑴　以下の目的のためになされる個人データの取扱は，以下の項における事項を損なうことがありうる限りにおいて，第 1 原則（附則 2，附則 3 における条件の遵守要求を除く）及び 7 条の適用から除外される。

（a）　犯罪の予防または探知

（b）　犯罪者の逮捕また訴追

（c）　税金・義務または，同種の賦課の評価または徴収

⑵　以下，略

30 条　健康・教育・社会福祉事業（Health, education and social work.）

⑴　内務大臣は，命令によって，データ主体の肉体的・精神的健康／状態に関する情報を構成する個人データに対して，情報主体の規定の適用の除外，または，その変更をなすことができる

⑵　内務大臣は，以下の個人データに関して，情報主体の規定の適用の除外，または，その変更をなすことができる

（a）　データ管理者が保有者である，教師である，学校である，学校の生徒である／あった者に関して情報を組成する個人データ

または，

（b）　データ管理者がスコットランドにおける教育機関である，霜害機転によって提供される教育を受け，／受けいれた者に関する情報を構成する個人データ

⑶　内務大臣は，以下の場合の処理されている情報に関して，情報主体の規定の適用の除外，または，その変更をなすことができる

（a）　政府部局，地方公共団体，任意組織，命令によって指定される組織によって処理される場合

かつ

(b)　データ主体もしくは個人に関して，社会福祉事業を行うにあたり，処理された，もしくは，処理されている場合

ただし，内務大臣は，本項のもと，それらの規定の適用が，社会福祉事業を遂行するのに支障をきたしうると判断する場合を除く。

31 条　規制についての行動（Regulatory activity.）

⑴　本項が適用される釈放機能（discharging functions）のために取り扱われる個人データは，それらの機能によって適切な機能に支障をきたすことがありそうだという範囲において，情報主体の規定の適用から除外される

⑵　⑴項は，以下のための機能に関して適用される

(a)　公衆を以下から保護するため

（ⅰ）銀行，保険，投資，または，その他の金融サービスまたは，企業経営陣における人員の不正直，処理のミス，その他の不適切な行為，または，不適任・無能による経済的損失

（ⅱ）解雇行為または破産による経済的損失

（ⅲ）専門的職務もしくはその他をなしうるとされている者の不正直，処理のミス，その他の不適切な行為，または，不適任・無能

(略)

(e)　勤務している人の健康，安全，福祉を確保するため

(f)　労働者の行為に関して，労働者以外の人の健康または安全に対して内外をとわず発生するリスクから保護するため

34 条　立法により公衆が利用可能となる情報（Information available to the public by or under enactment.）

データが，データ管理者が，公表にせよ，査察，もしくは，その他の手法であると，また，無料であると，対価支払がなされると否とを問わず，2000 年情報自由法に含まれる立法以外の立法のもと，公衆に対して利用可能になすことを義務づけられている場合には，個人データは，以下の規定の適用を除外される

(a)　情報主体の規定

(b)　データ保護の第 4 原則及び 14 条⑴ないし⑶

及び

(c)　非開示規定

40 条　執行通知（enforcement notices）

⑴　もし，コミッショナーが，データ管理者が，データ保護原則に違反した，もしくは違反

していると判断した場合において，データ管理者に対して，原則，もしくは，問題となっている原則を遵守し，

(a)　通知において特定された時間以内に，特定された手法を採用する，または，採用するのをやめる

もしくは，

(b)　特定された時間の後に，すべての個人データ，または，通知において特定された記述の個人データの取扱をやめる，または，特定された目的のための／特定された方法による取扱をやめる

ように求める通知（本法において「執行通知」という）を送達することができる。

⑵　執行通知を送達するかを決定するのに際しては，コミッショナーは，違反が，個人に対して損害もしくは迷惑を惹起している，もしくは，しそうかどうかを考慮する

⑶　第 4 データ保護原則（注：正確性・最新性の原則）違反の場合において，データ管理者に対して，その保有するデータの訂正･停止･消去･破棄命じる執行通知の場合には，データ管理者に対して，保有するすべてのデータの訂正･停止･消去･破棄を命じ，かつ，コミッショナーから不正確とみえるデータにもとづいていたという意見の表明を差し控えることを命じるができる。

⑷　以下略

41A 条　評価通知（Assessment notices）

⑴　コミッショナーは，データ管理者に対して，⑵項の限りにおいて，コミッショナーに対して，データ管理者が，データ保護原則を遵守していた，または，遵守しているかどうかを決定するために通知（本法において「評価通知」という）を送達することができる。

⑵　本項においてデータ管理者が，

(a)　政府の部局

(b)　内務大臣によってなされる命令によって本項のために指名される公的機関

(c)　同命令によって指名される個人

⑶　評価通知とは，データ管理者に対して

(a)　コミッショナーに対して特定の場所に立ち入ることを認める

(b)　コミッショナーに対してその場所において特定の記述がなされた文書を指し示す

(c)　コミッショナーに対して，その場所において，特定の記述がなされた情報を機器を用いて見読することができるように支援する

(d) コミッショナーの

（ⅰ）コミッショナーの特定する文書の複写

（ⅱ）コミッショナーが見読しうるように支援された情報（を要求された様式で）の複写

をなす要求を遵守する

(e)　その場において，コミッショナーに，記述で特定された機器もしくは物を指し示す

(f)　コミッショナーが，指し示された，もしくは，見読するよう支援された文書，情報，機材，物を査察し，検査することを許容する

(g)　コミッショナーが，その場においてなされる個人データの取扱を観察するのを許容する

(h)　特定されたデータ管理者のために個人データを取り扱う人（または，事情聴取に応じる人の）に対する事情聴取を可能にする

42 条　評価請求権

⑴　個人データの取扱によって，その取扱が，本法の定めに従ってなされた，もしくは，なされつつあるか，どうかに関して評価することを，直接的に影響を受ける，もしくは受けうると信じる者は，コミッショナーに請求することができる。

