論　　説

個人情報の刑法的保護の可能性と限界について（４）

佐　藤　結　美

目　　次

第５章　ドイツ法における個人情報保護

第１節　連邦データ保護法の概要

本章では、ドイツにおける連邦データ保護法[1](Bundesdatenschutzgesetz.

[1] ドイツ連邦データ保護法の邦訳は、平松毅『個人情報保護―理論と運用』(有信堂・2009年) 221 ～ 255頁、藤原靜雄「改正　連邦データ保護法 (2001年５月

略称はBDSG）について扱う。

具体的な検討の前に、データ保護法が成立するまでの背景について述べる[2]。イギリス・フランス等の諸外国と同様に、情報化によって個人情報が頻繁に取り扱われるようになったことが立法の背景となっている。コンピューターの情報処理によって、再び独裁者や国家が市民の権利を脅かすことのないように、個人情報保護法制を整備する必要があるとの問題意識から、1970年10月、ヘッセン州（Hessen）において世界で初めての個人情報保護法が採択された。そして、ドイツ連邦政府は1977年に連邦データ保護法を制定し、1978年に施行された。

その後の1983年12月、連邦憲法裁判所による「国勢調査判決」[3]が出され、自己の情報をどこまで公開するかということを自ら決定する「自己情報決定権（Recht auf informationelle Selbstbestimmung）」が基本権として承認された。本判決によると、誰が、いつ自己についての情報を知ったのかを市民が知ることができない社会秩序は、自己情報決定権とは両立しない。「人格の自由な発展」の基本権は、自己の個人情報の提供と使用を自身で決定する個人の権利を保障しているので、特に情報流通の透明性が保障され、個人の記録は秘密の伝達経路の中に隠されてはならず、その手段を本人が統制できなければならない、と解されている。この判決を受けて1990年に連邦データ保護法が改正され、1991年に施行された。1990年法における主な改正事項には、①公的機関によって発生し

23日施行）」季刊行政管理研究99号（2002年）76 ～ 94頁を参照した。

[2] データ保護法成立までの経緯については、野村武司「改正ドイツ連邦データ保護法」社会科学研究（山梨学院大学社会科学研究所・1993年）123 ～ 160頁、山下義昭「ドイツ連邦データ保護法の改正と残された課題（１）（２）」クレジット研究27号（2002年）184 ～ 193頁、クレジット研究29号（2003年）91 ～ 110頁、平松・前掲注（１）256頁以降と、藤原靜雄「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」（2008年３月）におけるドイツの章・112頁以降を参照した。URL: http://www.caa.go.jp/seikatsu/kojin/h21report3.pdf.

[3] BverfGE 65, 1. 人口、職業、住居、事業所などの国勢調査が、ドイツ基本法２条１項における「人格の自由な発展を求める権利」に反するか否かが争われた事件である。

た人格権侵害を含む損害に無過失損害賠償責任が認められたこと、②民間機関の損害賠償責任は無過失ではないものの立証責任が当該機関に科せられたこと、③保護の対象となる記録に文書記録が含まれるようになったこと等がある。

続いて、1995年 EU データ指令を受けて、2001年に再度の改正が行われた。EU 指令に伴って改正された事項につき、特に重要なものは次のとおりである。まず、① EU 指令８条を受けて、ドイツ連邦データ保護法３条９項にも「特別な種類のデータ」（いわゆる「センシティブデータ」である。詳細は後述する）という概念と、その取り扱いのための例外的適法化要件が導入された。特別な種類のデータを収集するための適法化要件は、EU 指令における要件を援用するものとなっている。②1990年データ保護法は、第三者機関である連邦データ保護監督官と監督官庁に対して、データ保護法違反の十分な根拠のある場合に限って監査を認めていたが、EU 指令28条３項にはそのような制限が設けられていないので、2001年データ保護法ではこの規定が削除され、権限が拡張されている。

また、EU 指令に依拠していない改正事項として、ビデオ監視がある。一般市民が立ち入ることのできる場所におけるビデオ監視は、2001年改正前のドイツの公的または民間機関によって行われていたが、2001年改正法６ｂ条によって、ビデオ監視に法的根拠が与えられるようになった。６ｂ条によると、ビデオ監視は①公的機関の職務遂行のため、②住居権の行使のため、③正当な利益を行使するために、具体的に確定された目的につき必要性があり、かつ、本人の保護に値する利益が優越するとの根拠がない場合に限って許容される。

このように、連邦データ保護法は EU データ指令を受けて多くの改正がなされたが、2009年８月14日にも法改正が行われ、2009年９月１日に施行されている。2009年の法改正では、個人信用調査会社へのデータの提供（28ａ条）と、本人との契約関係の開始・実行・終了について判断する目的で、本人との将来的な契約関係の可能性を示す数値（Wahrscheinlichkeitswert）のデータを収集または利用する（いわゆるスコアリング）ための条件（28ｂ条）についての規律が新しく設けられた。

第１項　基本事項について

データ保護法の目的は、「自己の個人データの扱いによって人格権（Persönlichkeitsrecht）を侵害されることから、個人を保護すること」である（１条１項）。

本法では「個人データ（Personenbezogene Daten）」が保護の対象となり、個人データの収集（Erhebung）と処理（Verarbeitung）および利用（Nutzung）が規制対象となる（１条２項）。ここでいう「収集」は本人に関するデータを入手することであり（３条３項）、「処理」は個人データを蓄積（Speichern）、変更（Verändern）、提供（Übermitteln）、封鎖（Sperren）、または消去（Löschen）することである（３条４項）。そして、「利用」は「処理」に関係しない個人データのあらゆる使用である（３条５項）。

本法３条１項によると、個人データは「特定のまたは特定しうる自然人（本人）の人的または物理的状況に関する個別の記載事項（Einzelangaben）」と定義される。この条文からは、個人に関する事実的な事項のみが対象となるように思われるが、個人についての評価を含む全ての情報が含まれると広く解されている[4]。そして、イギリス1998年データ保護法とフランス1978年法と同様に、ドイツ連邦データ保護法にも、取り扱いに特別な配慮を必要とする「センシティブ情報」という概念がある。連邦データ法３条９項では、「特別な種類の個人データ（Besondere Arten personenbezogener Daten）」と呼ばれており、「人種的および民族的出自、政治的意見、宗教的または哲学的な信条、労働組合への加入、健康または性生活に関する事項」と定義されている。特殊な種類の個人データの適法な取り扱いのための要件については後述する。

この法律において、本人には次の権利が認められている。それは、①自己業務目的で本人に知らせることなく個人データが蓄積された場合に、データの種類や収集・利用・処理の目的と責任機関について通知（Benachrichtigung）を受ける権利（33条１項）、②自己に関して蓄積された個人データ、データが譲渡される相手、データが蓄積される目的などについての開示（Auskunft）請求権（34条）、③データの訂正（35条１

[4] Gola/Klug, Grundzüge des Datenschutzrechts, C.H.Beck, 2003, S.40.

項)、消去 (35条２項)、封鎖 (35条３項) の権利、④異議を申し立てる (widersprechen) 権利 (35条５項、20条５項) である。

第２項　個人データの収集・処理・利用の適法化要件

（１）一般的な個人データについて

①官民共通の規定

個人データの取り扱いが認められるためにはいくつかの条件がある。まず、官民共通の規定について述べる。個人データを収集・処理または利用するためには、データ保護法もしくは他の法規定によって許容され、または命じられているか、または本人が同意している必要がある（４条１項)。次に、個人データは原則的に本人から収集されなければならない。本人以外からの収集が認められるのは、法規定が定め、または不可避であるとしている場合、本人からの収集が均衡を欠く過度の出費を要すると考えられる場合などであって、保護に値する重大な本人の利益が侵害される根拠 (Anhaltspunkte) が存在しない場合である（４条２項)。

次に、自らまたは委託によって個人データを収集、処理または利用する公的および民間機関は、データ保護法の規定の実施、特にこの法律の附則 (Anlage) に挙げられた要請の実施を保障するために、必要な技術的・組織的措置 (technischen und organisatorischen Maßnahmen) を講じなければならない(９条１文)。このような措置が必要とされるのは、もっぱら、達成しようとする目的と費用が「適切な比例関係 (angemessenen Verhältnis)」にある場合である（９条２文)。

９条の附則は以下の通りである。

個人データが自動的に処理または利用される場合、行政庁内または企業内の組織は、データ保護の特別の要請に適合するように編成されなければならない。その際、特に、保護される個人データまたはデータの範疇の種類に応じて、次のような措置が講じられなければならない。

１　個人データが処理または利用されるデータ処理施設 (Datenverarbeitungsanlagen) に無権限者が立ち入るのを禁止する（立ち入りの監督)

２　データ処理システムが無権限者に利用され得るのを防ぐ（アクセスの監督)

３　データ処理システムの利用権限者が、もっぱらその介入権限に服するデータのみに介入できることと、個人データが処理、利用の際および蓄積後に無権限で読まれたりコピーされたり、変更または除去され得ないことを保障する（介入監督）

４　個人データが電子工学的な伝送の際、またはその輸送中、またはデータ記録媒体への蓄積中に、無権限で読まれたりコピーされたり、変更または除去されたりする可能性のないことと、データ伝送の装置を通して､いかなる機関への個人データの提供が予定されていたかを審査し、確定することが可能であることを保障する（伝送の監督）

