KGRI
Keio University Global Research Institute

KGRI Working Papers

No.1

「Comparative Law Research on the Personal Data Protection Law in Various Countries」

Version1.0

November 2023

Editorial Representation

Tatsuhiko Yamamoto

Professor, Law School & Deputy Director of Keio University Global Research Institute, Keio University,

Editing

Kyoichi Iida

Researcher, Law School, Keio University & attorney at law

Taiki Sato

L.L.D. Candidate, Keio University

Keio University Global Research Institute

「Comparative Law Research on the Personal Data Protection Law in Various Countries」

【Editor's Representative】

Tatsuhiko Yamamoto (Professor, Law School & Deputy Director of Keio University Global Research Institute, Keio University)

【Editor】

Kyoichi Iida (Researcher, Law School, Keio University & attorney at law)

Taiki Sato (L.L.D. Candidate, Keio University)

【Author】

EU : **Elaine Fahey** (Professor, City University of London Law School)

Germany : **Meinhard Schröder** (Professor, Faculty of Law ,University of Passau)

Switzerland : **Florent Thouvenin** (Professor, Faculty of Law, University of Zurich)

France : **Yukiko Ogawa** (Assistant Professor, Faculty of Law, Teikyo University)

Thailand : **Thitirat Thipsamritkul** (Full-time Lecturer ,Faculty of Law, Thammasat University)

Taiwan : **Chien-Liang Lee** (Professor, Director, Institutum Iurisprudentiae, Academia Sinica, Taiwan)

South Korea : **Jiyoung Sang** (Visiting Researcher, Keio University & South Korea Attorney at law)

China : **Yuna Matsuda** (Visiting Researcher, KGRI)

Canada : **Kento Yamamoto** (Associate Professor, Faculty of Law, The University of Kitakyushu)

United States : **Jesse W. Woo** (MS CS Candidate at Columbia University・California State Attorney at law)

summary

The aim of “Decentralized Management and Law” (Principal Investigator: Prof. Tatsuhiko Yamamoto, Professor of Constitutional Law at Keio Law School), which is a part of the Moonshot R&D Program (Goal 9) by Japan Science and Technology Agency (JST), is to analyze the benefits and challenges of implementing personal AI in society from legal perspective. Personal AI is Artificial Intelligence that assists individual in management of his or her personal data, based on their privacy preference. This tool is expected to back up the right to informational self-determination or the right to control personal information.

In this research project, we analyze personal data protection laws from comparative law perspective in various countries such as the EU, Germany, Switzerland, France, Thailand, Taiwan, South Korea, China, Canada and the United States. We asked legal scholars from those countries to write reports on the right of data subjects to control their personal data, such as the right to erasure, access, and data portability. We considered the implications and challenges of the right to informational self-determination, focusing on the relationship between constitutional law and personal data protection laws.

Table of Contents

Question List(English)

1. The Relationship between Constitutional Law and Personal Data Protection Law

① Constitutional Status of the Right to Privacy or the Right to Informational Self-Determination

Is the right to privacy or the right to informational self-determination (i.e., the right to self-determination in the management of personal data; das Recht auf informationelle Selbstbestimmung) guaranteed as a constitutional right? If so, is the right to privacy interpreted to be different from the right to informational self-determination?

② Constitutional Significance of the Personal Data Protection Law

If the right to privacy or the right to informational self-determination is constitutionally protected in any sense, is such right defined or stipulated as a purpose or guiding principle of the personal data protection law? In other words, is the personal data protection law characterized as a statute that implements constitutional values or norms such as the right to privacy?

2. The Overview of Personal Data Protection Law

① The Influence of other countries' legal systems

Are there any countries that you have referred to as models in enacting your country's personal data protection law?

② Definition and Scope of "personal data"

Are cookies and other online identifiers included among personal data under the personal data protection law? What is the definition of personal data under the personal data protection law?

③ The Rights of Data Subjects and the Obligations of those who process personal data

(a) The right to erase personal data (e.g., GDPR Article 17) or the right to utilization cease

(b) The Status and Significance of Consent in Personal Data Protection Law (opt-in or opt-out?): When is the consent of the individual required under the personal data protection law? Whether a business is required to obtain the consent of the individual (data subject) when acquiring personal data? When personal data is provided to a third party, is the consent of the individual required to be obtained?

(c) The Limit of the Notice and Consent model and the countermeasure: If there are limits to the self-management model in terms of the limitations of human cognitive abilities, how does your country's personal data protection law address these challenges? For example, is an effective notice required for businesses?

(d) How are devices or architectures such as a Personal Data Store (PDS) being utilized to assist with the person's controllability of their personal data?

(e) Profiling regulations. E.g., the right to object to profiling (GDPR Article 21).

(f) The right to data portability or the right to transmit personal data (e.g., GDPR Article 20) And in what situations are these rights implemented in practice?

④ Organization and authority of the supervisory body enforcing personal data protection law. Sanctions and complaint mechanisms.

⑤ Judicial proceedings or judicial remedy (standing to sue. class action.)

⑥ Utilization of health data for research purposes: Is the consent of the patient required for the use of his/her medical record or biometric data for research purposes or drug development? What legal obligations (such as anonymization) do research institutions have when collecting and utilizing patient health data for research purposes?

＜質問項目（日本語）＞

1、憲法と個人情報保護制との関係性

① プライバシー権ないし情報自己決定権が、憲法上（条文または判例上）保障されているかどうか。またその際、プライバシー権と情報自己決定権との異同が意識されているかどうか。

② プライバシー権ないし情報自己決定権が憲法上の権利として保障されている場合、かかる権利が、個人情報保護法の目的規定のなかに読み込まれているかどうか。別言すると、個人情報保護法が、プライバシー権などの憲法的価値を実現する法令として位置付けられているかどうか。

2、個人情報保護法制の現状と課題

① 個人情報保護法を制定するにあたってモデルとした国はあるか。

② クッキー情報は個人情報保護法制における「個人データ（個人情報）」のなかに含まれているか。個人情報保護法上保護の対象となる「個人データ（個人情報）」の定義。

③ データ主体の権利と事業者の義務。

−(a) 利用停止請求権の範囲。例えば、日本の個人情報保護法では、令和二年の改正で利用停止請求権の範囲が拡大された。

−(b) 同意の位置付け（オプトイン方式かオプトアウト方式か）。本人の同意が要求される場面は。事業者が個人データを取得する場合に当該個人の同意を得ることが義務付けられているかどうか。また、個人データが第三者に提供される場合、当該個人の同意を得ることが義務付けられているかどうか。

−(c) ＜通知＝同意＞モデルの限界とその対策。個人の認知限界という観点から＜通知＝同意＞モデルの限界（同意疲れやプライバシーポリシーの流し読み）が予てから指摘されている。こうした課題に対して、各国の個人情報保護法制がどのように対応しているか（事業者に対して実効的な告知方法を義務付けるなど）。

−(d) 情報銀行や PDS(Personal Data Store)のように、パーソナル・データに対する本人の controllability を補助するための仕組みや制度はどのように社会実装されているか。

−(e) AI の利活用やプロファイリングの場面に特化したデータ保護の仕組みが存在するかどうか。

−(f) データ・ポータビリティ権は保障されているか。またこの権利は具体的にどのような場面で社会実装されているか。

④ 個人情報保護法を執行する監督機関の組織と権限（制裁や告訴の仕組み）。

⑤ 司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

⑥ 研究・医薬品開発を目的とした診療データの二次利用。診療記録等を医薬品開発などの研究目的で利用する場合に、データ主体である患者の同意は要請されるのか。診療データを二次利用するにあたって、匿名加工などの一定の義務が課せられるか。

