2013年12月22日堀部政男情報法シンポジウム

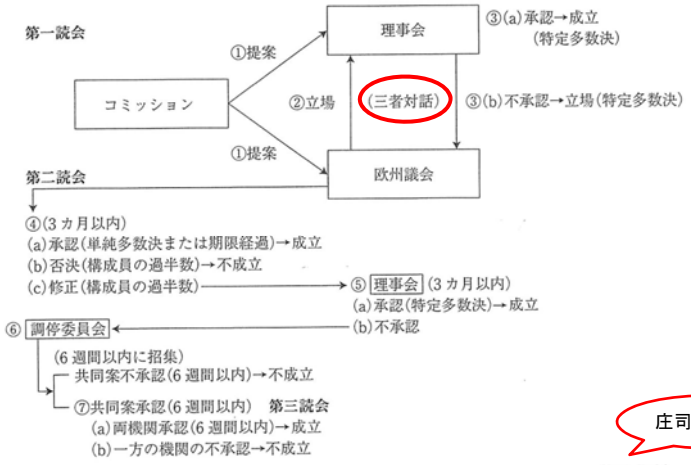
EU一般データ保護規則提案とLIBE委員会による修正案可決

筑波大学図書館情報メディア系
准教授　石井夏生利

1

採択までの手続①

図表 3-3　通常立法手続(EU 機能条約第 294 条)



庄司先生作成

(筆者作成)

庄司克宏『新EU法　基礎編』(岩波書店、2013年)89頁を一部修正

2

採択までの手続②

- 主管委員会は、市民的自由・司法・内務委員会 (Committee on Civil Liberties, Justice and Home Affairs, LIBE委員会)
- 報告担当者は、Jan Philipp ALBRECHT氏

✓ 2013年1月16日　LIBE委員会の草案
✓ 3000件以上の意見の絞り込み
✓ 採決の予定が遅れる。
✓ その間、PRISM問題や盗聴問題が発生。
✓ 2013年10月21日　LIBE委員会での修正案可決
✓ 2013年11月22日　本会議(第一読会)用の修正案
✓ 2014年3月11日　第一読会開催の見込み

*閣僚理事会は、総合方針(General Approach)により立場を決定:2013年12月5日～6日にかけて議論

3

追加・削除等

追加

- 前文：14項目(39a、39b、54a、58a、71a、71b、74a、75a、98a、106a、119a、122a、123a、125a)
- 本条：15条(第10a条、第13a条、第32a条、第33a条、第43a条、第45a条、第54a条、第58a条、第60a条、第80a条、第82a条、第83a条、第85a条、第85b条、第89a条)

削除

- 前文：6項目(34、40、41、73、107、132)
- 本条：3条(第18条、第59条、第60条)

*第28条「文書化の義務」は、多くの規定が削除

- 以上のほかに、多くの項目・規定が修正(内容が殆ど入れ替わった規定もある)
- タイトルの修正された節や規定もある。

4

変更なし

- 対象事項/目的(第1条)
- 監督機関(第46条)
- 監督機関の独立性等を定める第47条以下も、一部に文言の修正はあるものの、大きな修正はない。

⇩

目的・理念、監督機関の考え方については、EU関係者に大きな違いはないものと考えられる。

5

地域的範囲(第3条)

規則提案

- EU内の管理者又は処理者による個人データの取扱い

(EU内で設立されていない管理者による場合)

- EU内に居住するデータ主体に商品又はサービスを提供する場合
- 彼らの行動を監視する場合

⇩

LIBE修正案

- 取扱いがEU内で行われるか否かを問わない。

(EU内で設立されていない場合)

- 処理者にも適用
- EU内のデータ主体に対して商品又はサービスを提供する場合に、データ主体の支払いが義務づけられるか否かを問わない。
- データ主体を監視する場合

6

定義(第4条)

- 「データ主体」と「個人データ」の修正
- 「仮名データ」の追加
- 「暗号化データ」の追加
- 「プロファイリング」の追加
- 「第三者」の追加
- 「遺伝データ」の修正
- 「主たる事業所」の修正