５　個人データの、データ処理システム内への入力、変更または除去の有無、およびその行為者を、事後的に審査、確認することが可能であることを保障する（入力の監督）

６　委託によって処理される個人データは、委託者の指示通りにのみ処理することができるということを保障する（委託の監督）

７　個人データが、偶然の破壊または喪失から保護されていることを保障する（処理の監督）

８　異なる目的のために収集されたデータは、別々に処理できることを保障する

②公的機関の個人情報処理に関する規定

続いて、公的機関による個人情報処理の適法化要件は、データ保護法13条から16条に規定されている。まず､13条１項によると､当該個人データを知ることが責任機関の任務遂行のために必要な場合に限ってデータの収集が許容される。次に、個人データの蓄積、変更および利用は、責任機関の権限に属する任務の遂行のために必要であり、かつ、データの収集目的のために行われる場合に限って認められる。データの収集が事前に行われない場合、データは蓄積された目的のためにのみ変更または利用され得る（14条１項）。そして、他の目的のための蓄積、変更または利用は、本人が同意している場合、本人の利益のためになることが明らかであり、他の目的のためであることを知ることによって本人が同意しないと想定する理由がない場合、第三者の権利の重大な侵害を予防（Abwehr）するために必要な場合等には例外的に認められる（14条２項）。

15条と16条は公的機関によるデータの提供について規定する。まず、15条１項によると、公的機関から別の公的機関へのデータの提供は、（ｉ）当該データ提供が、提供する機関、もしくはデータの提供を受ける機関の所掌事務を遂行するために必要である場合と、（ii）利用が許容されるためのデータ保護法14条所定の要件が満たされている場合に許される。次に、16条１項によると公的機関から民間機関へのデータ提供は、（ｉ）当該データ提供が、提供する機関の権限に属する任務を遂行するために必要であり、かつ、利用が許容されるためのデータ保護法14条所定の要件が満たされている場合、または、（ii）データの提供を受ける第三者が、提供されるデータを知ることにつき正当な利益のあることを疎明（darlegen）し、かつ、本人が提供させないことについて保護に値する利益を有しない場合に許容される。

③民間機関の個人情報処理に関する規定

続いて、民間機関による個人情報処理の適法化要件については、データ保護法28条以下で規定されている。

28条１項は、自己の業務目的の遂行のための手段として個人データの収集、蓄積、変更もしくは提供し、または利用することは、次のいずれかに該当する場合に許容されることを規定する。

（ｉ）本人との契約関係または契約類似の信頼関係のために使用する場合

（ii）責任機関の正当な利益を保護するために必要であり、かつ、処理もしくは利用させないことについて、本人の保護に値する利益が優越すると推定する理由がある場合

（iii）データが一般にアクセス可能であるか、または責任機関がそれを公表することが許されている場合。ただし、処理または利用させないことについての本人の保護に値する利益が明らかに優越する場合はこの限りではない。

続いて、29条１項は第三者提供の目的で個人情報を収集・蓄積・変更するための条件について、29条２項は提供が許容されるための条件について規定する。

29条１項によると、宣伝（Werbung）、興信所（Auskunfteien）、名簿

業者（Adresshandel）に資するデータの収集、蓄積、変更は、次の場合に許容される。

（ⅰ）収集、蓄積または変更を拒否することについて、本人の保護に値する利益があると推定する理由がない場合

（ⅱ）データが一般に公表されている情報源から収集することができるか、または責任機関が公表してよい個人データである場合。ただし、収集、蓄積、変更を拒否することについて本人の保護に値する利益が明らかに優越する場合はこの限りではない。

（ⅲ）28条ａの１項または２項の必要条件が充足される場合。28条ａ２項第４文におけるデータは、収集または蓄積されてはならない。28条１項第２文と３項３ｂは適用されるべきである。

次に、29条２項は、１項による目的の範囲内での提供は（ⅰ）データを提供される第三者が、当該データを知ることについて正当な利益を疎明する場合で、かつ（ⅱ）データの提供を拒否することについて、本人の保護に値する利益があると推定する理由がない場合に許容される旨を定めている。

（２）特別な種類の個人データについて

第１項で述べた通り、データ保護法では人種や宗教に関するデータは「特別な種類の個人データ」として区別されている。ここでは、特別な種類の個人データの適法な取り扱いのための条件について概要を述べる。

第一に、特殊な種類の個人データが収集、処理または利用されるためには、明示的（ausdrücklich）で当該データと関連する同意が必要である（４ａ条３項）。これは、公的機関と民間機関に共通の条件である。

①公的機関による情報収集等に関する規定

続いて、13条２項によると、以下のいずれかに該当する場合には、公的機関による特殊な種類の個人データの収集が認められる。

（ⅰ）法令の規定があるか、または重要な公益上の理由により、収集が不可欠である場合

（ⅱ）本人が４ａ条３項に基づいて同意した場合

（ⅲ）本人の身体的または法的な理由から同意を与えることができな

い場合であって、本人の、または第三者の生死に関わる利益（lebenswichtiger Interessen）の保護のために必要な場合

（iv）本人が公表したことが明確な個人データが問題になっている場合

（v）公的な秩序に対する著しい危険を防止するために必要な場合

（vi）公共の福祉（Gemeinwohl）に対する重大な不利益の防止、または公共の福祉上重大な利益の保護のために必要な場合

（vii）健康への配慮（Gesundheitsvorsorge）、医学上の診断（medizinischen Diagnostik）、健康管理（Gesundheitsversorgung）または公衆衛生業務（Gesundheitsdiensten）の取り扱いもしくは公衆衛生業務のために必要であり、かつ、これらのデータの処理が医師または同様の守秘義務（Geheimhaltungspflicht）を有する者によって行われる場合

（viii）学術研究（wissenschaftlicher Forschung）のために必要であり、かつ、研究計画の実施についての学術上の利益が、データ収集を拒否する本人の利益に著しく優越し、かつ研究目的が他の方法で達成できないか、またはその達成のために均衡を欠く過度の出費を要する場合

（ix）防衛（Verteidigung）、または危機の克服（Krisenbewältigung）もしくは紛争の阻止（Konfliktverhinderung）もしくは人道的措置（humanitäre Maßnahmen）の領域における連邦の公的機関の、国家を超えた義務もしくは国家間の義務（wischenstaatlicher Verpflichtungen）の遂行のために必要な場合

ここまでは、特別な種類の個人データの収集に関する規定であるが、14条５項１号・２号は、このようなデータの蓄積・変更・利用の際の条件について定めている。14条５項１号によると、上記13条２項１号から６号と９号による収集が認められる場合に蓄積･変更･利用が許容され、14条５項２号には、学術研究の実施に必要な場合、という13条２項８号と同一の規定が置かれている。そして、14条６項は、上記13条２項７号の目的のために特別な種類の個人データの蓄積・変更・利用は、13条２項７号に掲げられた者（医師または医師と同様の守秘義務を有する者）に適用される守秘義務規定に従う旨を規定する。このように、13条２項の規定の内容とほとんど重複しており、特別な種類の個人データの収集、蓄積、変更、利用には共通のルールが適用されるといえる。

②民間機関による情報収集等に関する規定

データ保護法28条６項から９項は、民間機関による特殊な種類の個人データの取り扱いについての条件を定めている。

28条６項によると、自己の業務目的のための特殊な種類の個人データの収集、処理、利用は、本人が４ａ条３項による同意をしない場合には以下の各号の場合に認められる。

（ⅰ）本人の身体的または法的な理由から同意を与えることができない場合であって、本人の、または第三者の生死に関わる利益の保護のために必要な場合

（ⅱ）本人が公表したことが明確な個人データが問題になっている場合

（ⅲ）法律的な請求権（rechtlicher Ansprüche）の主張（Geltendmachung）、行使（Ausübung）、または防御（Verteidigung）に必要であり、かつ、収集、処理、利用を拒否する本人の保護に値する利益が優越することを推定させる根拠が存在しない場合

（ⅳ）学術研究のために必要であり、かつ、研究計画の実施についての学術上の利益が、データ収集を拒否する本人の利益に著しく優越し、かつ研究目的が他の方法で達成できないか、またはその達成のために均衡を欠く過度の出費を要する場合

続いて、28条７項１文によると、「健康への配慮、医学上の診断、健康管理または公衆衛生業務の取り扱い、もしくは公衆衛生業務のために必要であり、かつ、これらのデータの処理が医師または同様の守秘義務を有する者によって行われる場合」には特別な種類の個人データの収集が認められる。そして、28条７項２文によると、上記28条７項１文における目的のためにデータを処理・利用する場合には、１文に掲げられた者（医師および医師と同様の守秘義務を有する者）に適用される守秘義務規定に従う。

28条８項１文によると、上記６・７項以外の目的のためには、28条６項１号から４号まで、または28条７項第１文の要件のもとでのみ、提供・利用することができる。そして、28条８項２文によると、このようなデータの提供と利用は、国家および公共の安全（staatliche und öffentliche Sicherheit）にとっての重大な危険（erheblichen Gefahren）の防止のた

めに、ならびに著しく重大な犯罪行為（Straftaten von erheblicher Bedeutung）の追求（Verfolgung）のために必要な場合にも認められる。

28条９項１文によると、政治的、哲学的、宗教的または労働組合的で、営利目的を追求しない組織は、組織活動にとって必要である限り、特別な種類の個人データを収集、処理または利用することができる。第１文の規定は、組織の構成員（Mitglieder）の個人データ、または組織の活動目的との関係で、組織と定期的な接触（regelmäßig Kontakte）を有する者の個人のデータにのみ適用される（28条９項２文）。

４ａ条３項に基づく本人の同意がある場合に限り、この個人データを組織外の者または他の機関に提供することができる（28条９項３文）。

29条５項によると、民間機関が提供目的のために、特別な種類の個人データの業務上収集と蓄積を行う場合には、上記28条６項から９項までの規定が準用される。

このように、公的機関と民間機関では重複する条件もあるが、民間機関の方が、特別な種類の個人データを扱うことが認められるための例外が若干多く設けられている（上記28条９項には政治的・哲学的・宗教的または労働組合的な団体のためのデータ処理の規定があるが、この条項は公的機関によるデータの取り扱いには設けられていない）。