I. EU

Prof. Elaine Fahey, City Law School, City, University of London

Elaine.fahey.1@city.ac.uk

Question List: EU data privacy

1. The Relationship between Constitutional Law and Personal Data Protection Law

①Constitutional Status of the Right to Privacy or the Right to Informational Self-Determination

European data protection law rests on the assumption that individuals should have control of personal data about them. This control is often labelled as "informational self-determination[1] which is an underlying rationale of the fundamental right to the protection of personal data as enshrined in Art. 8 of the Charter of Fundamental Rights of the European Union. It is understood to relate to the individuals' right to determine which information about themselves will be disclosed, to whom and for which purpose.[2] It differs to a degree from self-management of data privacy, which is not a form of concept applicable to EU law. This distinctive turn backed up by a broad bureacractisation of rights through an architecture of decentralised enforcement with oversight has generated one of the most important divides as to privacy globally. US law has shifted somewhat towards these ideals yet ultimately still champions values that are the antithesis of EU values eg 7 US states now have data privacy laws.[3]

The right to the protection of personal data is enshrined in Article 16 of the Treaty on the Functioning of the European Union (EU) and Article 8 of the EU Charter of Fundamental Rights, thus primary EU law and is subject of a vast enforcement regime at national level and EU level.[4]

---

1 Kuner, Christopher and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary(New York, 2020; online edn, Oxford Academic), https://doi.org/10.1093/oso/9780198826491.001.0001, accessed 30 June 2023.

2 P. Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", The American Journal of Comparative Law, Vol. 37, No. 4, 1989, pp. 675-701

3 IAPP, "US State Privacy Legislation Tracker", https://iapp.org/resources/article/us-state-privacy-legislation-tracker/, accessed 26 June 2023.

4 Vogiatzoglou, Plixavra, and Peggy Valcke (eds), 'Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU Law', Eleni Kosta, Ronald Leenes and Irene Kamara (eds), Research Handbook on EU Data Protection Law (Edward Elgar Publishing 2022) https://www.elgaronline.com/display/edcoll/9781800371675/9781800371675.00010.xml ; Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019) The European Union general data protection

In each Member State there is a data protection authority (DPA) that supervises the application of the data protection law and handle complaints against its violations and a vast range of procedures and remedies are applicable, as outlined below.

Art. 52(3) of the Charter provides that in so far as both documents of the Charter of Fundamental Rights and the European Convention on Fundamental Rights contain corresponding rights the meaning and scope of the rights laid down in the Charter shall be the same as those laid down by the European Convention on Human Rights. However, this provision does not prevent EU law from providing more extensive protection and EU law has developed an autonomous understanding of privacy of note. The European Court of Human Rights ECtHR requires an additional element of privacy in order for personal information to be included in the scope of private life. In this regard, however, EU law may be said to autonomously grant a broad range of rights, albeit with close links conceptually and substantively to ECHR law.

② Constitutional Significance of the Personal Data Protection Law

According to Art. 1 (2) GDPR the regulation aims at protecting "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" The Charter of Fundamental Rights provides for the protection of personal data in Article 8. In EU law, the Charter of Fundamental Rights is now a binding source of rights since the Treaty of Lisbon, including a reference to data protection rights. ECHR law is an important source of law for EU law as its basis, given that the Charter is inspired by it and EU law provides for the accession of the EU to the ECHR in its treaties, currently still ongoing. The Court of Justice increasingly relies upon the Charter of Fundamental Rights to influence the evolution of European data protection law.

↓

2. The Overview of Personal Data Protection Law

① The Influence of other countries' legal systems

regulation: what it is and what it means, Information & Communications Technology Law, 28:1, 65-98, DOI: https://doi.org/10.1080/13600834.2019.1573501 ; Paul De Hert, Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Spriner 2009) https://link.springer.com/book/10.1007/978-1-4020-9498-9#toc

Several global and international organsiations are widely understood to have had the first privacy treaties eg OECD or Council of Europe yet Eurpesan countries retain a specific place for their early adoption of privacy rules. For instance. Sweden, Germany, Austria, Denmark, France, and Luxembourg legislated for privacy laws after the first world data protection law in Germany in 1970.[5] In January 1981, the Council of Europe adopted its Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, the world's first data protection treaty which influenced EU law. Now, rather than tracing other countries influence upon EU law, it is important to note the EU's intent to influence other countries stnadards through global standards on privacy in the form of the GDPR.[6]

②Definition and Scope of "personal data"

The ePrivacy Directive, commonly called the Cookie Law, was passed in 2002 and was amended in 2009 and was intended to be passed to become a so-called ePrivacy Regulation in 2018, at the same time as the GDPR came into force, but it is yet to be adopted. A later ePrivacy Regulation proposal of 2021, was intended to introduce stricter rules regulating the use of cookies (ID identifiers from a user's browser). Under the GDPR, cookie IDs are considered personal data. The law on cookies has provided an extensive basis for the UK to consider removing certain key protections of the GDPR in UK post-Brexit.

↓

③ The Rights of Data Subjects and the Obligations of those who process personal data

a) The right to erase personal data (e.g., GDPR Article 17) or the right to utilization cease

An individual can ask the data controller to erase their personal data, for example if the data is no longer needed to fulfil the processing purpose. In 2014 in its landmark decision in Case C-131/12 *Google Spain and Google* EU:C:2014:317 the CJEU set out the so-called right to be

5 Streinz, Thomas, The Evolution of European Data Law (January 18, 2021). Paul Craig and Gráinne de Búrca (eds), The Evolution of EU Law (OUP, 3rd edn 2021), 902-936, Available at SSRN: https://ssrn.com/abstract=3762971 or http://dx.doi.org/10.2139/ssrn.3762971; Graham Greenleaf, How far can Convention 108+ 'globalise'? Prospects for Asian accessions, Computer Law & Security Review, Volume 40, 2021, 105414, https://doi.org/10.1016/j.clsr.2020.105414.

6 E.g. 2017 Communication from the European Commission, 'Exchanging and Protecting Personal Data in a Globalised World' COM 2017 7 final.

forgotten. This right is now enshrined in law in Art. 17 of the GDPR). In *Google v CNIL* (C-507/17), the Court had to determine the territorial scope of the right to be forgotten and established a general rule of EU-wide de-referencing in connection with measures preventing or at least seriously discouraging access to non-EU search results. Nonetheless, it has as a concept been adopted globally and such caselaw is regarded to be iconic of EU law and has generated much debate as to its implementation, search engine transparency and public figures.[7]

b) The Status and Significance of Consent in Personal Data Protection Law (opt-in or opt-out?)

Processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing. While being one of the more well-known legal bases for processing personal data, Consent is only one of six bases mentioned in the General Data Protection Regulation (GDPR). The others are: contract, legal obligations, vital interests of the data subject, public interest and legitimate interest as stated in Article 6(1) GDPR. The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. Consent must be freely given, specific, informed and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. Caselaw In C-673/17 – *Planet 49 GmbH* ECLI:EU:C:2019:80 as to Article 6(1) GDPR the CJEU held that consent must be given by a clear affirmative act and this rights-centric view of EU law appears key.[8]

c) The Limit of the Notice and Consent model and the countermeasure

As noted above, consent is a core principle of the operation of the GDPR. Its individualism and focus upon human-centric applications of privacy dominates its operation and arguably is at the anthtiesis of the principles outlined by Solove.

