

(2014年5月7日)

**プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告 (2013)**

堀部政男、新保史生、JIPDEC (野村至) 仮訳

"Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data"日本語版の質およびオリジナル版との整合性については日本語版の著者である JIPDEC が責任を有する。ガイドラインのオリジナル版と日本語版で翻訳等に不一致が認められる場合、オリジナル版のテキストが優先される。本翻訳は仮訳であって、正確には原文を参照されたい。

The quality of the Japanese version of the work which is "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" and its coherence with the original language text of the work are the sole responsibility of JIPDEC as the author of the Japanese version of the work. In the event of any discrepancy between the original work and the Japanese version of the work, the text of the original work shall prevail.

OECD によるオリジナル版 (英語版とフランス語版) は以下のタイトルで発行されている:

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

© 2013 JIPDEC for this Japanese edition

Originally published by the OECD in English and in French under the titles:

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

© 2013 JIPDEC for this Japanese edition

## 勸告附属文書

### Annex

# プライバシー保護と個人データの国際流通についてのガイドライン Guidelines governing the protection of privacy and transborder flows of personal data

## 第1部 総論

### PART ONE. GENERAL

#### 定義

##### Definitions

1. 本ガイドラインにおいて、
  1. For the purposes of these Guidelines:
    - a) 「データ管理者」とは、国内法によって個人データの内容及び利用に関して決定権限を有する者を意味し、当該管理者又はその代理人が、当該データを収集、保有、処理若しくは提供するか否かは問わない。
    - a) “Data controller” means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.
    - b) 「個人データ」とは、識別された又は識別されうる個人（データ主体）に関するすべての情報を意味する。
    - b) “Personal data” means any information relating to an identified or identifiable individual (data subject).
    - c) 「プライバシーを保護する法」とは、国内の法律又は規則を意味し、当該法令の施行により、本ガイドラインと一貫性を有する個人データ保護の効果を有する。
    - c) “Laws protecting privacy” means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines.
    - d) 「プライバシー執行機関」とは、プライバシーを保護する法の執行に係る責任を有し、調査の実施又は執行手続きを遂行する権限を有する各加盟国が設置する公的機関を意味する。
    - d) “Privacy enforcement authority” means any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings.

- e) 「個人データの国際流通」とは国境を越えて、個人データが移転することを意味する。
- e) “Transborder flows of personal data” means movements of personal data across national borders.

## ガイドラインの適用範囲

### Scope of Guidelines

2. 本ガイドラインは、個人データの処理の態様又は利用の性質若しくは状況に鑑み、プライバシー及び個人の自由へのリスクを生じさせる、公的分野又は民間分野における個人データの取扱いに適用する。

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties.

3. 本ガイドラインの原則は相互に補完的な関係にあり、すべての原則を総括的に解釈すべきである。本ガイドラインは、次のように解釈すべきではない。

3. The principles in these Guidelines are complementary and should be read as a whole. They should not be interpreted:

- a) 個人データの性質及びその収集、保有、処理及び提供の状況から、個人データの種類の違いに応じて、異なる保護措置を適用することを妨げるもの、又は、

- a) as preventing the application of different protective measures to different categories of personal data, depending upon their nature and the context in which they are collected, stored, processed or disseminated; or

- b) 表現の自由を不当に制限するもの。

- b) in a manner which unduly limits the freedom of expression.

4. 本ガイドラインの適用が除外される例外は、国家の主権、国家の安全保障及び公序良俗に関係するものも含め

4. Exceptions to these Guidelines, including those relating to national sovereignty, national security and public policy (“ordre public”), should be:

- a) できる限り少なくすること、及び、

- a) as few as possible, and

- b) 国民に知らしめること。

- b) made known to the public.

5. 連邦国家のように特別の場合には、ガイドラインの遵守は、連邦制における権力の分立によって影響を受けることがある。

5. In the particular case of federal countries the observance of these Guidelines may be affected by the division of powers in the federation.

6. 本ガイドラインは最低限の規範を定めたものであって、プライバシー及び個人の自由を保護するため、個人データの越境流通にも影響を与える可能性があることに鑑み、その他の基準により補完することができる。

6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data.