43 条　情報通知（Information notices.）

⑴　もし，コミッショナーが，

(a)　個人データの取扱に関する 42 条にもとづく請求を受けた場合，もしくは

(b)　データ管理者が，データ保護原則を遵守している，もしくは，遵守しつつあるかどうかを決定するという目的のために情報をもとめることが合理的な場合においてデータ管理者に対して，コミッショナーに請求に関する，または，原則の遵守に関する特定の情報を提供することを求める通知を送達することができる。

50 条　立入及び査察の権利（Powers of entry and inspection）

附則 9（Powers of entry and inspection）は効力を有する

と定めている。なお，附則 9（令状の発行［Issue of warrants］）は，

1⑴　巡回区裁判所または地方判事（治安裁判所）において，コミッショナーが，宣誓書で

(a)　データ管理者がデータ保護原則のいずれかに反している

もしくは

(b)　98 年法に，反する犯罪をなしている

と疑う合理的な根拠があり，証拠がその情報において特定された場所で見つかるであろうとした場合において，納得するときは，⑵項とパラグラフ 2 に従って，コミッショナーに対して令状を発布することができる

と定めている。

55A 条　コミッショナーの金銭制裁通知を課す権限（Power of Commissioner to impose monetary penalty）

⑴　コミッショナーはデータ管理者に対し，データ管理者による，

（a）　4 条⑷項の重大な違反（serious contravention）があり，

（b）　当該違反が，現実的な損害または危険を生じさせる可能性があり，

（c）　⑵または⑶項が適用される場合に

金銭的制裁通知（monetary penalty notice）を送達することができる

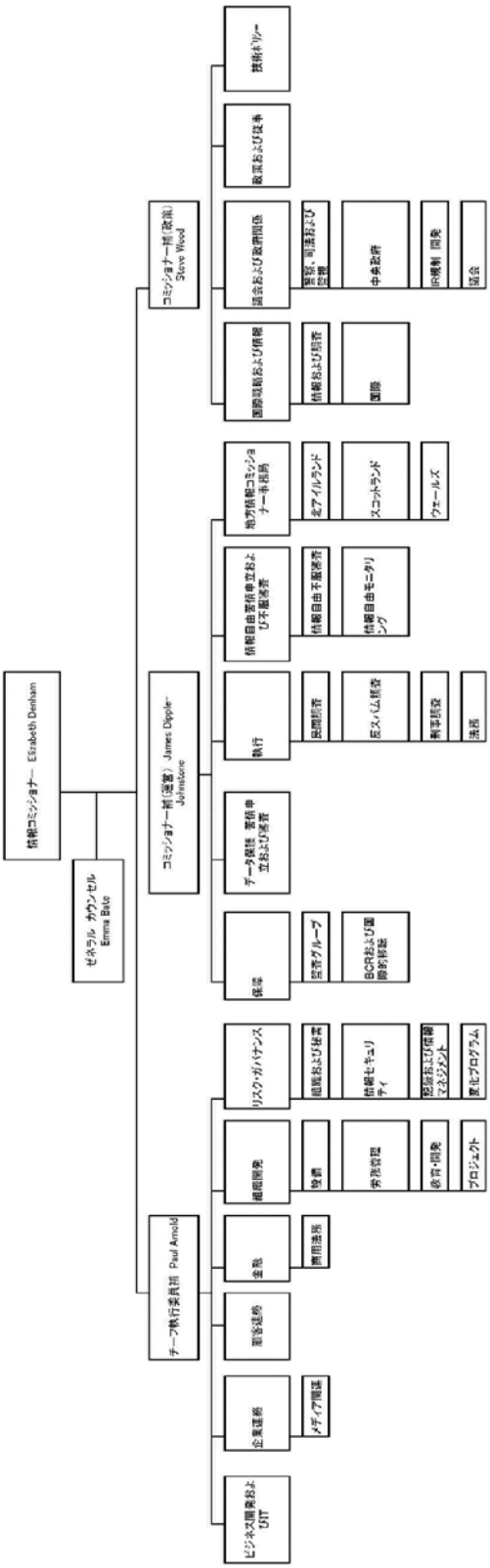
⑵　その違反が，熟慮に基づく（deliberate）場合

⑶　もし，データ管理者が，

（a）　違反が発生する危険性があり，かつ，そのような違反が，現実的な損害または危険を生じさせる可能性があるが，

（b）　違反を予防するための合理的な手段（reasonable steps）が採られていない場合

付録１　情報コミッショナー組織図



【執筆者一覧】

（五十音順）

※所属等は本調査報告書執筆時のもの

板　倉　陽一郎（弁護士［ひかり総合法律事務所］）

第２部・第１（ベルギー）

第２部・第６（ポーランド）

高　橋　郁　夫（弁護士［駒澤綜合法律事務所］）

第２部・第４（アイルランド）

第２部・第５（イタリア）

第２部・第７（英国）

宮　下　　紘（中央大学総合政策学部准教授）

第１部

第２部・第２（ドイツ）

第２部・第３（フランス）