7 See https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf Vrabec, Helena U., 'The Right to Be Forgotten', Data Subject Rights under the GDPR (Oxford, 2021; online edn, Oxford Academic, 22 July 2021), https://doi.org/10.1093/oso/9780198868422.003.0006, accessed 22 May 2023.

8 Wiedemann, K. The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?. IIC 51, 543–553 (2020). https://doi.org/10.1007/s40319-020-00927-w

d) How are devices or architectures such as a Personal Data Store (PDS) being utilized to assist with the person's controllability of their personal data?

Personal data stores (PDSs) represent a complex class of technologies that raise interesting many uncertainties in relation to the responsibilities under the GDPR. Processing special categories of personal data is prohibited by Article 9(1) GDPR unless an exemption applies; in commercial contexts, this is generally explicit consent [9] The 'personal and household exemption', which precludes the GDPR from applying to data processing whenever processing occurs 'by a natural person in the course of a purely personal or household activity' with no connection to a professional or commercial activity, is interpreted narrowly. Although PDSs raise challenges under the GDPR where platforms themselves can also pursue commercial objectives by processing user data for their own intentions. PDSs are consent-oriented and may provide means to assist in appropriately obtaining user consent.[10] Overall, their objectives are similar: to empower individual users with more transparency and control over the processing of their personal data.

e) Profiling regulations. E.g., the right to object to profiling (GDPR Article 21).

Under Article 22 of the GDPR, data subjects have the right not to be subject to a decision with legal or significant effects based solely on automated processing or profiling. When automated decisions are exceptionally allowed, according to the conditions set in the second paragraph, the data controller shall implement suitable safeguards for the data subject, such as the right to obtain human intervention, to express their point of view and to contest the decision (Article 22(3) GDPR).

Profiling is 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic

9 Janssen, Heleen and Cobbe, Jennifer and Norval, Chris and Singh, Jatinder, Decentralised Data Processing: Personal Data Stores and the GDPR (December 28, 2020). International Data Privacy Law, Volume 10, Issue 4 Pages 356–384, https://doi.org/10.1093/idpl/ipaa016 (28 December 2020).

10 Bodó, B. and Irion, K. and Janssen, H. and Giannopoulou, A. (2021). Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks. Internet Policy Review,[online] 10(3). Available at: https://policyreview.info/articles/analysis/personal-data-ordering-context-interaction-meso-level-data-governance-regimes [Accessed: 22 May. 2023].

situation, health, personal preferences, interests, reliability, behaviour, location or movements.' (Art. 3(4) LED; Art. 4(4) GDPR). Profiling is itself thus a form of automated decision-making Article 21 GDPR provides that the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. EU data protection law does not prevent the use of either systemic or individualised predictive policing applications if such applications are provided for by law while an array of provisos and conditions detract from the law's certainty and may further limit its utility.[11]

f) The right to data portability or the right to transmit personal data (e.g., GDPR Article 20) And in what situations are these rights implemented in practice?

Article 20 GDPR provides for the right to data portability and the exercise of the right is said to still requires clarification, as a narrow interpretation of this would result in fewer benefits for individuals whilst a wide interpretation of this concept would be a concern for data controllers. As despite the lack of clarity, Article 20 of the GDPR will potentially not cover the transfer of data that has been generated by the service provider for statistical and analytical purposes such as online reputations. It is argued that the wording of the Article 20 of the GDPR limits the scope of the right to data portability to a great extent.

Businesses cannot use Article 20 of the GDPR as the right to data portability is only available to living and identifiable individuals. The right to data portability under Article 20 of the GDPR might not deliver the intended results due to its ambiguity and due to the inherent limitations contained therein such as the rights and freedoms of other data subjects. The right to data portability has many implications eg facilitating market access, preventing high switching costs and alleviating network effects that threaten potential competition in a marketplace.[12]

④Organization and authority of the supervisory body enforcing personal data protection law. Sanctions and complaint mechanisms.

11 Lynskey, Orla, ' Article 20 Right to data portability', in Christopher Kuner and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary (New York, 2020; online edn, Oxford Academic), https://doi.org/10.1093/oso/9780198826491.003.0052, accessed 30 June 2023

12 Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335.

A vast apparatus of provisions is provided for in the GDPR as to supervision mechanisms, authorities and procedures in Articles 75 GDPR onwards, as outlined in the literature review. The CJEU in Case C-132/21 *Budapesti Elektromos Művek* ECLI:EU:C:2023:2 that it was up to the Member States to ensure the consistent and homogeneous application of such GDPR remedies provisions, but they also had to provide safeguards, such as ensuring that Article 47 CFR would not be violated

A not-for-profit body, organisation or association whose statutory objectives are in the public interest and which is active in the field of the protection of data subjects' rights and freedoms may lodge a complaint to a DPA on behalf of a data subject or exercise the right to judicial remedy and the right to seek compensation on behalf of data subjects on account of Article 80 GDPR. The CJEU held recently that under Article 80(2) GDPR, national legislation may allow consumer protection associations to bring legal proceedings for GDPR violations. C-319/20 *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände* ECLI:EU:C:2022:32.

The Advocate General issued an opinion in Case C-300/21 *UI v Österreichische Post* AG ECLI:EU:C:2022:756 regarding preliminary questions asking about the nature of non-material damages for violations of Article 82 GDPR. Among other things, the AG concluded that the compensation for non-material damage does not cover mere upset which a data subject may feel as a result of an infringement.

According to Article 83(5)-(6) GDPR the maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or four percent of an undertaking's worldwide turnover for the last financial year and has been the subject of a highly significant decision in 2023.[13]

⑤Judicial proceedings or judicial remedy (standing to sue, class action.)

13 See EDPB/ Irish Data Protection Commissioner decision as to Meta March 2023. 'Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation' https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf

As outlined in Recital 143 of the GDPR, a vast range of judicial remedies apply as to the Regulation from Article 78 GDPR onwards as will be outlined here. The supervisory authorities under the GDPR are mandated with the powers to consider complaints against infringements of the rights of individuals under the GDPR and also to impose penalties in the form of fines up to a very significant maximum amount on controllers or processors in order for the penalties to be effective. As a result, such entities must be established by Member State law as independent authorities with a fixed term of office and legal guarantees against premature removal from office and full jurisdiction in the matters entrusted to their powers of investigation and decision. As data protection supervisory authorities do not satisfy the requirements for being 'tribunals' under EU law, their decisions must be subject to judicial review by a court pursuaunt to Article 78 GDPR. The objectives of Articles 77–79 must be fulfilled effectively in national law irrespective of any other remedies which may exist under national law.

④Organization and authority of the supervisory body enforcing personal data protection law. Sanctions and complaint mechanisms.

Article 78(1) requires there to be the opportunity under national law *to appeal to a court against* legally binding *decisions of a supervisory authority*. In addition, Article 78(2) requires a judicial remedy to be available against the *inactivity* of a supervisory authority which has been seized of a complaint.'[14]

National courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation.[15] that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid.

14 Indeed, the CJEU has emphasised that it is incumbent on supervisory authorities to examine such complaints 'with all due diligence'. See Case C-362/14 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650, para 5.

15 Case C-645/19 Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit ECLI:EU:C:2021:483.

⑤Judicial proceedings or judicial remedy (standing to sue. class action.)

The main reason for the increased attention garnered by the GDPR can be attributed to its new sanctions regime, which seems inspired by EU competition law. Whereas the DPD had largely left it to Member States how to sanction violations, the GDPR required 'effective, proportionate and dissuasive penalties' and stipulated that administrative fines could amount to up to 4 per cent of an undertaking's worldwide annual turnover.