## 第2部 国内適用における基本原則

### PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

#### 収集制限の原則

##### Collection Limitation Principle

7. 個人データの収集には制限を設け、いかなる個人データも、適法かつ公正な手段によって、及び必要に応じてデータ主体に通知し、又は同意を得た上で収集すべきである。

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

#### データ内容の原則

##### Data Quality Principle

8. 個人データは、利用目的の範囲内において利用し、かつ利用目的の達成に必要な範囲内で正確、完全及び最新の内容に保つべきである。

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

## 目的明確化の原則

### Purpose Specification Principle

9. 個人データの収集目的は、データが収集された時点よりも前に特定し、当該利用目的の達成に必要な範囲内における事後的な利用又はその他の目的での利用は、その利用目的に矛盾しない方法で行い、利用目的を変更するにあたっては毎回その利用目的を特定すべきである。

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

## 利用制限の原則

### Use Limitation Principle

10. 個人データは、第 9 項により特定された目的以外の目的のために開示すること、利用可能な状態に置くこと又はその他の方法で利用すべきではない。ただし、以下の場合はこの限りではない。

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) データ主体の同意がある場合、又は、
- a) with the consent of the data subject; or
- b) 法令に基づく場合。
- b) by the authority of law.

## 安全保護措置の原則

### Security Safeguards Principle

11. 個人データは、その滅失若しくは不正アクセス、き損、不正利用、改ざん又は漏えい等のリスクに対し、合理的な安全保護措置を講ずるべきである。

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

## 公開の原則

### Openness Principle

12. 個人データの活用、取扱い、及びその方針については、公開された一般的な方針に基づくべきである。その方法は、個人データの存在及び性質に応じて、その主要な利用目的とともにデータ管理者の識別及び通常の所在地を認識できる方法によって示すべきである。

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

## 個人参加の原則

### Individual Participation Principle

13. 個人は次の権利を有する。

13. Individuals should have the right:

- a) データ管理者が自己に関するデータを保有しているか否かについて、データ管理者又はその他の者から確認を得ること。
  - a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
  - b) 自己に関するデータを保有している者に対し、当該データを
  - b) to have communicated to them, data relating to them
    - i. 合理的な期間内に、
    - i. within a reasonable time;
    - ii. 必要がある場合は、過度にならない費用で、
    - ii. at a charge, if any, that is not excessive;
    - iii. 合理的な方法で、かつ、
    - iii. in a reasonable manner; and
    - iv. 本人が認識しやすい方法で、
    - iv. in a form that is readily intelligible to them;
- 自己に知らしめられること。
- c) 上記 (a) 及び (b) の要求が拒否された場合には、その理由が説明されること及びそのような拒否に対して異議を申立てることができること。
  - c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

- d) 自己に関するデータに対して異議を申し立てること及びその異議が認められた場合には、そのデータを消去、訂正、完全化、改めさせること。
- d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

## 責任の原則

### Accountability Principle

- 14. データ管理者は、上記の諸原則を実施するための措置を遵守する責任を有する。
- 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

## 第3部 責任の履行

### PART THREE. IMPLEMENTING ACCOUNTABILITY

- 15. データ管理者は以下のことに責任を有する。
- 15. A data controller should:
  - a) 以下のプライバシーマネジメントプログラムを構築すること。
  - a) Have in place a privacy management programme that:
    - i. 管理下にあるすべての個人データに対するガイドラインを実施し、
    - i. gives effect to these Guidelines for all personal data under its control;
    - ii. 取扱いの体制、規模、量、センシティブリティに応じて、
    - ii. is tailored to the structure, scale, volume and sensitivity of its operations;
    - iii. プライバシーリスク評価に基づく適切な保護措置を実施し、
    - iii. provides for appropriate safeguards based on privacy risk assessment;
    - iv. ガバナンス体制への組み入れと内部監査メカニズムを確立し、
    - iv. is integrated into its governance structure and establishes internal oversight mechanisms;
    - v. 問合せ及びインシデントへの対応計画を含め、
    - v. includes plans for responding to inquiries and incidents;
    - vi. 継続的なモニタリングと定期的評価を考慮した見直しを実施すること。
    - vi. is updated in light of ongoing monitoring and periodic assessment;