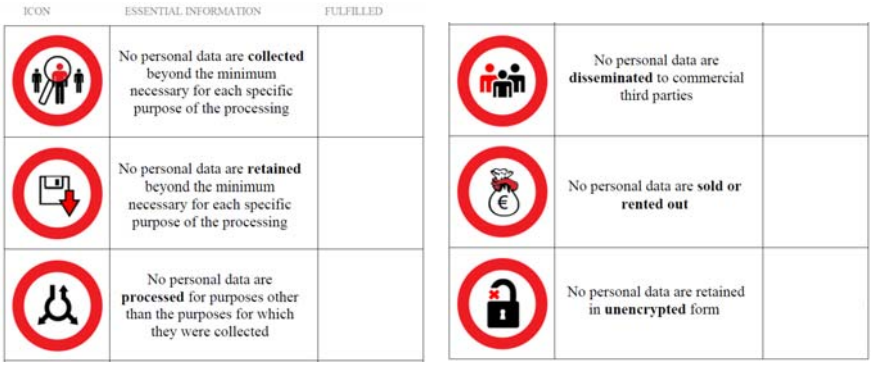
7

個人データの取扱いに関する諸原則(第5条)

- 「適法性、公正性及び透明性」、「目的制限」、「データ最小化」、「正確性」、「保存最小化」、「責任」の名称追加
- 「データ主体が自らの権利を効果的に行使できるような方法で取り扱う」(有効性)の追加
- 「適切な技術的又は組織的な措置を用いて、無権限又は違法な取扱い、及び、偶発的な紛失、破壊又は損失から保護される方法で取り扱う」(完全性)の追加

8

標準化された情報ポリシー(第13a条)



ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **processed** for purposes other than the purposes for which they were collected	
	No personal data are **disseminated** to commercial third parties	
	No personal data are **sold or rented out**	
	No personal data are retained in **unencrypted** form	

わかりやすさの追求

(http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN)

9

忘れられる権利及び削除権(第17条)→削除権

LIBE修正案

- 管理者に対し、自らに関する個人データを削除させる権利、当該データのさらなる拡散を停止させる権利
- 第三者に対し、当該データのあらゆるリンク、コピー又は複製を削除させる権利

*データ管理者によるデータ主体の本人確認能力に依拠する。

- 管理者は、第6条1項(適法な取扱いのための条件)に基づく正当化理由なしに個人データを公開していた場合、第三者による削除を含め、当該データを削除するためのあらゆる合理的措置を講じなければならない。
- 管理者は、データ主体に対し、可能な場合には、関連する第三者が取った行動を通知しなければならない。

10

プロファイリングに基づく措置(第20条)
→プロファイリング

LIBE修正案

- 「プロファイリング」とは、自然人に関する一定の個人的側面を評価すること、又は、特に、当該自然人の職務上の成果、経済状況、位置、健康、個人的嗜好、信頼性若しくは行動を分析若しくは予測することを意図した、あらゆる形式の自動個人データ処理をいう。
- 異議申立権
- 差別的措置の禁止
- データ主体に法的効果を生じさせる措置等をもたらすプロファイリングには、人の評価を含めなければならない。

*仮名化データの取扱いのみに基づくプロファイリングは、データ主体の利益、権利又は自由に重大な影響を与えないと推定すべきである。単一情報源の仮名データに基づくか、異なる情報限からの仮名化データの集積に基づくかによらず、管理者がプロファイリングにより、仮名化データを特定のデータ主体に帰属させることができる場合、取り扱われるデータは、もはや仮名とはみなされるべきではない。(前文58a項)。
*リスク評価項目の1つにプロファイリングが追加。

(参考)欧州評議会の2010年勧告文書(CM/Rec(2010)13)でも取り上げられている。 11

例外規定

第2条「実体的範囲」:LIBE修正案

- 限定数の人々のみがアクセスすることを合理的に期待できる場合における、個人データの公表
- 共同体の機関や組織等→規則が適用される
- 自然人の個人的活動(非営利性を問わない)