As noted above, a not-for-profit body, organisation or association whose statutory objectives are in the public interest and which is active in the field of the protection of data subjects' rights and freedoms may lodge a complaint to a DPA on behalf of a data subject or exercise the right to judicial remedy and the right to seek compensation on behalf of data subjects on account of Article 80 GDPR.

⑥Utilization of health data for research purposes

Article 9 (2) (g) of GDPR provides that "the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person [and] data concerning health" are permitted if " [such a] processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".
We have a question about the relationship between this provision and the utilization of health data for research purposes. Is the consent of the patient required for the use of his/her medical record or biometric data for research purposes or drug development? What legal obligations, other than consent, do research institutions have when collecting and utilizing patient health data for research purposes?
And we would like to know about a recent development in European Health Data Space (EHDP).

In the European Union General Data Protection Regulation 2016/679 (GDPR) there are four elements to its operation: data protection principles; legal bases for processing personal data; information that must be given to the data subject; and, rights of the

data subject; Each element contains a balance of interests. For stand-alone research with human participants directly contacted by the researcher Security and data minimisation standards (i.e. only gathering, analysing and keeping data for such a time necessary for the purpose of the project) must be clear; data subjects must be informed about the project fully, and data subjects rights must be respected. More complex data-sharing methodologies are said to be more difficult to negotiate through the GDPR eg as to whether original consents are valid for the new processing.[16] Together with the Data Governance Act (DGA) and the General Data Protection Regulation (GDPR), the proposal for a Regulation on the European Health Data Space (EHDS) forms the new regulatory and governance framework for the use of health data in the European Union.[17] The European strategy for data, aims to create a single market for data in the EU, and to establish common European data spaces in several strategic fields including health to enable data to become available for use in the economy and society, whilst also protecting the individuals who generate the data in control.[18] Still, there are many controversies as to the rights-centric nature of these issues in EU data protection law- or lack thereof.[19]

A major debate has existed as to decisional privacy and much complexity surrounds how informed must a choice be to qualify as a valid choice from an individual eg in many modern

[16] Townend, D. (2021). Privacy. In G. Laurie, E. Dove, A. Ganguli-Mitra, C. McMillan, E. Postan, N. Sethi, et al. (Eds.), *The Cambridge Handbook of Health Research Regulation* (Cambridge Law Handbooks, pp. 73-80). Cambridge: Cambridge University Press. doi:10.1017/9781108620024.010

[17] European Health Data Space." European Commission.; European Commission, "Proposal for a Regulation of the European parliament and of the Council on the European Health Data Space" COM/2022/197 FINAL, May 3, 2022 <https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en> (accessed 1 July 2023).

[18] Also: in the Digital Services Act (DSA), online platforms and online search engines must assess their risk from design, functioning or use on the protection of public health, minors, and serious negative consequences to a person's physical and mental well-being. In the Digital Markets Act (DMA), the Commission grants an exemption to gatekeepers on the grounds of public health and allows the processing of personal data previously prohibited.

[19] EDRi. "EU's proposed health data regulation ignored patients' privacy rights." EDRi. March 6, 2023. <https://edri.org/our-work/eu-proposed-health-data-regulation-ignores-patients-privacy- rights/>(accessed 1 July 2023).

.

biomedical research methodologies, is contested.[20] Prior to the EHDS, although Article 7(3) GDPR provided that that data subjects had the right to withdraw their consent at any time, there was no indication of the correlative duties of data controllers. The EHDS introduces additional non-scientific justifications for the secondary use of health data. development and innovation activities, algorithmic and AI projects and applications of personalized health care (Art. 34 (1)f-g EHDS). Developing further upon the GDPR, the EHDS will make provisions for the secondary use of health data and is intended to contribute to the 'general interest of society'. Article 34 provides for a permitted purpose as to training, testing and evaluating of algorithms. Other provisions related to other purposes eg scientific research, public health, health-related statistics, education activities, and providing personalised healthcare. Secondary use is prohibited for activities that are detrimental or otherwise harmful to individuals or society at large.

α:The right of access by data subjects (Article 15 GDPR) and AI Article 15 (h) of GDPR provides that the data subjects shall have the right to obtain from the controller confirmation as to "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in 22 those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject". What does "meaningful information" in this provision mean? Generally, common people have no special capacity or expertise to understand the algorithm of AI. What kind of explanation is considered "meaningful information" under case law and guidelines?

Health Data Access Bodies (HDABs) may grant access to health data for secondary use, by issuing a data permit eg to support development, training, testing, and validation of AI systems in health domain under the AI Act.[21] Empirical research in 30 countries (27 EU and 3 EFTA EEA Member

[20] Townend, D. (2021). Privacy. In G. Laurie, E. Dove, A. Ganguli-Mitra, C. McMillan, E. Postan, N. Sethi, et al. (Eds.), *The Cambridge Handbook of Health Research Regulation* (Cambridge Law Handbooks, pp. 73-80). Cambridge: Cambridge University Press. doi:10.1017/9781108620024.010.

[21] See Teodora Lalova Spinks, 'People Have the Power: Patient empowerment in the European Health Data Space proposal (Part I)'

https://www.law.kuleuven.be/citip/blog/people-have-the-power-patient-empowerment-in-the-european-health-data-space-proposal-part-i/ (accessed 1 July 2023); Tjaša Petročnik and Sofia Palmier 'The AI Act and European Health Data Space Proposal Seeing AI

States), consisting of a survey amongst all Data Protection Authorities (DPAs) and interviews with experts of privacy organisations has shown that several types of potentially 'meaningful information' that could be in scope of right of access requests were assessed, as well as several types of information on the consequences for data subjects but rather most of these types of information are rarely or not at all provided in practice.[22]

β)The right of access by data subjects (Article 15 GDPR), the right to data portability and medical records

By exercising the right of access by data subjects (Article 15 GDPR), can the data subject obtain from a hospital his/her medical records or health data? And are these health data included in the data portability rights?

It is conceivable that medical data could be aggregated into an individual app for more personalized medical services. I would like to know about the relationship between such a personalized medical service and European Health Data Space (EHDP).

The GDPR defines the right to data portability in Article 20(1), stating that individuals have the right to receive their personal data in a clear, easy way, and the right to send these data to another controller without hindrance from the original controller. Under the EHDS, the right data portability is found in Article 3(8) EHDS.[23] It is understood to be linked to the primary use of health data in order to allow patients to exchange and provide access to their primary health data processed by public or private controllers between multiple healthcare providers (Article 10(2)(o)(4) EHDS as pharmacies, hospitals, and other points of care).[24] According to the

---

to Ai with one another European Law' Blog 26/2023 < https://europeanlawblog.eu/2023/05/30/the-ai-act-and-european-health-data-space-proposal-seeing-ai-to-ai-with-each-other/> (accessed 1 July 2023).

[22] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) 46 Computer Law & Security Review' 105727.

[23] Florina Pop and Laura Grant 'Data portability in the European Health Data Space: Benefits, Risks, and Challenge' <https://www.eipa.eu/blog/data-portability-in-the-european-health-data-space/#> EUIA Blog (accessed 1 July 2023);

[24] See Teodora Lalova Spinks, 'People Have the Power: Patient empowerment in the European Health Data Space proposal (Part I)' https://www.law.kuleuven.be/citip/blog/people-have-the-power-patient-empowerment-in-the-european-health-data-space-proposal-part-i/ (accessed 1 July 2023).

definition of "electronic health data" and Recital 12, primary data portability in the EDHS, unlike the GDPR, also covers inferred data.