第３項　連邦個人データ・情報自由保護監察官

イギリス1998年データ保護法とフランス1978年法と同様に、ドイツ連邦データ保護法においても、情報処理等を取り締まる第三者機関が置かれている。しかし、イギリスが情報コミッショナーを、フランスがCNILを置いているのとは異なり、ドイツでは単一の監督機関が国内のデータ処理等を一括して監督するのではなく、監督機関が３層に分けられている。ドイツの連邦公的機関と、民営化された鉄道・郵便・通信事業は「連邦データ・情報自由保護監察官（Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. 以下、連邦監察官とする）」によって監督され、州の公的機関は州のデータ保護監察官（Landesdatenschutzbeauftragte）によって監督される。そして、州の民間機関は監督官庁（Aufsichtsbehörde）または州のデータ保護監察官による監督を受ける。まず本項では、連邦公的機関と一部の民営化事業を

監督する連邦監察官の制度概要について述べる。

（１）連邦監察官の地位

連邦監察官は、連邦政府（Bundesregierung）の提案に基づき、ドイツ連邦議会（Deutsche Bundestag）の過半数以上の可決によって討議なしに（ohne Aussprache）[5]選出される（22条１項１文）。選出される際に35歳以上であること（22条１項２文）以外に、連邦監督官の資格要件についての規定はない。

連邦監督官は独立して（unabhängig）職務を行い、データ保護法にのみ従う（22条４項２文）。2009年データ保護法22条４項３文には、「連邦監察官は連邦政府の法的監督の下にある」という規定が存在したが、2015年の法改正によって削除されている。そして、法改正前の22条５項には、「連邦監察官は連邦内務省の下に置かれる。連邦監察官は連邦内務省の職務監督を受ける」と規定されていたが、2015年法改正により「連邦監察官は最上級連邦官庁の一つである」と規定されるに至った。法改正以前も実際には連邦監察官は独立して職務を遂行していたのであるが、監察官はあらゆる外的影響を受けてはならないとする2010年、2012年の欧州司法裁判所の判決を受けて、現在の条文となった[6] [7]。これらの条文は、連邦監察官が独立した第三者機関であることの根拠となる。内務大臣の指揮命令に服することはなく、データ保護法のみに拘束される。

（２）連邦監察官の職務

①苦情処理

データ保護法21条では、連邦公的機関による自己の個人データの収集、処理、利用の際に自己の権利を侵害されたと考える者は誰でも、連邦監察官に助力を求めることが認められている。各個人に与えられた苦情申

[5] 連邦データ保護法2015年２月25日改正（2016年１月１日施行）によってこの文言が追加された。

[6] 渡辺富久子「【ドイツ】連邦データ保護監察官の独立性を強化」外国の立法263巻２号（2015年）27頁。

[7] C-518/07, C-614/10

立ての権利により、苦情処理は連邦監察官の主要な任務となっている。連邦監察官は、職務において打ち明けられた事実や申し立てを行った人物について証言を拒否する権利があり（23条４項）、職務上知り得た事実について守秘義務がある（23条５項）。このような証言拒絶権と守秘義務によって、個人の苦情申立ての権利は担保されている。

②監督と調査

データ保護法24条１項では、連邦の公的機関がこの法律の規定とデータ保護に関する他の法律の規定を遵守しているか否かを、連邦監察官が監督する（kontrollieren）ことが定められている。連邦監察官とその委任を受けた者は、監督任務の遂行にあたって、次の権限を与えられている（24条４項）。

１　質問への回答（Auskunft）、並びに24条１項による監督と関連したあらゆる書類（Unterlagen）、特に蓄積されたデータ（die gespeicherten Daten）とデータ処理プログラム（Datenverarbeitungsprogramme）を閲覧すること

２　すべての執務室（Diensträume）にいつでも立ち入ること

連邦監察官は、監督の対象となった公的機関にその結果を報告することになっている（24条５項１文）。連邦監察官はこの報告において、データ保護の改善（Verbesserung）、特に個人データの処理または利用の際の瑕疵（Mängeln）の除去について提案することができる（24条５項２文）。そして、連邦監察官によるこの提案は、25条に規定されている異議（Beanstandungen）とは独立して行われる（24条５項３文）。

③異議[8]

連邦監察官は、この法律の規定またはデータ保護に関する他の法律の規定に関する違反（Verstöße）、またはその他データの処理もしくは利用に際して瑕疵を確認した場合に、次の者に対して異議を唱えることができる（25条１項）。

[8] 藤原・前掲注（１）87頁では“Beanstandungen”という単語が「異議」と訳出されている一方で、平松・前掲注（１）270頁では「警告」と訳出されている。「警告」という訳は原語と合致しないので、ここでは「異議」という訳に従う。

１　連邦行政については、これを所管する最上級連邦官庁（zuständigen obersten Bundesbehörde）

２　連邦鉄道資産（Bundeseisenbahnvermögen）については、代表者（Präsidenten）

３　ドイツ連邦郵便（Deutsche Bundespost）の特別財産から、法律によって設立された企業については、郵便法に基づく排他的な権利が帰属する限りで、その取締役会（Vorständen）

４　連邦直属の公法上の社団（Körperschaften）、施設および財団、ならびにこれら社団、施設および財団の連合（Vereinigungen）については、その理事会またはその他の代表権のある機関

連邦監察官にはこのように異議を申し立てる権限があるが、問題となっている瑕疵が些細な、または一時的なものである場合、連邦監察官は異議を見合わせ、または関係機関に対して、瑕疵についての態度表明（Stellungnahme）を要求するのをやめることができる（25条２項）。連邦監察官による異議が申し立てられた場合には、上記の機関は当該違反や瑕疵についての見解を表明しなければならないが、25条２項は例外規定となっている。また、連邦監察官は連邦政府と連邦機関に対して、データの改善に関する勧告（Empfehlung）や、データ保護の照会に対する助言（Beratung）を行うことができる（26条３項）。

④報告

連邦監察官は、ドイツ連邦議会に２年ごとに活動報告（Tätigkeitsbericht）をしなければならない。この活動報告は、ドイツ連邦議会と一般市民（Öffentlichkeit）に対して、データ保護の重要な展開について知らせるものである（26条１項）。連邦監督官は連邦の公的機関と民営化された一部の事業について監督するが、この報告書は個人情報保護を実践・改善し、個人情報保護意識を高める手段であるという理由から、報告書では民間部門における個人情報保護の状況についても記述しなければならないとされている[9]。

[9] Alexander Roßnagel, Handbuch Datenschutzrecht : die neuen Grundlagen für Wirtschaft und Verwaltung, C.H.Beck, 2003, S.515.

以上、連邦監察官の職務権限について概観してきた。連邦監察官は、個人情報保護の監督のために調査・立ち入り検査をしたり、異議を申し立てることができるものの、他の行政機関に対して刑罰を科したり、フランスの CNIL のように違反に対して金銭制裁を科したりする権限はない。2015年の法改正後も、そのような権限は与えられていない。その理由は、連邦監察官はいずれの組織のもとにも属さず、他の行政組織との間に上下関係が存在しないことにある。ドイツでは、行政組織内部で刑罰を科すには、自らの組織が上級行政庁である必要があると考えられている[10]ので、独立の存在である連邦監察官は刑罰を発動する主体たり得ないのである。

第４項　監督官庁

ドイツでは、民間機関と一部の公法上の競争企業によるデータ処理は、連邦監督官ではなく各州の監督官庁（38条１項）または州のデータ保護監察官による監督の対象となる（38条１項）。

監督官庁は、この法律またはデータ保護に関する他の法律の規定に対する違反を確認した場合には、違反について本人に知らせ、訴追又は処罰する権限を有する機関に違反を告発する権限がある。そして、重大な違反の場合には、違反のあったことを営業監督官庁（Gewerbeaufsichtsbehörde）に、営業法上の措置（gewerberechtlicher Maßnahmen）の実施のために知らせる権限を有する。連邦監察官が報告を義務付けられているのと同様に、監督官庁は、定期的に、遅くとも２年ごとに活動報告書を公表しなければならない（38条１項５文）。

連邦の公的機関に関する21条１文が準用され、非公的機関による自己の個人データの収集、取扱い又は利用に際して、自己の権利を侵害されたと考える者は誰でも、監督官庁に助力を求めることができる。

続いて、38条４項によると、監督官庁によって監督を委託された者は、監督官庁に託された任務の実行に必要な限りで、営業および業務時間内

---

[10] 藤原靜雄「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」（2011年３月）におけるドイツの章・67頁。
URL: http://www.caa.go.jp/seikatsu/kojin/h22report2.pdf.