- b) 当該プライバシーマネジメントプログラムが適切に実施されていることを証明する準備を行い、特に、権限を有するプライバシー執行機関又は行動規範若しくは本ガイドラインに拘束力を与えるのと同等の取り決めの遵守を促進させる上で責任を有するその他の組織からの求めに応じて対応すること。
- b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and
- c) 個人データに影響を及ぼす重大なセキュリティ侵害があった場合、必要に応じてプライバシー執行機関又は他の関連機関に通知すること。当該セキュリティ侵害がデータ主体に不利益を及ぼすと思料される場合は、データ管理者は不利益を被るデータ主体に通知すべきである。
- c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

#### 第4部 国際的適用における基本原則—自由な流通と合法的制限

##### PART FOUR. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

16. データ管理者は、管理下にある個人データに対して、当該データの所在に関係なく責任を有し続ける。

16. A data controller remains accountable for personal data under its control without regard to the location of the data.

17. 加盟国は、自国と他の国との間における個人データの国際流通について、ガイドラインに一致する継続的な保護のレベルを保つために、(a) 他の国がガイドラインを実質的に遵守している場合、又は (b) 効果的な執行メカニズム及びデータ管理者により導入される適切な措置を含め、十分な保護措置がある場合、この流通を制限することを控えるべきである。

17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.



18. 個人データの国際流通に対するいかなる制限も、顕在するリスクに比例した制限でなければならず、データのセンシティブティ並びに処理の目的及び状況を考慮すべきである。

18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

## 第5部 国内実施

### PART FIVE. NATIONAL IMPLEMENTATION

19. ガイドラインを履行するにあたり、加盟国は以下の事項を実施すべきである。

19. In implementing these Guidelines, Member countries should:

- a) 政府機関全体で調整を行った提案を反映した国内のプライバシー保護方針を  
発展させ、
- a) develop national privacy strategies that reflect a co-ordinated approach across  
governmental bodies;
- b) プライバシーを保護する法を整備し、
- b) adopt laws protecting privacy;
- c) プライバシー執行機関を設立して維持し、当該機関の権限を効果的に行使し、  
客観的かつ公正で一貫した基準に基づく決定を行うために必要な管理組織、  
リソース、技術的専門知識を備え、
- c) establish and maintain privacy enforcement authorities with the governance,  
resources and technical expertise necessary to exercise their powers effectively and to  
make decisions on an objective, impartial and consistent basis;
- d) 行動規範又はその他の形式による自主規制を奨励し及び支援し、
- d) encourage and support self-regulation, whether in the form of codes of conduct or  
otherwise;
- e) 個人の権利を行使するための合理的な手段を提供し、
- e) provide for reasonable means for individuals to exercise their rights;
- f) プライバシーを保護する法が遵守されないとき、適切な制裁及び救済手段を  
提供し、
- f) provide for adequate sanctions and remedies in case of failures to comply with laws  
protecting privacy;
- g) 教育及び普及啓発、能力開発並びにプライバシー保護に資する技術的措置の  
向上を含め、補完となる基準の採択を検討し、
- g) consider the adoption of complementary measures, including education and  
awareness raising, skills development, and the promotion of technical measures  
which help to protect privacy;

- h) データ管理者以外の者が果たすべき役割を、各個人の役割に応じて検討し、
- h) consider the role of actors other than data controllers, in a manner appropriate to their individual role; and
- i) データ主体が不公正な差別を受けないようにすること。
- i) ensure that there is no unfair discrimination against data subjects.

## 第6部 国際協力と相互運用性

### PART SIX. INTERNATIONAL CO-OPERATION AND INTEROPERABILITY

20. 加盟国は、プライバシー法の国境を越えた執行協力を容易にするために、特に、プライバシー執行機関の間で情報共有を強化することにより、適切な措置を講ずるべきである。

20. Member countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.

21. 加盟国は、本ガイドラインに実質的に影響を及ぼすプライバシーフレームワーク間の相互運用性を促進させる国際協定醸成を推進し、支援すべきである。

21. Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.

22. 加盟国は、プライバシー及び個人データの国際流通に関する政策決定プロセスに知見を提供するために、国際的に比較できる評価指標の開発を推進すべきである。

22. Member countries should encourage the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.

23. 加盟国は、本ガイドラインの遵守状況の詳細を公表すべきである。

23. Member countries should make public the details of their observance of these Guidelines.