The CJEU held that Article 15(1)(c) GDPR obliges the controller to disclose the identity of specific recipients of personal data if the data subject requests it, unless the request is manifestly unfounded or excessive, in which case information about categories of recipients is sufficient: C-154/21, *RW v Österreichische Post*, 12 January 2023.[25] In 2023, Advocate General Nicholas Emiliou, in an Opinion in the case of C-307/22 *FT v DW* found that Art. 12(5) and Art. 15(3) GDPR had to be interpreted as requiring a data controller to provide the data subject with a copy of his or her personal data, even relating to proceedings where the data subject requested the copy for purposes unrelated to data protection.[26] In that case, a patient of a dental practice, who suspected a treatment error, requested that the dental practice provide him, free of charge, with a copy of all medical records concerning him that were in the possession of the dental practice in preparation for litigation.

※This work was supported by JST [Moonshot R&D][Grant Number JPMJMS2293]

[25] ECLI:EU:C:2023:3.

[26] ECLI:EU:C:2023:315

II. Germany

Report on personal data protection law in Germany

Report über Datenschutzrecht in Deutschland

by *Prof. Dr. Meinhard Schröder* and *Alexander Frammersberger*

University of Passau

Question List/ Fragenkatalog

1. The Relationship between Constitutional Law and Personal Data Protection Law

①Constitutional Status of the Right to Privacy or the Right to Informational Self-Determination

"Is the right to privacy or the right to informational self-determination (i.e., the right to self-determination in the management of personal data; das Recht auf informationelle Selbstbestimmung) guaranteed as a constitutional right? If so, is the right to privacy interpreted to be different from the right to informational self-determination?"

a) Right to privacy

Art. 2 Abs. 1 GG eröffnet mit den Worten: „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit". Damit sollen nach verbreiteter Ansicht[1] zwei eigenständige Grundrechte zum Ausdruck gebracht werden, zum einen die allgemeine Handlungsfreiheit[2] und zum anderen das allgemeine Persönlichkeitsrecht.[3] Während der allgemeinen Handlungsfreiheit nur die Funktion eines Auffanggrundrechts zukommt und sie gegenüber spezielleren Freiheitsrechten subsidiär ist,[4] wurde das allgemeine Persönlichkeitsrecht durch die Rechtsprechung zu einem den Spezialfreiheitsrechten gleichen Recht entwickelt.[5] Es wird stets als „Kombinationsgrundrecht" in Verbindung des Persönlichkeitsrechts aus Art. 2 Abs. 1 GG mit

[1] Andere Ansicht wohl *Kube*, in: HStR VII, § 148 Rn. 108.
[2] Die Garantie derselben ergibt sich vor allem aus einer historischen Auslegung – Art. 2 des Herrenchiemsee-Entwurfs lautete: „Jedermann hat die Freiheit, innerhalb der Schranken der Rechtsordnung und der guten Sitten alles zu tun, was anderen nicht schadet.", vgl. JbÖffR, NF Bd. 1 S. 55 – und aus einer systematischen Auslegung unter Berücksichtigung der weiten Schrankenregelung.
[3] BVerfGE 95, 267 (303); BVerfGE 6, 32 (36 f.); BVerfGE 80, 137 (152 f.).
[4] BVerfGE 85, 214 (217 f.); BVerfGE 148, 267 Rn. 38.
[5] BVerfGE 153, 182 Rn. 205; BVerfGE 118, 168 (183); BVerfGE 106, 28 (36).

der Menschenwürde gem. Art. 1 Abs. 1 GG zitiert.[6] Allerdings kommen dogmatisch nicht zwei Grundrechte kumulativ zur Anwendung, sondern die Verbindung mit Art. 1 Abs. 1 GG dient lediglich als Interpretationsimpuls und Verdeutlichung des Gewährleistungsumfangs.[7] Die Aufladung des allgemeinen Persönlichkeitsrechts durch die Menschenwürde führt dazu, dass von der ursprünglichen ausdrücklichen Kodifikation in Art. 2 Abs. 1 GG etwas abgerückt wurde; der tatsächliche Umfang des allgemeinen Persönlichkeitsrechts also erst in der Kombination dargestellt werden kann. Gewährleistungsgehalt des allgemeinen Persönlichkeitsrechts ist die Integrität der Persönlichkeit, das heißt, das Sein im Unterschied zum Tun.[8] Das Grundrecht gewährleistet dem Einzelnen einen Rückzugsraum der Individualität; er hat das Recht, „in seiner Privatheit in Ruhe gelassen zu werden"[9], „sich selber zu gehören"[10]. Das beinhaltet bis zu einem gewissen Grade auch ein Recht auf Anonymität.[11] Das BVerfG hat dies in der Lebach-Entscheidung anschaulich in die Worte gefasst: „Jedermann darf grundsätzlich selbst und allein bestimmen, ob und wieweit andere sein Lebensbild im ganzen oder bestimmte Vorgänge aus seinem Leben öffentlich darstellen dürfen".[12]

b) Informationelle Selbstbestimmung

Aus dem allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG hat das BVerfG 1983 im Volkszählungsurteil das Recht auf informationelle Selbstbestimmung entwickelt.[13] Das Gericht führte dabei aus, dass die bisherigen Konkretisierungen des Allgemeinen Persönlichkeitsrechts nicht abschließend sind; insoweit kann sich dieses also auch im Zuge neuer Gefahren durch die fortschreitende Entwicklung der Technologie weiterentwickeln.[14] Es bestand also auch bereits vor dem Volkszählungsurteil Schutz für personenbezogene Daten, was das BVerfG mit den Verweisen auf die Entscheidungen „Mikrozensus",[15] „Scheidungsakten",[16] „Arztkartei",[17] „Lebach",[18] und

[6] Im Anschluss an die zivilrechtliche Rechtsprechung BVerfGE 34, 269 (278); schon in der Lüth Entscheidung Art. 2 Abs. 1 GG mit Art. 1 GG in Verbindung bringend BVerfGE 6, 32 (41).
[7] BVerfGE 27, 344 (351); *Rixen*, in: Sachs, GG, 9. Aufl. 2021, Art. 2 Rn. 63.
[8] Vgl. *Rixen*, in: Sachs, GG, 9. Aufl. 2021, Art. 2 Rn. 59; siehe auch bereits *Dürig*, JR 1952, 259 (261).
[9] *Starck*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 2 Abs. 1 Rn. 85.
[10] *Arndt*, NJW 1967, 1845 (1846).
[11] Vgl. dazu *Neumann-Duesberg*, Juristen-Jahrbuch VII, S. 138. Siehe auch *v. Mutius*, Anonymität als Element des allgemeinen Persönlichkeitsrechts – terminologische, rechtssystematische und normstrukturelle Grundfragen, in: Bäumler/v. Mutius, Anonymität im Internet, 2003, S. 12 ff. Siehe auch BGH, NJW-RR 2007, 619 (620).
[12] BVerfGE 35, 202 (220).
[13] BVerfGE 65, 1.
[14] BVerfGE 65, 1 Rn. 152.
[15] BVerfGE 27, 1 (6).
[16] BVerfGE 27, 344 (350 f.).
[17] BVerfGE 32, 373 (379).
[18] BVerfGE 35, 202 (220).