に、対象となっている機関の敷地および事業所に立ち入り、そこで審査(Prüfungen)および視察(Besichtigungen)を行う権限を有する。そして、被委託者は業務上の書類、特に４ｇ条２項１文による一覧表（データ処理を行う機関の名称、データ処理の目的、データ処理権限のある者等が記載されている)、ならびに蓄積されている個人データおよびデータ処理プログラムを閲覧することができる。連邦公的機関に対する連邦監察官の調査権限や立ち入り権が認められているのと同様に、民間機関も立ち入りや書類閲覧などの審査・調査の対象となっている。

そして、監督官庁はデータ保護を保障するために、個人データの収集、処理および利用について確認された違反、または技術的若しくは組織的な瑕疵（Mängel）を除去（Beseitigung）するための措置を命じることができる（38条５項１文)。2009年の法改正前までは、監督官庁のこのような命令権には「データ保護法等の規定が、個人データの自動処理または自動化されていないデータファイル内もしくはデータファイルからの個人データの処理を規律している限り」、「９条に基づく要求の範囲内で」という条件が付されていたが、法改正によって削除された。

第５項で後述するように、この命令に従わなかった者には過料(Bußgeld)が科せられる(43条１項11号)。重大な違反および瑕疵の場合、特に人格権への特別な危険と結びついている場合、38条５項１文に基づく命令（Anordnung）に反し、かつ強制金（Zwangsgeldes）を科されたにもかかわらず、当該違反もしくは瑕疵が相当な期間内に除去されなかった時は、個人データの収集、処理、利用または個々の処理方式の使用を禁止（untersagen）することができる（38条５項２文)。連邦監察官が是正命令や過料、または刑罰を発動する権限を有さない一方で、監督官庁には強い法的権限が認められている。

第５項　過料と刑事罰

データ保護法43条には過料規定が、44条には罰則規定が置かれている。まず、過料規定の中で特に重要なものを概観する。

（１）過料規定

過料規定はデータ保護法43条１項と２項にあり、１項は、情報の取り

扱いに必要な届け出を行わない、本人に必要な告知をしないといった、比較的単純な手続違反が秩序違反となることについて規定する。そして、38条５項１文による監督官庁の命令に違反する行為が43条１項11号によって秩序違反（Ordnungswidrigkeit）となる。

２項は、手続違反を超えた、情報の不正取得等について規定しており、故意（vorsätzlich）または過失（fahrlässig）によって以下の行為をする者は秩序違反に問われる。

１　権限なく（unbefugt）、一般的にはアクセスできない個人データを収集または処理する行為

２　権限なく、一般的にはアクセスできない個人データを、自動処理方法を用いていつでも呼び出せるようにする行為

３　権限なく、一般的にはアクセスできない個人データを呼び出し、または、自動処理による、または自動化されていないデータファイルから自ら入手しまたは他者に入手させる行為

４　一般的にはアクセスできない個人データの提供（Übermittlung）を、虚偽の申告（unrichtige Angaben）によって受ける行為

データ保護法10条５項は、「一般的にアクセス可能」という文言を、「事前の届出、許可または対価の支払いの有無にかかわらず、何人も利用できる（nutzen kann）データ」と定義しているので、43条２項１～４号における「一般的にアクセスできないデータ」は利用が制限されているデータのことである。

５　16条４項１文、28条５項１文に反し、および29条４項、39条１項１文または40条１項との関連で、提供機関から提供されたデータを他の目的のために利用する行為

16条４項１文と28条５項１文によると、データの提供を受ける第三者は提供された目的の実現のためにのみ、データを処理または利用することが認められる。39条１項１文は、「職業もしくは特別の職業上の秘密に服する個人データ、およびその職業上または職務上の義務を果たす際に、守秘義務のある機関の自由な使用に供された個人データについて、責任機関は当該個人データを得た目的のためにのみ処理または利用をすることが許される」と規定し、40条１項は、「学術研究目的で収集または蓄積された個人データは、学術研究目的のためにのみ処理または利用

することを認められる」と規定する。このように、データ保護法にはデータが当該目的のためにのみ処理・利用されるべきことが定められており、目的外の利用が秩序違反行為となる。

５ｂ　28条４項１文に反して、宣伝（Werbung）または市場調査・世論調査（Markt- oder Meinungsforschung）の目的のためにデータを処理または利用する行為

28条４項１文は、「本人が責任機関に対して、宣伝または市場調査・世論調査の目的のための自己のデータの処理または利用について異議を申し立てている場合、この目的のための処理または利用は認められない」と定めており、故意または過失による違反が秩序違反となる。

７　42ａ条１文に反して、告知（Mitteilung）をしないこと、不正確な、不完全な、または遅延した通知を行うこと

42ａ条１文は、「２条４項に規定される民間機関、または27条１項１文２号に規定される公的機関は、貯蔵された

１　特別な種類の個人データ（３条９項）

２　職業上の秘密に関する個人データ

３　犯罪行為または秩序違反行為、または犯罪行為や秩序違反行為の嫌疑に関する個人データ

４　銀行またはクレジットカードに関する個人データについて、違法に伝達されているか、またはその他の方法によって第三者の知るところとなっていて、かつ本人の権利または保護すべき利益に対して重大な障害があり、本条２文から５文までの規定に従って、所轄の監督官庁ならびに本人に即座に告知されなければならないことを確認する」と規定している。42ａ条１文１号から４号の個人データの漏洩による不利益が発生している場合に、データを扱う民間機関と公法上の競争企業としての公的機関には適正な告知を行う義務があり、故意または過失によって当該義務に違反した場合には過料の対象となり得る。

以下は、過料の金額についての規定である。43条３項によると、１項に規定される秩序違反には50000ユーロ以下の過料を、２項に規定される秩序違反には300000ユーロ以下の過料が科される。43条１項の秩序違

反よりも43条２項のそれの方が重大であることが、上記の法定刑に反映されている。過料は、秩序違反による行為（der Täter aus der Ordnungswidrigkeit）がもたらした経済的な利益（wirtschaftlichen Vorteil）を上回らなければならない（43条３項２文）。この場合、43条３項１文に規定された金額では不十分であれば、これを超えることができる（43条３項３文）。

（２）刑罰規定

データ保護法における刑罰規定は以下の通りである。

前述の43条２項の秩序違反行為を、対価を得て、または自己もしくは他人の利益を図るために、または他人を害することを意図して行った場合には、２年以下の自由刑（Freiheitsstrafe）または罰金刑に処す（44条１項）。

犯罪行為は告訴（Antrag）によってのみ訴追される。告訴権者は本人、責任機関（verantwortliche Stelle）、連邦監察官または監督官庁である（44条２項）。

以上、データ保護法における過料・刑罰規定の概要について整理した。ドイツ連邦データ保護法では、連邦の公的機関のデータの取扱いを取り締まる連邦監察官には過料や刑罰を科す権限はないが、民間機関のそれを取り締まる監督官庁には、データの不正取得や目的外使用などの不正な取り扱いに対して過料を科すことができる。一般的な個人データとは区別されたセンシティブな個人データ（特別な種類の個人データ）という概念を設けている点では、イギリス1998年データ保護法とフランス1978年法およびフランス刑法と共通している。その一方でドイツ連邦データ保護法では、特別な種類の個人データの漏洩が不利益をもたらしている場合に適切な告知をしないという手続違反が43条２項７号によって構成要件化されているにとどまっており、フランス刑法とは異なり、特別な種類の個人データの入力や保存といった、手続違反を超えた不正な取り扱いは個別に構成要件化されていない。ドイツ連邦データ保護法に「特別な種類の個人データ」という概念が導入されたのは、EU データ指令を受けた2001年改正法からであり、2001年改正の契機となった

EU データ指令にも、センシティブなデータに対する不正取得等を特別の構成要件で処罰する規定は存在しない。このことから、ドイツ連邦データ保護法は EU 指令に沿って、特別な種類の個人データについては別個の処理条件を設ければ足り、過料・刑罰の特別な構成要件化までは必要ないと解したのではないだろうか。43条２項７号に該当する行為以外は、特別な種類の個人データであるか否かにかかわらず、同一の過料・刑罰規定が予定されているといえる。

第２節　データ保護法における過料と刑罰について

第１項　過料

第１款　客観的な成立要件

第１節第５項ではデータ保護法における過料・刑罰規定の概要について触れたので、本節ではその成立要件の詳細について扱う。

データ保護法43条１項と２項は、秩序違反行為につき過料を科すことを定めている。１項は単純な法定手続違反に関する規定である一方、２項は手続違反を超えた、個人データの不正な取り扱いについて規定している。

43条２項１号は、無権限者による個人データの収集と処理を対象としている。データの利用は対象外であるが、データの抹消はデータ保護法３条４項所定の「処理」の中に規定されているので、抹消によって本人の利益が侵害されることから、抹消の代わりに封鎖が行われるべきである場合（35条３項２号）に抹消する行為は過料の対象となり得る[11]。

43条２項２号は、無権限者が個人データをいつでも呼び出せるようにする行為を対象とする。実際にデータを呼び出すことは犯罪成立要件ではない。データの呼び出しは常に大量に行われるわけではないので、場合によっては呼び出しが行われたか否かが判然としないこともあり、データ呼び出しの準備行為には、貯蔵されたデータを危険にさらす蓋然性があるので、抽象的危険犯（abstraktes Gefahrdungsdelikt）として位

[11] Peter Gola / Christoph Klug/ Barbara Körffer, BDSG : Bundesdatenschutzgesetz : Kommentar, 12Aufl., 2015, § 43 Rn.20.

置づけられる[12]。

43条２項３号前段では、無権限者が個人データを実際に呼び出す行為が対象となる。この号で保護される個人データは、呼び出すことが可能であり、自動化処理されたものに限定され、43条２項２号とは異なり、データの呼び出しのために準備されているか否かは問題とならならず、呼び出しが技術的に可能なデータであることが要求される[13]。

43条２項３号後段は、無権限者が自動処理により、または自動化されていないデータファイルから自らデータを入手し、または他者にデータを入手させる行為が規定されている。自己の利益のためではなく、他者のために行われた場合も本号の構成要件が満たされる[14]。

43条２項４号は、一般的にはアクセスできない個人データの提供を、虚偽の申告によって受ける行為について規定する。本号はハッカーによる情報の入手などにも適用され得る。ハッキングは形式的には「虚偽の申告」ではなく、有効なパスワードによってデータを入手する行為であるが、パスワードの利用によってデータを騙し取る行為として本号の規制対象となる[15]。前述の通り、43条２項１～４号では、一般的にアクセスできない個人データが対象となる。

43条２項５号は、個人データの提供を受けた者が、提供された目的以外の処理と利用を行うことを対象としている。16条４項に規定されているように、データ提供機関（übermittelnde Stelle）はデータを提供する際に、目的について指示しなければならない。提供目的外のデータ処理・利用が禁止されると同時に、データ処理等の目的は明確に説明される必要があり、再三にわたってデータが伝達されるような場合には目的が明白に区別されなければならない[16]。2009年の法改正以前の43条２項５号では、「第三者に譲渡することを通じて、提供されたデータを他の目的のために利用する」行為が秩序違反になっていたが、法改正によって「第

[12] Peter Gola et al, a.a.O, §43 Rn.21.
[13] Peter Gola et al, a.a.O, §43 Rn.22.
[14] Peter Gola et al, a.a.O, §43 Rn.22.
[15] Peter Gola et al, a.a.O, §43 Rn.23.
[16] Peter Gola et al, a.a.O, §43 Rn.24.