第21条「制限」:LIBE修正案

- 制限対象の規定が一部削除(第5条の一部と第20条)
- 立法措置による場合に求められる要件の追加
- 民間の管理者による追加データの保有

第80条「個人データの取扱いと表現の自由」:LIBE修正案

- 構成国は、EU基本権憲章に基づき、個人データ保護の権利と表現の自由を保護するルールを調和させるために必要な場合はいつでも、第Ⅱ章～第Ⅶ章、及び、第Ⅸ章における特別のデータの取扱状況からの適用除外又は特例の規定を設けるものとする。

12

データ保護侵害通知（第31条、第32条）

監督機関への通知義務

- 「過度に遅滞することなく、かつ、実行可能な場合には個人データ侵害を認識した時から24時間までに」→「過度に遅滞することなく」
- 情報は段階的に通知することができる。

取扱者から管理者への警告及び情報提供義務

- 「直ちに」→「過度に遅滞することなく」

13

「データ保護影響評価及び事前の許可」→「ライフサイクルデータ保護管理」

- 第32a条「リスクの考慮」(新設)：取扱業務に関するリスク評価及び分析に基づき、一定の義務が課せられる。
- 第33条「データ保護影響評価」：個人データの全ライフサイクル管理を考慮しなければならない。
- 第33a条「データ保護遵守審査」(新設)：データ保護影響評価の実施から2年後までの間に遵守審査を実施しなければならない。
- 第34条「事前協議」(タイトル変更)：第三国又は国際機関へのデータ移転に関して、監督機関から事前の許可を取得することを義務づける規定の削除。

14

認証制度の重視(第39条)

- 管理者又は処理者による認証申請(特に、第5条、第23条、第30条の諸原則、管理者及び処理者の義務、データ主体の権利)
- 監督機関と欧州データ保護会議による一貫性の仕組み(第57条)を通じた協力
- 第三者による審査可
- 認証を受けた管理者又は処理者に対する「欧州データ保護シール」の付与
- 「欧州データ保護シール」は、管理者又は処理者が本規則を遵守し続ける限りで有効(ただし認証は最大5年間)。
- 欧州データ保護会議は、電子的な公募を設置し、有効及び無効の認証を一般公衆が見られるようにしなければならない。

*監督機関の権限及び義務に、管理者及び処理者の認証が追加

15

第三国等への移転

十分性 ⇨ 適切な安全保護措置 ⇨ 特例

BCR、標準データ保護条項、データ保護シールなど

同意など

- 第41条「十分性決定に伴う移転」:法の実施、先行する判決、十分な制裁権限
- 第42条「適切な安全保護措置による移転」
- 第43条「拘束的企業準則による移転」
- 第43a条「EU法が許可していない移転又は開示」(新設)
- 第44条「特例」:「管理者又は処理者の追求する適法な利益のために必要である場合」が削除
- 第45a条「委員会による報告」(新設)

16

安全保護措置に基づく移転(第42条)

- 欧州委員会が十分性決定を下していない場合、ないしは、**「第三国又は第三国の地域若しくは取扱部門、又は、国際機関が十分な保護レベルを確保していないと決定した場合」**は、法的に拘束力ある方法において、個人データ保護に関する適切な安全保護措置を提示した場合に、データ移転を行うことができる。

⇩

- ✓ その1つが、管理者及び受領者に対して有効な「欧州データ保護シール」
- ✓ BCR、標準データ保護条項、欧州データ保護シールに基づく移転には、特別の許可を求めてはならない。

17

行政的制裁(第79条)

規則提案:違反の種類による段階的制裁金

- 250,000ユーロ、又は、企業の場合は全世界の年間総売上の0.5%まで
- 500,000ユーロ、又は、企業の場合は全世界の年間総売上の1%まで
- 1,000,000ユーロ、又は、企業の場合は全世界の総売り上げの2%まで

考慮事項:侵害の性質、重大性及び期間、侵害に関する故意又は過失の性質、自然人又は法人の責任の程度、当該人物の過去の違反行為、第23条に基づき実施された技術的及び組織的措置及び手続、並びに、侵害を回復するために行った監督機関との協力の程度