„Suchtkrankenberatungsstelle“[19] belegt. Das BVerfG nahm allerdings die neuen Gefahren durch moderne Informationstechnologie zum Anlass, eine spezifische Ausprägung aus dem Persönlichkeitsrecht in Form der informationellen Selbstbestimmung abzuleiten und so der durch die technischen Neuerungen gesteigerten Bedeutung des Allgemeinen Persönlichkeitsrechts Rechnung zu tragen.[20] Obwohl es sich bei dem Recht auf informationelle Selbstbestimmung um eine Ableitung aus dem Allgemeinen Persönlichkeitsrecht handelt, hebt die Rechtsprechung dessen Eigenständigkeit zunehmend hervor.[21] Das Recht auf informationelle Selbstbestimmung ist als ursprüngliche Ausprägung des Allgemeinen Persönlichkeitsrechts auch von Verfassungsrang; weist aufgrund seiner Ableitung und der damit verbundenen spezifischen Schutzrichtung allerdings keinen expliziten Niederschlag in der Verfassung auf.

c) Difference

Da sich das Recht auf informationelle Selbstbestimmung aus dem Allgemeinen Persönlichkeitsrecht entwickelte, muss man weniger von der Unterschiedlichkeit, sondern eher von der Spezialität sprechen. Das Allgemeine Persönlichkeitsrecht schützt vor staatlichen Eingriffen in die persönliche Integrität. Die einzelne Person muss ihre „Individualität selbstbestimmt entwickeln und wahren“ können.[22] Das allgemeine Persönlichkeitsrecht schützt dabei nur solche Elemente der Entfaltung der Persönlichkeit, die – ohne bereits den besonderen Freiheitsgewährleistungen des Grundgesetzes zu unterliegen – diesen an persönlichkeitskonstituierender Bedeutung nicht nachstehen.[23] Dementsprechend umfasst das Allgemeine Persönlichkeitsrecht etwa das Recht am eigenen Wort,[24] das Recht an eigenen Aufzeichnungen und am eigenen Bild,[25] oder auch die Sexualität des Menschen.[26] In diese Fallgruppen reiht sich grundsätzlich auch der Schutz vor der Verarbeitung personenbezogener Daten ein: Die Daten werden geschützt, da sich aus ihnen Rückschlüsse auf die Persönlichkeit ziehen lassen. Durch die automatisierte Datenverarbeitung ist das allgemeine Persönlichkeitsrecht in besonderem Maße bedroht, worauf mit der besonderen Ausprägung des Rechts auf informationelle Selbstbestimmung reagiert wurde. Insoweit differieren das

[19] BVerfGE 44, 353 (372 f.).
[20] *Dreier*, in: Dreier, GG, 3. Aufl. 2015, Art. 2 I Rn. 79.
[21] BVerfGE 115, 320 (341); BVerfGE 120, 351(360); BVerfGE 133, 277 Rn. 105; ebenso *Jarass*, in: Jarass/Pieroth, GG, 17. Aufl. 2022, Art. 2 Rn. 40.
[22] BVerfGE 141, 186-220, Rn. 32; BVerfGE 35, 202 (220); BVerfGE 79, 256 (268); BVerfGE 90, 263 (270); BVerfGE 117, 202 (225).
[23] BVerfGE 141, 186-220, Rn. 32; BVerfGE 79, 256 (268); BVerfGE 99, 185 (193); BVerfGE 120, 274 (303).
[24] BVerfGE 34, 238 (246 ff.); hinsichtlich der Abgrenzung zu Art. 10 GG oder Art. 13 GG vergleiche etwa *Starck*, in: Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 2 Abs. 1 Rn. 92.
[25] BVerfGE 80, 367 (375).
[26] BVerfGE 47, 46 (73 f.).

Allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung primär hinsichtlich des sachlichen Anknüpfungspunktes und weniger hinsichtlich der abstrakten Schutzintensität. Gleichwohl „flankiert und erweitert" die informationelle Selbstbestimmung den Schutzbereich hinsichtlich spezifischer Gefahren moderner Datenverarbeitung; so verschiebt sich der potentielle Eingriff in den Schutzbereich schon auf das Stadium einer Gefährdung.[27] Für einen effektiven Grundrechtsschutz erweitert die Rechtsprechung den Schutzbereich der informationellen Selbstbestimmung auch dahingehend, dass jede Verarbeitung personenbezogener Daten einen Eingriff darstellt, insoweit soll es kein „belangloses Datum" mehr geben.[28]

Zusammenfassend lässt sich festhalten, dass die informationelle Selbstbestimmung als verselbstständigte Ausprägung des Allgemeinen Persönlichkeitsrechts zu begreifen ist, welche in ihrer Ausformung an die besonderen Anforderungen der Datenverarbeitung bzw. die damit verbundenen Gefahren angepasst wurde. Diese Abgrenzung findet auch Rückhalt in den Ausführungen des BVerfG zu „Recht auf Vergessen I". Darin lag dem Gericht ein Sachverhalt über die Bereithaltung von Presseberichten in einem Onlinearchiv vor. Die Abgrenzung zwischen dem Allgemeinen Persönlichkeitsrecht und der informationellen Selbstbestimmung nahm das Gericht anhand des Schutzbedürfnisses des Betroffenen vor. Insoweit realisiert sich die Gefahr in diesem Fall nicht durch die Datenverarbeitung, sondern durch die öffentliche Verbreitung bestimmter Informationen.[29]

② Constitutional Significance of the Personal Data Protection Law

"If the right to privacy or the right to informational self-determination is constitutionally protected in any sense, is such right defined or stipulated as a purpose or guiding principle of the personal data protection law? In other words, is the personal data protection law characterized as a statute that implements constitutional values or norms such as the right to privacy?"

Die DSGVO statuiert in Art. 1 Abs. 2 DSGVO ausdrücklich, dass es Ziel der Verordnung ist, die Grundrechte natürlicher Personen zu schützen, insbesondere deren Recht auf Schutz personenbezogener Daten. Entscheidend dabei ist, dass die DSGVO nicht *nur* auf den Schutz personenbezogener Daten abzielt, was bereits durch das „insbesondere" in Art. 1 Abs. 2 Hs. 2 DSGVO zum Ausdruck gebracht wird, sondern die Grundrechte insgesamt geschützt werden

[27] So etwa bei der automatischen Kennzeichenerfassung BVerfGE 150, 244 Rn. 37.
[28] BVerfGE 65, 1 (45).
[29] BVerfGE 152, 152 Rn. 91.

sollen. Dies trägt auch dem Umstand Rechnung, dass effektiver Datenschutz nur durch den Schutz verschiedener Grundrechte gewährleistet werden kann.[30]

Aus der Perspektive der europäischen Grundrechte realisiert die DSGVO vor allem Art. 7 und Art. 8 GRCh.[31] Das Ziel des Datenschutzrechts, die einschlägigen verfassungsrechtlichen Positionen zu wahren, verdeutlichen sich auch durch die das Datenschutzrecht prägenden Prinzipien (Prinzip der Schutzräume, Zweckbindungsgrundsatz, Grundsatz der Datenminimierung, Grundsatz des verantwortlichen Datenumgangs).[32] Diese Grundsätze versuchen den Eingriff in die grundrechtliche Positionen auf das Notwendigste zu begrenzen und gewährleisten auch im Falle einer Datenerhebung einen interessengerechten Umgang mit den Daten; insoweit wird dadurch der Grundrechtsschutz des Betroffenen maximiert.