三者に譲渡することを通じて」という文章が削除され、目的外のデータ利用がすべて秩序違反として構成されるようになった。

そして、43条２項５号では、①職業もしくは特別の職業上の秘密に服する個人データ、およびその職業上または職務上の義務を果たす際に、守秘義務のある機関の自由な使用に供された個人データについて、当該個人データを提供された者が、責任機関がデータを得た目的以外で個人データを利用する行為と、②学術研究目的で収集または蓄積された個人データの提供を受けて、学術研究目的以外で利用する行為も秩序違反行為となる。本号の対象となるのは、これらの秘密の保持を義務付けられている者自身ではなく、正当な方法でそのようなデータの提供を受けた者または機関である。したがって、データの提供が行われれば、医師などの特定の職務を行う者、または公職者に科せられた守秘義務とその違反行為は、本号の対象外となる[17]。

43条２項５ｂ号は、本人が責任機関に対して、宣伝または市場調査・世論調査の目的によるデータ処理・利用について異議を申し立てているにもかかわらず、これらの目的のためにデータ処理・利用する行為について規定しており、2009年の改正によって新設された条項である。宣伝を行う企業は調査の結果、宣伝目的でのデータの利用や処理を拒否していない者のみについて行われることを証明（sicherstellen）しなければならない[18]。これまでは本人の拒否があった場合について十分に対応することができなかったが､法改正によって処罰の間隙が一部埋められた。監督官庁が、宣伝を行う企業による本号の違反について訴追する場合、当該企業は入念な検査と、場合によっては企業の組織的な行為が法に適合することを要請されるものの、本号が新設されたことによって本人の拒否権と、望まない宣伝で「満杯になった郵便ポスト（überfüllten Briefkästen）」によって煩わされない権利が本当に強化されたのか否かは疑問視されている[19]。このような問題意識により、宣伝産業における

[17] Peter Gola et al, a.a.O, §43 Rn.24.

[18] Coriana Holländer, Datensündern auf der Spur－Bußgeldverfahren ungeliebtes Instrument der Datenschutzaufsichtsbehörden?, RDV 2009, S.219.

[19] Holländer, a.a.O, S. 219.

監督官庁の権限強化に向けた再検討が必要であると指摘されている[20]。

データ保護法43条２項各号の秩序違反行為は、権限のない者によって所定の行為がなされることによって成立するので、この法律やデータ保護についての他の法律に適合していることが正当化事由となる。

データ保護法違反者に制裁金支払い能力がないことが確実である場合、過料を科すことは無意味なので、行政執行法（Verwaltungs－Vollstreckungsgesetz, VwVG）16条に基づく代替強制拘留（Ersatzzwangshaft）が用いられ得る[21]。

また、ドイツの各州において、州のデータ保護法（Landesdatenschutzgesetz）が施行されている。多くの州のデータ保護法では過料と刑罰の両方が規定されているが、シュレースヴィヒ＝ホルシュタイン（Schleswig-Holstein）州データ保護法では過料規定のみが存在する。一方、ベルリン州とラインラント＝プファルツ（Rheinland-Pfalz）州データ保護法では刑罰規定のみが存在する。

第２款　主観的な成立要件

43条１項・２項は、故意と過失の両方を秩序違反の対象としている。ドイツ刑法学における過失は、「認識ある過失（bewusste Fahrlässigkeit）」と「認識なき過失（unbewusste Fahrlässigkeit）」に分けられる。ドイツ刑法における「未必の故意（bedingter Vorsatz）」は、発生し得る法益侵害に向けた決定であるのに対して、認識ある過失は、許されない危険創出（unerlaubter Gefahrschaffung）であるにもかかわらず、行為者が結果の不発生を信じる場合であり、この２つは明確に区別される[22]。一方、「認識なき過失」は、一定の作為または不作為において、必要な注意をせず、その結果として法的な構成要件的結果を認識せずに発生させるこ

---

[20] Holländer, a.a.O, S.219.

[21] Holländer, a.a.O, S.222.

[22] Claus Roxin, Strafrecht Allgemeiner Teil, Band Ⅰ Grundlagen・Der Aufbau der Verbrechenslehre 4.Aufl, C.H.Beck.2006, S.1087. 山中敬一（監訳）『ロクシン刑法総論第１巻［基礎・犯罪論の構造］【第４版】［翻訳第２分冊］』（信山社・2009年）625頁以降参照。

とをいう[23]。

認識ある過失と認識なき過失は理論上区別されているものの、ある行為が認識ある過失による行為であると同時に、認識なき過失による行為でもあり得ることが指摘されている[24]。論者によると、ある者が結果発生の蓋然性を10％であると見積もって、結果の不発生を信じたものの、実際には結果発生の蓋然性は25％であったという場合に、行為者はすでに認識ある過失で行為している。同時に、より高度の危険性が認識可能だったということで認識なき過失も存在する[25]。論者は、認識の有無によって法的効果が左右されないということにより、認識ある過失と認識なき過失を区別する意義が乏しい旨を指摘する[26]が、実際の事例においても両者を截然と区別することは容易ではないだろう。

前述の通り、データ保護法43条１・２項における「過失」には、認識ある過失と認識なき過失の両方が含まれる。したがって、自己に権限のないことを認識せず、一般的には自由に利用できない個人データを収集する行為などの、単純な不注意による行為も広く過料の対象となり得る。

第２項　刑罰

データ保護法44条は、前項で扱った43条２項所定の秩序違反行為を、対価を得て、または自己もしくは他人の利益を図るために、または他人を害することを意図して行った場合には、自由刑または罰金刑が科せられることを規定する。

44条は刑罰規定であり、一般的にはアクセスできない個人データが保護法益となる。この規定の客観的構成要件は、対価を得ること、または自己利益を図ること、もしくは他害を図ることである。ここでいう「対価」とは、ドイツ刑法典（StGB）11条１項９号が規定する「財産的利益に存

---

[23] Johannes Wessels / Werner Beulke, Strafrecht Allgemeiner Teil, 42., überarb. Aufl, C.F. Müller, 2012, S.262.

[24] Roxin, a.a.O, S.1089.

[25] Roxin, a.a.O, S.1089.

[26] Roxin, a.a.O, S.1087, Wessels et al, a,a,O, S.262も、認識ある過失と認識なき過失の区別は、量刑判断のみに必要となることを述べている。

するすべての反対給付（jede in eimem Vermögensvorteil bestehende Gegenleistung）」のことである[27]。「反対給付」の概念は、何らかの相応する取り決め（entsprechende Vereinbarung）の存在を前提としており、その取り決めによって自己の利益を図ったり、現実に利益を得たりすることは要求されない[28]。データ保護法の下では故意による行為のみが刑罰の対象となることは、条文の文言より明らかである。

ドイツの各州にも州データ保護法が存在するのは前述の通りである。刑罰法規の有無や内容は州ごとに異なっており、バーデン - ヴュルテンブルク州、ブランデンブルク州、ブレーメン州等のデータ保護法では未遂（Versuch）も刑罰の対象となる。

現行法の前身である1990年連邦データ保護法43条にも罰則規定があり、そこではデータ保護法によって保護され、周知のもの（offenkundig）となっていない個人データを無権限で蓄積、提供する行為等が処罰の対象となっていた。そして、現行法では「周知のものとなっていない」という文言から、「一般的にはアクセスできない」という文言に変更され、1990年法では刑罰の対象となっていたデータの無権限の呼び出しや入手などの行為が、現行法では過料の対象へと変更されている。旧法に比して、現行法では刑罰の対象となる行為が制限される。そして、現行法への法改正に伴い、データの内容が広く知られているか否かにかかわらず、アクセスにつき制限のない個人データはデータ保護法による保護の対象外とされるようになった。

1990年データ保護法において規定されていた、データが「周知のものである」という文言には、「一定数の人々に知られているか、または他の情報なしに（ohne weiteres）知覚可能であり、人々の間で確定的に保持されていること」という定義があるものの、インターネットや電子工学的なデータ転送によるデータの提供には地域的・時間的・量的な限界がないので、今日ではすべてのデータは「周知のもの」となり得る[29]。ま

---

[27] Peter Gola et al, a.a.O, §44 Rn.5.

[28] Peter Gola et al, a.a.O, §44 Rn.5.

[29] Thilo Weichert, Datenschutzstrafrecht-ein zahnloser Tiger?, NStZ 1990, S.491.