⇩

LIBE修正案:違反行為の類型は特定せず

- 本規則に定める義務を遵守しない者に対し、監督機関は、少なくとも、次に掲げる制裁の一を課すものとする。
  a) 初回の、故意によらない違反の場合は、文書による警告
  b) 定期的なデータ保護監査
  c) 100,000,000ユーロ、又は、企業の場合は全世界の年間総売上の5%までの制裁金のうち、いずれか高い方

より詳細な考慮事項を規定

*規則提案では、データ保護シールの悪用は、「1,000,000ユーロ…総売り上げの2%まで」の対象であったが、LIBE修正案では、管理者等が有効な「欧州データ保護シール」を保有している場合には、制裁金は、故意又は過失による違反の場合のみとされている。

18

委任行為

規則提案：26の規定に関する委任行為

⇩

LIBE提案：10の規定に変更(追加＆削除)

- 標準化された情報ポリシー(第13a条)
- 削除権(第17条)
- 行動規範(第38条)
- 認証(第39条)
- 十分性決定に伴う移転(第41条)：十分性の保証と非保証
- 拘束的企業準則による移転(第43条)
- 行政的制裁(第79条)
- 健康に関する個人データの取扱い(第81条)
- 雇用状況における取扱い(第82条)

*欧州データ保護会議への事前の意見照会を条件とするもの
*(削除された規定に関して)欧州データ保護会議が指針等を発出するもの
*利害関係者への意見照会が求められるもの
*廃止条項を設けなければならないもの
*特段の条件は付されていないもの

19

実施行為

規則提案

- データ主体の権利行使やデータ管理者の義務等に関する標準書式、手続、技術標準、電子的手段による情報交換のための書式及び手続等、その他一部の実体的事項に関する規定についての採択権限

⇩

LIBE修正案

- 手続関係規定を削除し、実体規定を委任行為へと変更する等の修正

20

一貫制の仕組み

- 制度趣旨：EU域内の複数の国をまたいで事業を行う管理者にとって、複数のデータ保護機関の各監督に服するという不安定さを取り除くこと。

LIBE修正案：主管機関(第54a条)

- EU内の管理者又は処理者が一を超える構成国で設立された場合、又は、複数の構成国の住民の個人データが取り扱われる場合、管理者又は処理者の主たる事業所の監督機関は、主管機関として活動し、全ての構成国における管理者又は処理者の取扱いを監督する責任を負う。

21

セーフ・ハーバーの継続(第41条8項)

規則提案

- データ保護指令第25条6項又は第26条4項に基づき採択された決定は、欧州委員会によって修正され、置き換えられ、又は廃止されるまでの間は効力を有する。

⇩

LIBE修正案

- データ保護指令第25条6項又は第26条4項に基づき採択された決定は、本規則施行後5年の間は、効力を有する。ただし、当該期間満了前に、欧州委員会によって修正され、置き換えられ、又は廃止された場合はこの限りでない。

22

5000人要件の妥当性？

LIBE提案

- 例外事項：「従業員が250人未満の企業」→「連続する12ヶ月間に5000人未満のデータ主体に関する個人データを取り扱い、かつ、第9条(1)項に定める特別なカテゴリの個人データ、大規模なファイリングシステム内で位置データ又は児童若しくは従業員のデータを取り扱わない管理者」
- リスク評価の項目：「連続する12ヶ月間に5000人を超えるデータ主体に関する個人データを取り扱う場合」
- 義務要件：「従業員が250人以上の企業」→「取扱いが法人により行われ、連続する12ヶ月間に5000人を超えるデータ主体に関する個人データを取り扱う場合」

(cf)　FTCプライバシーレポート

枠組の適用範囲：枠組は、特定の消費者、コンピュータ又は装置と合理的に結びつけられる消費者データを収集又は利用する全ての営利事業者に適用される。ただし、当該事業者が、年間5000人未満の消費者の非センシティブデータのみを収集し、第三者との間でそのデータを共有しない場合は、この限りではない。

23

その他

- 欧州データ保護会議の権限、センシティブデータ、「管理者又は取扱者の求める正当な利益」の妥当性、個別の例外規定の範囲、法執行機関とそれ以外の機関との越境データ流通等、種々の論点あり

24