Aus der Sicht des Verfassungsrechts, das im Fall von Öffnungs- und Spezifizierungsklauseln der DSGVO sowie bei der Umsetzung der JI-Richtlinie bedeutsam bleibt, stellt das BDSG einfachgesetzliche Ausprägungen des Rechts auf informationelle Selbstbestimmung dar, insbesondere mit Blick auf die hinreichende Bestimmtheit der gesetzlichen Grundlagen für Datenverarbeitungen, und zugleich auch zum Schutz der Art. 10 GG und Art. 13 GG. Die Einwilligung (Art. 6 Abs. 1 lit. a), Art. 7 DSGVO) ist dabei in besonderem Maße Ausdruck informationeller Selbstbestimmtheit (zur Einwilligung noch S. 11), aber gerade bei der Datenverarbeitung durch öffentliche Stellen aufgrund der möglicherweise fehlenden Freiwilligkeit kontrovers diskutiert. Die Hinweispflichten, welche vor allem bei mittelbarer Erhebung von Bedeutung sind, realisieren Selbstbestimmung (auf einer niedrigeren Stufe), indem sie dem Betroffenen die Information verschaffen, „wer was über ihn weiß“[33] und vermitteln ihm erst die Möglichkeit zur Wahrung seiner Rechte (zur Hinweispflicht, noch S. 14).

[30] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 1 Rn. 36.
[31] Hinsichtlich weiterer relevanter Grundrechte *Buchner*, in: Kühling/Buchner, 3. Aufl. 2020, Art. 1 Rn. 13 f.
[32] Siehe dazu etwa *Wolff*, in: BeckOK Datenschutzrecht, Stand 01.11.2021, Einl. Rn. 6 ff.
[33] BVerfGE 65, 1 (42).

2. The Overview of Personal Data Protection Law

① The Influence of other countries' legal systems

"Are there any countries that you have referred to as models in enacting your country's personal data protection law?"

Weltweit erkannten zuerst die deutschen Bundesländer die Notwendigkeit einer gesetzlichen Regelung moderner automatisierter Datenverarbeitung. So wurde am 30.09.1970 durch das Hessische Datenschutzgesetz der weltweite Grundstein des Datenschutzrechts gelegt.[34] Daran anschließend erließ auch das Land Rheinland-Pfalz im Jahr 1974 ein Landesdatenschutzgesetz, welches erstmalig neben der technischen Datensicherheit auch das persönliche Interesse des Einzelnen mitberücksichtigte.[35] Im Jahr 1977 wurde unter diesen Eindrücken das „Bundesgesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung" verabschiedet,[36] welches ähnlich der aktuellen Regelung den Datenschutz auf „alle personenbezogenen Daten" unabhängig ihrer Darstellungsform erstreckte.[37] Die Entwicklung des Datenschutzrechts fand somit weitestgehend seinen Ursprung in Deutschland und basiert somit zunächst in seiner Grundidee nicht auf den Erwägungen anderer Länder. Maßgeblich beeinflusst wurde das nationale Datenschutzrecht durch die im Laufe der Zeit zunehmende Europäisierung des Datenschutzrechts. Somit musste zuerst die Datenschutzrichtlinie (95/46/EG) in nationales Recht umgesetzt werden. Diese wurde nach mehr als 20 Jahren von der DSGVO abgelöst, welche aufgrund der nun erfolgten Ausgestaltung als Verordnung und nicht mehr als Richtlinie zugleich den primären Anknüpfungspunkt für nationales Datenschutzrecht darstellt (vgl. Art. 288 AEUV). Die nationalen Regelungen gerieten somit in den Hintergrund und regeln nur von der Verordnung nicht erfasstes bzw. durch Öffnungsklauseln zugänglich gemachte Bereiche. Soweit ersichtlich basiert auch die DSGVO nicht auf Erwägungen anderer Datenschutzgesetze. Umgekehrt steht die DSGVO etwas pointiert formuliert als grundrechtsfundiertes Modell den chinesischen und amerikanischen Regelungen gegenüber.[38]

[34] GVBl. I 1970, 625.
[35] GVBl. I 1974 S. 31.
[36] GVBl I 1977 S. 201.
[37] Vgl. dazu *Wolff/Brink*, in: BeckOK Datenschutzrecht, Stand 01.02.2022, Einleitung zur DSGVO Rn. 5.
[38] *Kühling/Raab*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Einl. Rn. 1.

② Definition and Scope of "personal data"

"Are cookies and other online identifiers included among personal data under the personal data protection law? What is the definition of personal data under the personal data protection law?"

a) *Definition of personal data under the personal data protection law*

Personenbezogene Daten sind gem. Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Die Definition in der JI-Richtlinie und dem sie umsetzenden § 46 BDSG sind identisch.

Die Legaldefinition des Art. 4 Nr. 1 DSGVO erfasst zu einem großen Teil auch die Fälle sog. „faktischer Anonymität",[39] in denen eine Person zwar nicht unbedingt identifiziert werden soll, aber (zumindest *ex post*) identifiziert werden kann; auch die DSGVO folgt insofern einem risikobasierten Ansatz. Umstritten ist allerdings, in welchem Umfang bei der Frage der Identifizierbarkeit „Zusatzwissen" zu berücksichtigen ist, mit dessen Hilfe eine Verbindung zwischen der Information und einer Person hergestellt werden kann. Eine (Minder-)Meinung im Schrifttum folgt dazu der Theorie des „absoluten Personenbezugs" und lässt es ausreichen, dass das zur Identifizierung erforderliche Zusatzwissen überhaupt irgendwo existiert.[40] Das überzeugt aber nicht, denn damit würden nahezu alle Daten einen Personenbezug aufweisen, während EG 26 Satz 5 DSGVO klar davon ausgeht, dass es auch anonyme Informationen gibt, die nicht dem Datenschutzrecht unterfallen. Auch der Zweck von Pseudonymisierung und Verschlüsselung, der gerade darin liegt, zwischen Inhabern des „Schlüssels" (i.w.S.) und der breiten Masse zu differenzieren, würde in Frage gestellt. Daher stellt die überwiegende Rechtsprechung darauf ab, über welche Möglichkeiten der für die Datenverarbeitung Verantwortliche verfügt.[41] Sie folgt damit der Theorie des relativen Personenbezugs, die darauf abstellt, ob gerade der Verantwortliche in der Lage ist, den Personenbezug herzustellen.[42] Diese

[39] *Hornung/Wagner*, CR 2019, 565, Rn. 7; vgl. auch EG 26 DSGVO.
[40] Zu den Theorien statt vieler *v. Lewinski/Rüpke/Eckhardt*, DaSR, 2. Aufl. 2022, § 10 Rn. 30.
[41] Dazu etwa BGH GRUR 2015, 192 (194).
[42] Zu den Theorien statt vieler *v. Lewinski/Rüpke/Eckhardt*, DaSR, 2. Aufl. 2022, § 10 Rn. 30. Für die relative Theorie bspw. *Brauneck*, EuZW 2019, 680 (683 f.); *Karg*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.),

Sichtweise führt dazu, dass dasselbe Datum für eine Person Personenbezug aufweisen kann, für eine andere dagegen nicht. Das überzeugt, gerade auch vor dem Hintergrund der auch in der DSGVO anerkannten Ziele von Pseudonymisierung und Verschlüsselung. Auch der für die Auslegung des europäischen Datenschutzrechts letztzuständige EuGH hat sich in der Rechtssache *Breyer*, in der es um den Personenbezug dynamischer IP-Adressen ging, (tendenziell) dieser Auffassung angeschlossen: Zwar hat er das Zusatzwissen Dritter mit einbezogen, wenn es zur Bestimmung der betreffenden Person (objektiv) eingesetzt werden kann,[43] allerdings hat er eine Identifizierbarkeit abgelehnt, wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar und damit das Identifizierungsrisiko de facto vernachlässigbar wäre,[44] und damit ein einzelfallbezogenes, bis zu einem gewissen Grad subjektives (da auf den konkreten Verantwortlichen bezogenes) Element hinzugefügt.[45]

b) Are cookies and other online identifiers included among personal data under the personal data protection law?