た、データが「周知のもの」であるか否かは、データ処理の目的、性質、地域的・人的・時間的状況によって左右され得るという指摘もされている[30]。

このように、データの「周知性」という概念は曖昧で、インターネット等によって情報の伝達が容易に行われる現代ではその実効性を失っているので、2001年データ保護法への改正において、保護客体が「一般的にはアクセスできない」データに変更されたことには意義がある。しかし、本来であれば一般人の自由なアクセスに供するべきではない性質の個人データであるにもかかわらず、データの責任機関等の安全措置に問題があって、不当にも自由なアクセスができる状況になってしまっているような場合には、現行法の43条２項の条文で十分に対応できるかどうかは疑問である。安全措置の甘さが「一般的にはアクセスできない」という構成要件該当性を阻却してしまう不当な結果になることは回避すべきであろう。

第３節　監督機関による規制の実態

第１項　州における監督体制

ドイツでは連邦の公的機関については連邦データ保護観察官が、州の民間部門については監督官庁（38条１項）または州のデータ保護観察官等が監督する。

州によって監督体制は様々であり、（１）州内務省の下にある監督官庁が所管している州（バーデン＝ビュルテンブルク州、ブランデンブルク州）、（２）州の行政区域が所管している州、（バイエルン州、ヘッセン州）（３）州の公的部門と民間部門の両方を州のデータ保護観察官が所管する州（ベルリン州、ブレーメン州、ハンブルク州、メクレンブルク＝フォアポンメルン州、ニーダ―ザクセン州、ノルトライン＝ヴェストファーレン州、ラインラント＝プファルツ州、ザクセン州）、（４）州の行政庁が所管する州（ザクセン＝アンハルト州、チューリンゲン州）、（５）データ保護のための独立した委員会を設けている州（シュレース

[30] Weichert, a.a.O, S.491.

ヴィヒ＝ホルシュタイン州、ザールラント州）に分けられる。

このように、ドイツでは民間部門の情報取り扱いを規制する機関が多岐にわたっているが、この中で独立した第三者的な立場にあるのは州のデータ保護観察官と、シュレースヴィヒ＝ホルシュタイン州の独立センター（Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. 以下、ULD とする）である。

また、ザールラント州では、従来は州のデータ保護観察官が公的機関の情報処理を所管し、民間部門をザールラント州内務・ヨーロッパ事項省（Saarland Ministerium für Inneres und Europaangelegenheit）が所管していたのであるが、2011年５月18日にザールラント州データ保護法（Saarländischen Datenschutzgesetzes）が改正されたことにより、2011年６月からはザールラント州独立情報保護センター（Unabhängiges Datenschutzzentrum Saarland. 以下、UDS とする）が公的機関と民間部門の両方を所管することとなった。それに伴い、UDS はデータ保護法所定の秩序違反行為に対して過料を科す権限を付与された。

そこで本節では、ドイツ16州の中で情報保護のための独立委員会を有しているシュレースヴィヒ＝ホルシュタイン州とザールラント州を取り上げることで、第三者機関による取り締まりの実態を明らかにする。

第２項　独立委員会による過料

第１款　シュレースヴィヒ＝ホルシュタイン州

個人情報保護のためのシュレースヴィヒ＝ホルシュタイン州独立センター（ULD）の業務は、州におけるデータ保護法違反に対する異議に基づく瑕疵の除去要求と、データ保護の問題について企業や州の市民に助言をすること、毎年の活動報告（Tätigkeitsberichte）を行うこと等である。州における民間機関と公的機関の両方を監督する。

シュレースヴィヒ＝ホルシュタイン州のデータ保護法では、44条に以下のような過料規定がある。刑罰規定は設けられていない。

44条１項　秩序違反は、この法律に違反して、周知のものとなっていない個人データを

１　収集、貯蔵、目的外の処理、変更、伝達、呼び出すための準備、

消去した場合と、
２　呼び出し、閲覧、入手、または誤った事実による欺罔行為（Vortäuschung）を通して、自己または他人に伝達させる行為について成立する。

44条２項　秩序違反は、以下の場合にも成立する。
１　匿名化された、または偽名化されたデータを他の情報と共に照合し、それによって一人または複数の本人を特定する場合
２　この法律に違反して、偽名化されたデータについて、与えられた権限を超えてアクセスを入手した場合、または
３　この法律の５条１項による技術的・組織的な措置を採ることを完全に（vollständig）怠った場合
３項　秩序違反には50000ユーロ以下の過料が科され得る。

そして、技術的・組織的な措置について規定した５条１項の内容は以下の通りである。

この法律の規定、またはデータ保護に関する他の規定（３条３項所定）[31]の実行（Ausführung）は、技術とデータ保護の必要性の観点から、必要で妥当な技術的・組織的措置を通して行われなければならない。
以下のことを保証しなければならない。
１．手続（Verfahren）とデータが時宜に適って自由使用に任され得る状態であり、合法的に使用され得ること（自由裁量）
２．データが破損しておらず、完全であり、分類可能であり（zurechenbar）、最新のものであること（完全性）
３．認められた方法のみによってデータが呼び出され得ること（機密性）
４．期待可能な出費（Aufwand）による個人データの処理が、後付け

[31] シューレスヴィヒ＝ホルシュタイン州データ保護３条３項は「個人データの取り扱いに関する特別の規定のある場合、それらはこの法律の規定に優越する」と定めている。

られ（nachvollziehen）、調査され、評価され得ること（透明性）

５．個人データが、決められた目的以外の目的のために収集され、処理され、利用され得ないこと、または、決められた目的に従うには過度に高額の出費を伴う（mit unverhältnismäßig hohem Aufwand）場合に限って収集、処理、利用を可能とすること（不可連鎖性　Nicht-Verkettebarkeit）、そして

６．26条から30条までの条文で認められた本人の権利行使を有効なものにするような（情報処理の）方法であること（異議の可能性）

26条から30条には、自己のデータを処理される目的などの告知を受ける権利、データ処理への拒否権等が規定されている。

このように、シュレースヴィヒ＝ホルシュタイン州のデータ保護法では、技術的・組織的措置を採ることを怠る行為を秩序違反の対象としている。このような秩序違反規定は、シュレースヴィヒ＝ホルシュタイン州と同様に独立のデータ保護委員会を有するザールラント州データ保護法にも、連邦データ保護法にも存在しない特徴的なものである。連邦データ保護法９条では必要な技術的・組織的措置を採ることを義務付けた上で、38条５項において、技術的・組織的な瑕疵の除去のための措置を命ずる権限を監督官庁に認めている。この命令に違反した場合に初めて過料の対象となり得るという構成を採っている一方で、シュレースヴィヒ＝ホルシュタイン州データ保護法が「命令違反」を経由せず、必要な技術的・組織的措置を講じないという段階で秩序違反を構成するという点は注目に値する。個人データの目的外使用や不適切な処理などの様々な違反行為が「措置の懈怠」として扱われ、直ちに過料の対象となり得るからである。

以上の条文を前提として、本款では、ULD が発表する活動報告書から、過料に関する実務について探ることとする。

ULD は２年に１回活動報告書を発表している。2013年３月の報告書[32]では、ULD がデータ保護法の秩序違反行為の他に、通信メディア法

[32] 34. Tätigkeitsbericht des ULD, S. 24. URL: https://www.datenschutzzentrum.de/tb/tb34/uld-34-taetigkeitsbericht-2013.pdf.

（Telemediengesetz）の秩序違反行為に対して最大50000ユーロの過料を科すことができるようになったことが紹介されている。これは、州の秩序違反行為管轄命令（Ordnungswidrigkeiten-Zuständigkeitsverordnung）3.5.2が改正されたことによる。

2011年３月に出された報告書では、過料の事例が次のように紹介されている。ULD の過料に対する姿勢を理解する必要上、若干長くなるが引用する。

「銀行の以前の顧客が、宣伝目的によるデータの利用について異議を唱えたにもかかわらず、当該銀行からの再三にわたる宣伝を受け取った。我々（ULD）は、過料を科さなければならなかった（Wir mussten ein Bußgeld verhängen.）。

連邦データ保護法によると、何人も責任機関に対して、宣伝または市場調査・世論調査目的による自己のデータの利用または転送について異議を唱える権利を有する。前述のケースのような、宣伝目的によるデータの利用に対しても異議を唱えることが認められる。問題となった銀行の対応（Reaktion）は、我々に対して懸念を抱かせた。それというのも、銀行は企業の組織の内部における重大な瑕疵について認識していながら放置していたからである。当該データについての異議が完全に遵守されるか、または遵守され得るという技術的・組織的な保障もなされていなかった。このことは、本人の異議が無視されるという結果につながった。過料決定は法律上の効力のある（rechtskräftig）ものである」[33]。

この事例報告からは、当該銀行には瑕疵の認識があり、違反について故意は認められなくとも、違反結果についての認識ある過失はあったであろうということがわかる。銀行による宣伝が一度ではなく再三にわたって送られたという事情も、違反の悪質性を基礎づけるだろう。このことから、ULD は結果の重大性や瑕疵の治癒の見込みなどを考慮して、悪質なケースに限定して過料決定を下しているのではないだろうか。なお、前述の通り、シュレースヴィヒ＝ホルシュタイン州のデータ保護法では刑罰規定が設けられていない。

[33] 33. Tätigkeitsbericht des ULD, S.94. URL:https://www.datenschutzzentrum.de/tb/tb33/uld-33-taetigkeitsbericht-2011.pdf.

次に、2007年３月に出された報告書では、１件の過料の事例が挙げられている。保険会社の従業員が、雇用主のレターヘッド（Briefkopf）を用いて、自動車の許認可の所轄官庁（Kfz-Zulassungsstelle）に申し立てた上で、車両所有者に試問を行った。実際には当該車両による被害について何らの届出もなされていなかったにもかかわらず、当該従業員は試問で得られる情報を全くの私的な目的で使用するために、正当な権限なく試問を行ったのである。当該従業員によるこの行為は、車両所有者についての一般的にはアクセスできない情報を故意に不正取得するという秩序違反に該当し、ULD は従業員に過料を科した[34]。報告書の記載の通り、従業員の行為は故意による不正な情報収集であり、過料決定が下されるにあたり、故意行為であることと、私的な目的のために虚偽の試問によって情報を収集したという行為の悪質性が考慮されたのではないかと思われる。

続いて、2006年３月の報告書では、「過料―それは時には不可避である」というサブタイトルが付された記述がある。本報告は、ULD による過料実務を次のように要約する。「通常、企業は ULD がデータ保護の改善のために行う要求・指示・助言には大いに譲歩し、理解を示している。しかし、違反が再三行われた場合、特に故意による重大な法律違反の場合は、個々の過料手続が必要となる」[35]。

続いて、本報告書は過料の事例について以下のように詳述する[36]。

「データ保護監督官庁の事情調査のためには、法律で明確に定められた情報提供（Auskunftserteilung）義務は無視できるものではない…（中略）…企業が我々（ULD）の調査における照会（Aufragen）に応じることなく、それが再三にわたる場合、ULD は過料を下さなければならない。…（中略）…複数の市民から同様の申請（eingaben）がなされることは、過料手続が導入される根拠となる。市民たちは、ある利益団体

[34] 29. Tätigkeitsbericht des ULD, S.90. URL: https://www.datenschutzzentrum.de/tb/tb29/tb29.pdf.

[35] 28. Tätigkeitsbericht des ULD, S.83. URL: https://www.datenschutzzentrum.de/tb/tb28/tb28.pdf.

[36] 28. Tätigkeitsbericht des ULD, a,a,O, S.83.

(Gewinnspiel) に加入するための通知を受け取った。実際には、通知を受け取った彼らのうちの誰もその団体に参加せず、企業からも告知がなかった。にもかかわらず、彼らの生年月日、口座番号、電話番号が一部、企業に提供されていた。データ管理者は、支払い不能の (insolvent) 企業から50万人のデータが、本人の承諾なしに、既に何年も前に提供されていたことを認めた。その間に、この企業はすべての商業活動を中止したことを通知した。したがって、一般的にアクセスできない個人データの故意による処理についての疑いは晴れていない (nicht vom Tisch)」。

このような報告書の記載からは、複数の者の個人データが違法に、そして故意によって処理された以上のケースについて、実際に過料決定が下されたのか否かということは定かではない。しかし、被害が広範であれば過料決定が選択される余地があるということを表しているだろう。

また、再三の異議 (Beanstandung) があったにもかかわらず、極めて頑なな家主が公道で権限なくビデオ監視を行った事例につき、ULD が過料決定を下したところ、この過料決定についての異議が区裁判所に申し立てられたことも報告されている[37]。

以上、シュレースヴィヒ＝ホルシュタイン州のデータ保護委員会によって報告された事例を通して、過料の実務の実態について検討してきた。これらの事例からは、データ保護法の違反があり、それが州のデータ保護法の過料規定に合致するとしても、直ちに過料決定が下されることはなく、実際には特に悪質なケースに限って過料が下されるということがわかる。そして、2006年の報告書にも記載されているように、州のデータ保護法の監督下にある企業等の機関は、ULD の監督や規制に対して協力的である場合が一般的であり、このことも過料の事例が少ない原因の一つとなっている。このことから、第三者機関である ULD の監督は、データ保護法の違反に対する抑止力としての機能を一定程度は果たしていると考えられる。

第２款　ザールラント州

個人情報保護のためのザールラント州独立センター (UDS) は、ザー

[37] 28. Tätigkeitsbericht des ULD, a,a,O, S.83.

ルラント州の公的機関と民間機関の両方を監督する。

シュレースヴィヒ＝ホルシュタイン州とは異なり、ザールラント州データ保護法（Saarländisches Datenschutzgesetz）には過料規定と刑罰規定の両方が存在する。まず、過料規定は以下の通りである。

36条１項　秩序違反は、この法律によって保護される周知のものとなっていない個人データに対する以下の行為に対して成立する。

１．収集、蓄積、改変、伝送、閲覧または呼び出しのための準備、消去または利用

２．呼び出し、閲覧、入手、または誤った事実による欺罔行為（Vortäuschungfalscher Tatsachen）によって、自己または他人に転送させる行為

36条２項　秩序違反には、50000ユーロ以下の過料が科され得る。

続いて、刑罰規定は以下の通りである。

35条１項　この法律によって保護されている一般的にアクセスできない個人データについて、対価を得て、または自己もしくは他人の利益を図るために、または他人を害することを意図して、

１．収集、蓄積、改変、転送、閲覧または呼び出しのための準備、消去または利用

２．呼び出し、閲覧、入手、または誤った事実による欺罔行為（Vortäuschung falscher Tatsachen）によって、自己または他人に転送させる行為に出た者には、２年以下の自由刑または罰金刑が科される。

これらの行為の未遂（Versuch）も可罰的である。

35条２項　当該行為が他の刑罰規定に触れない限りにおいて、１項の規定が適用される。

このように、ザールラント州データ保護法では、シュレースヴィヒ＝ホルシュタイン州とは異なり、技術的・組織的措置の懈怠は過料・刑罰の対象とはなっておらず、個人データの収集や利用等の行為が客観的要件となっている。以上の条文を前提として、本款では、UDS が発表する活動報告書から、過料に関する実務について検討する。なお、ザール

ラント州では２年間で１つの報告書が提出されており、2009年・2010年までは公的機関については州データ保護監察官が、民間部門については監督官庁が各自で報告書を作成している。そして、2011年からUDSが公的機関と民間部門の両方を所管することになったので2011年・2012年からは報告書が一本化されている。

USDが設立され、データ保護法違反に対して過料決定を下せるようになったのは2011年６月以降であるが、どのような事例に過料が科され得るのか（あるいは科され得ないのか）を検討するために、2011年以前の報告書についても取り上げることとする。

まず、非公的機関についての2003年・2004年の報告書には、次のような過料の事例がある[38]。

ある銀行の従業員は、どの範囲で個人データを貸主（Vermieter）に提供してもよいのかという本人の意思決定（Entscheidung）を待つことなく、借主である複数の当事者のデータをSchufaに照会したところ、Schufaは私人に対していかなる情報も提供しないので、たとえ銀行員であっても個人データの提供を受けることはできなかった。

Schufaの正式名称は、“Schutzgemeinschaft fuer allgemeine Kreditsicherung（貸主保護団体）”であり、ドイツ在住者と企業の経済力や信用について査定を行い、この査定結果であるSchufa-Auskunftを家主や銀行などの貸し主に販売する事で利益を得る団体である。

そこで銀行員は、借主である当事者自身を促して、Schufaへの照会をさせることによって当事者の個人データを得た。銀行員は、当事者本人がこの手続に同意しており、Schufaへの照会が合法であると主張していた。しかし、当事者本人にSchufa-Auskunftについて告知せずに照会を行わせたということから、本人の同意は法律上有効なものではないとされた。

本人の有効な同意を得ずにSchufaにデータ照会をさせてそのデータを得るという銀行員の行為は、連邦データ保護法43条２項４号における

[38] Tätigkeitsberichte der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Datenschutz des Saarlandes 2. Tätigkeitsbericht 2003/04 URL: http://www.lfdi.saarland.de/images/stories/pdf/Berichte/tbnoe_2.pdf, S.47~48.

不正な申告による個人データの受け取りという客観的要件を満たしているとして、当該銀行の従業員には過料決定が下された[39]。

この事件では、被害者は複数である。さらに、銀行員の行為は“Täuschungshandlung（詐欺的行為）”であると表現されていることから、銀行員が故意により、そして当事者本人を欺罔するような形でデータを収集したということに過料決定の根拠があると考えられる。

2015年４月に発表された2013年・2014年のUDSの報告書では、次の過料の事例が紹介されている[40]。

（１）ビデオ監視について

2013年４月、ピザチェーン店において従業員に対するビデオ監視が行われていているとの匿名の請願がUDSになされた。連邦データ保護法38条１項に基づき、この店の監督が行われたところ、従業員が360個のネットワークカメラによって監視されていたことが判明した。店長は、当該カメラはネットワークから離されており、それゆえカメラに捉えられる可能性はないことを主張していたが、調査の結果、このカメラが引き続き使用可能な状態であり、実際に利用されていることが判明した。この事例では、店長は事実に反する申し立てを自覚的に行っていたことから、UDSによる過料決定が下された。

（２）自治体に対する市民の苦情について

一人の市民が自治体のプールの水質についてＥメールで苦情を申し立てた。返事のメールには市長の署名がなされていて、実行された水質調査に対する市民の苦情は退けられた。そして、追伸には「二度と私たち（自治体）を煩わせないでください」と記載されてあった。この返事について、市民はザールラント放送局に相談を持ち掛け、ラジオで報道が行われた。ラジオ放送の内容は、地方自治体のプールの水質に関することと、市長が市民に対して向けた追伸の言葉遣いに関することであり、

[39] 2. Tätigkeitsbericht 2003/04, a,a,O, S.48.

[40] 25 Tätigkeitsberichte, Unabhängiges Datenschutzzentrum Saarland 2013/2014, S 101～104. ULR: https://datenschutz.saarland.de/fileadmin/tberichte/25_Taetigkeitsbericht_2013-2014.pdf.

市民も言葉を発したが、匿名のままであった。

報道を受けた市長は、自治体の広報の雑誌の中で態度表明をするとともに、苦情を述べる市民のＥメールの全文と実名を公開し、市民に対する非難の姿勢を明らかにした。UDS は市長の行動について、周知のものとなっていない個人データを無権限に伝送するものであり、ザールラント州データ保護法36条１項に違反するとして、過料決定を下している。

事例（１）では行為者が意図的に虚偽の申し立てを UDS に対して行ったことが、事例（２）では行為者が周知のものとなっていない個人データを故意で公開したことが注目される。ULD のみならず、UDS も悪質な秩序違反行為に限って過料を科しているように思われる。

第３項　過料に対する監督機関の姿勢

第２項では、個人データ保護のための特別な委員会を有しているシュレースヴィヒ＝ホルシュタイン州とザールラント州の実務について検討した。これら２つの州では、データ保護法の違反に対して過料・刑罰が科される例は稀であったが、この傾向はドイツ全土にもいえることである。データ保護法の違反につき、2008年に初めて高額の過料が科された代表的なケースが２つある。その一つは、ビデオ監視を行った Tönnies という食肉加工企業に対してノルトライン＝ヴェストファーレン州のデータ保護監察官が80000ユーロの過料を科したというものである。問題となった企業は、社内の更衣用個室や食堂など、合計200以上のカメラを設置して従業員を監視していた。衛生上の必要から、食肉生産室にはカメラを設置することが認められていたものの、それ以外の場所に対するカメラ設置がデータ保護法違反として問題となったのである。Tönnies 社は州データ保護監察官による過料決定を受け入れ、食肉生産室以外のカメラを撤去した[41]。

もう一つは、食料品のディスカウントショップチェーンの Lidl が盗

[41] Focus-Online v.15.09.2008; http://www.focus.de/politik/deutschland/datenschutz-toennies-muss-wegen-videoueberwachung-bussgeld-zahlen-_aid_333478.html.

撮によって従業員を監視していたことにつき、バーデン＝ヴュルテンブルク州のデータ保護監督官庁が150万ユーロの過料を科したという事例である。Lidl が管理していた35の販売会社が調査の対象となり、ドイツの複数の州の監督官庁が携わったが、Lidl の本拠地がネッカーズルムであることから、バーデン＝ヴュルテンブルク州が所管することとなった。Lidl 社は219の支店にカメラを設置しており、複数の労働組合員が企業による広範囲な監視について明らかにした後、Lidl 社は監督官庁による過料決定を受諾している[42]。

この２つの事例では企業に高額の過料が科されているが、これまでの監督官庁の業務の中で、過料を科すことはあまり行われていなかった。2005年９月から2006年８月までの間、ドイツ共和国全体で下された過料決定は44件であり、2008年にベルリン州のデータ保護監察官が下した過料決定は３件である[43]。

データ保護法における秩序違反の訴追につき、監督官庁がこれまで制限的であったのはなぜかということが問題となる。違反の数は毎年増加傾向にあるので、データ保護法が完全に遵守されているから過料決定の数が少ないと解することはできず、監督官庁の人員が定員を満たしていないことが、過料手続が実行される件数の少ない理由の一つであるとする見解がある[44]。データ保護法の秩序違反を訴追するには、人的資源が求められるからである。過料を科すのは最後の手段（ultimaratio-Mittel）とされており、データ保護法38条５項による監督官庁の権限に基づいて、データ保護法違反が取り除かれた可能性が見いだせない場合、監督官庁は過料を科すことが可能である。しかし、監督官庁の人員が不足していること、不十分な管理権限、そして企業に対して過料を科すことに慎重な態度により、個人データが危険に晒され得ることが指摘されている[45]。

監督官庁による実務の実態に加えて、2009年のデータ保護法改正後も

---

[42] Welt-Online vom11.09.2008; http://www.welt.de/wirtschaft/article2428529/Spitzelaffaere-kostet-Lidl-1-5-Millionen-Euro.html.

[43] Holländer, a,a,O, S.215.

[44] Holländer, a,a,O, S.215.

[45] Holländer, a,a,O, S.215.

依然として処罰の間隙がある[46]。第１節で述べた通り、データ保護法９条は、個人データを収集･処理･利用する公的･民間機関に対して、データ保護のために必要な技術的かつ組織的な措置を講ずる義務を定めている。しかし、2009年の法改正後も、企業等の機関がこの義務に違反する行為は処罰の対象となっていない。過料の対象となる行為が法律で定められていることは、一般予防と特別予防の両方の効果を有する[47]。しかし、秩序違反法における起訴便宜主義（Opportunitätsprinzip）に依拠すれば、すべての違反に対して過料が科されることはなく、過料規定の予防効果の程度は、監督官庁が違反を訴追するのか否か、そしてどの程度訴追の対象とするのかということに依存するので、監督官庁は過料を科すことを回避するのではなく、過料を法益保護の手段とみなすべきであることが指摘されている[48]。

ドイツではデータ保護法違反に対して過料が科されるケースが少なく、刑罰規定は過料規定よりも対象となる行為が限定されているので、刑罰が科されるケースは更に希少なのが現状である。実際に過料や刑罰が下されることが少ない根拠として、人員が不十分であることを指摘する前述の見解があり、監督業務におけるそのような困難さは否定できないだろう。それに加えて、監督官庁が過料を科すことに慎重な態度を採っていることも確かである。過料が科されるのはデータ保護法違反による被害が広範囲であったり、再三の異議を無視したりといった悪質なケースが多く、刑罰はその対象とする範囲の狭さも手伝って、刑罰が科された事例はほとんど見られない。その一方で、前述の報告書にも記載されていたように、多くの企業は監督機関の指導・助言に対して受容的であり、監督業務に対しても協力的である。全体的な傾向として、監督官庁の指示等に従わない悪質なケースが過料の対象となっていることに鑑みれば、過料や刑罰の規定が存在することと、監督機関による業務の２つが協同することが、データ保護法違反についての一定程度の抑止力になっていると考えられる。

---

[46] Holländer, a,a,O, S.221.

[47] Holländer, a,a,O, S.222.

[48] Holländer, a,a,O, S.222.

第４節　小括

本章では、ドイツのデータ保護法におけるデータの不正な取り扱いに対する過料と刑罰の成立要件および、データ保護のための監督による実務の実態について検討してきた。

ドイツのデータ保護法制において、情報の不正な取り扱いに対する抑止力となり得るのは、監督機関による監督業務と、違反に対する過料・刑罰規定である。ドイツ連邦データ保護法と州のデータ保護法では、単純な手続違反と共に個人データの不正収集・提供などの行為に対して過料が予定されており、刑罰の適用される範囲は図利または加害目的等によってデータの不正収集等を行った場合に限定される。

いわゆる情報窃盗や第三者提供などの、日本においても頻発している行為態様は連邦データ保護法43条２項各号によって規定されており、イギリス1998年データ保護法55条と、フランス刑法における諸規定（刑法226－22条を除く）とは異なり、故意のみならず過失による行為も対象となっている。ドイツ刑法学では、過失は「認識ある過失と」「認識なき過失」の両方を含むので、単純な不注意による情報漏洩も過料の対象としてカヴァーされる。そのような過失による情報漏洩や第三者提供によっても甚大な被害の発生する場合があることから、過失行為も対象とすることには意義がある。

ドイツでは、民間機関による情報処理に対する規制が各州に任されており、各州のデータ保護法の中には、過料規定が存在せず刑罰規定のみが設けられている州や、未遂も刑罰の対象となっている州がある。ドイツは連邦国家であるので、州によって過料規定や刑罰規定に差異があることにも一定の合理性があるだろう。しかし、そのような社会実体のない日本では、刑罰や過料の規定を含んだ個人情報保護法制は統一的なものであるべきだろう。また、EU データ指令を受けて、一般的な個人データとは区別された「特別な種類の個人データ」という概念を導入している点は、イギリスデータ保護法とフランス1978年法と共通している。「特別な種類の個人データ」には、人種的出自・宗教的信条・健康状態などといった情報が含まれる。ドイツ連邦データ保護法においても、イギリス・フランスと同様に「特別な種類の個人データ」の取り扱いのための

個別の条件を設けており、一般的な個人データのそれに比して条件が多く、内容も具体的なものになっている。しかし、一般的な個人データとは区別されるものとして規定されているにもかかわらず、特別な種類の個人データを不正取得する等の行為について個別の過料・刑罰規定が設けられていないという点についてはイギリスデータ保護法と同様である。イギリスと同様、ドイツ連邦データ保護法も「センシティブな個人データ」という概念をEU指令からそのまま導入しており、個別の規定を設ける必要性までは検討していなかったのではないだろうか。データの取り扱いの段階で厳密な条件を設けるという事前規制によって十分な保護が図られると解したものと思われる。

第３節で述べたとおり、ドイツにおいては過料の科される事例が希少である。その根拠について、監督官庁の人員が不十分であることによって監督業務が満足に行われていないとする指摘もあるが、多くの企業が監督機関の実務に対して協力的であるという州の独立委員会の報告もなされている。特に企業にとっては、過料や刑罰を科されることは社会からの信用を損なうことにつながりかねないので、監督機関による指導・助言に従う場合が多いのだと思われる。その結果、過料が科されるのは、データ保護法違反による被害が広範囲であったり、再三の違反が行われたりするような悪質なケースに限られている。刑罰にいたっては、ほとんど実例を見ない。

このように、過料・刑罰が科される事例が希少であるということになれば、過料・刑罰規定の存在意義と、将来的に刑罰規定を創設することについて疑問が呈される余地もあるだろう。しかし、過料・刑罰規定の存在には一般予防・特別予防の効果が認められるはずである。ドイツにおいても、イギリス・フランスと同様に、独立の第三者機関による取り締まりと監督に加えて、情報窃盗などの行為を直接的に処罰する規定の存在することにより、悪質な違反行為が一定程度抑制されているといえるのではないだろうか。過料・刑罰の濫用の危険については、ドイツ各州の監督機関が慎重に過料・刑罰の実務を行うことによる予防が効果的に行われている。また、企業等は社会的信用を損なうことを危惧して、過料・刑罰の対象となり得る行為を控えることが考えられるが、一般人は必ずしもそうではないと考えられる。やはり、情報窃盗や無権限によ

る第三者提供などの行為を予防するためには刑罰規定が必要とされる場合もあるだろう。

［付記］本稿は、北海道大学審査博士（法学）学位論文（2014年３月25日授与）「個人情報の刑法的保護の可能性と限界について」に加筆・修正したものである。