Regelmäßig lässt der Datensatz eines Cookies keinen Rückschluss auf die Person zu. Fügt die Person allerdings vor oder nach der Platzierung des Cookies weitere Identifikationsmerkmale hinzu, kann der Datensatz des Cookies mit den Identifikationsmerkmalen des Nutzers verbunden werden und stellt so ein personenbezogenes Datum dar.[46]

Die Einordnung einer dynamischen IP-Adresse als personenbezogenes Datum lässt sich ähnlich bewerten. Grundsätzlich weiß nur der Internetanbieter des jeweiligen Nutzers, welchem Nutzer er zu welcher Zeit welche IP-Adresse zugeordnet hat; für diesen ist also eine dynamische IP-Adresse immer ein personenbezogenes Datum.[47] Für alle anderen Akteure stellt sich die dynamische IP-Adresse wiederum nur dann als personenbezogenes Datum dar, wenn sie in Verbindung mit anderen Informationen die Identifikation der Person ermöglichen.[48]

Datenschutzrecht, 1. Aufl. 2019, Art. 4 Nr. 1 DSGVO Rn. 64. Ausdrücklich für diesen relativen Personenbezug jetzt auch EuG, Urt. v. 26.4.2023 - T-557/20 (SRB/EDSB), ECLI:EU:T:2023:219, Rn. 97 ff.

[43] EuGH, C-582/14, ECLI:EU:C:2016:779 – Breyer, Rn. 43.

[44] EuGH, C-582/14, ECLI:EU:C:2016:779 – Breyer, Rn. 46.

[45] Siehe zum Ganzen jüngst *Schröder*, DVBl. 2023, 794 (796).

[46] Dazu EuGH, Urt. v. 01.10.2019, C 673/17, ECLI:EU:C:2019:801 – Planet 49; *Klar/Kühling*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 4 Rn. 36.

[47] EuGH Urt. v. 24.11.2011 – C-70/10, ECLI:EU:C:2011:771 Rn. 51 – Scarlet Extended; *Klar/Kühling*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 4 Rn. 35.

[48] Personenbezug hinsichtlich eines Webseitenbetreibers, sofern diesem rechtlichen Mittel zustehen, Daten vom Internetzugangsanbieter heraus zu verlangen EuGH (2. Kammer), Urteil vom 19.10.2016 – C-582/14 (Breyer/Deutschland)

Unproblematisch ist die Einordnung als personenbezogenes Datum bei eindeutigen Identifizierungsmerkmalen, wie Klarnamen in einer E-Mail-Adresse.[49]

[49] *Klar/Kühling*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 4 Rn. 39.

③ The Rights of Data Subjects and the Obligations of those who process personal data

a) *The right to erase personal data (e.g., GDPR Article 17) or the right to utilization cease*

Die Regelung der Löschung personenbezogener Daten ist eines der zentralen Elemente einer interessengerechten Ausgestaltung des Datenschutzrechts. Art. 17 Abs. 1 DSGVO enthält sowohl eine Verpflichtung des Verantwortlichen zur Löschung von Daten als auch ein Recht der betroffenen Person, von dem Verantwortlichen die unverzügliche Löschung der ihn betreffenden personenbezogenen Daten zu verlangen.

Die Löschung hat – vorbehaltlich der Ausnahmen in Art. 17 Abs. 3 DSGVO, die ggf. eine Abwägung erfordern – zu erfolgen, wenn einer der in Art. 17 Abs. 1 DSGVO abschließend aufgezählten Gründe vorliegt: fehlende Notwendigkeit zur Zweckerreichung (lit. a), Widerruf der Einwilligung und Fehlen einer anderweitigen Rechtsgrundlage (lit. b), Widerspruch der betroffenen Person (lit. c), unrechtmäßige Datenverarbeitung (lit. d), Erfüllung einer Rechtspflicht (lit. e), Erhebung in Bezug auf Dienste der Informationsgesellschaft für Kinder (lit. f). Zur Abwägung mit den Ausnahmen existiert einige Rechtsprechung des EuGH[50] und der deutschen Gerichte.[51]

Das Recht auf Löschung wird schon in der Überschrift des Art. 17 DSGVO auch als „Recht auf Vergessenwerden“ bezeichnet. Art. 17 Abs. 2 DSGVO erinnert jedoch daran, dass insoweit technische Probleme bestehen: Einem vollständigen Vergessen steht gegebenenfalls nicht nur die Erinnerung der mit der Datenverarbeitung befassten natürlichen Personen entgegen, sondern auch die Veröffentlichung von Daten („Das Internet vergisst nichts“). Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gem. Art. 17 Abs. 1 DSGVO zur Löschung verpflichtet, trifft ihn gem. Art. 17 Abs. 2 DSGVO eine Informationspflicht an die für die Datenverarbeitung Verantwortlichen; das Ziel ist es, die Auffindbarkeit der Daten insbesondere in Suchmaschinen zu verhindern („De-Listing“). Aufgrund der Nichtrückholbarkeit veröffentlichter Daten stößt das Recht auf Löschung und somit zugleich das Recht auf Vergessen sowohl an rechtliche als auch an tatsächliche Grenzen.[52] Insoweit verkommt das Recht auf Löschung im Falle einer Veröffentlichung der personenbezogenen Daten zu einem stumpfen Schwert. Sind die Daten nicht veröffentlicht, sondern nur an einzelne Dritte übermittelt worden, greift Art. 19 DSGVO ein.

[50] Grundlegend EuGH, Urteil vom 13.5.2014, C-131/12 – Google und Google Spain; EuGH, Urteil vom 8.12.2022 – C-460/20 (TU)

[51] BVerfGE 152, 216 Rn. 141; BGH, NJW 2020, 1595; BGH, NJW 2020, 3444.

[52] So auch *Dix*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 17 Rn. 21. Zur territorialen Reichweite des De-Listings siehe EuGH, 24.9.2019 – C-507/17, BeckRS 2019, 22051.

Neben dem Recht auf Löschung wird dem Betroffenen gem. Art. 18 DSGVO auch der Anspruch auf Einschränkung der Verarbeitung zuteil. Dabei sollen die Daten zwar nicht gelöscht werden, sie sollen aber auch nicht mehr anderweitig verarbeitet werden dürfen („freezing"). Die von der Einschränkung betroffenen Dateien sind im Sinne des Art. 4 Nr. 3 DSGVO zu markieren. Die Einschränkung der Verarbeitung als Minus zur Löschung wird etwa dann relevant, wenn der Löschung das Interesse der betroffenen Person entgegensteht (Abs. 1 lit. b, c), oder wenn die Überprüfung von Löschungsansprüchen eine gewisse Zeit erfordert (Abs. 1 lit a und d).[53]

b) The Status and Significance of Consent in Personal Data Protection Law (opt-in or opt-out?):

When is the consent of the individual required under the personal data protection law? Whether a business is required to obtain the consent of the individual (data subject) when acquiring personal data? When personal data is provided to a third party, is the consent of the individual required to be obtained?

aa) Significance of Consent

Die Bedeutung der Einwilligung, definiert als jede von der betroffenen Person freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (Art. 4 Nr. 11 DSGVO), könnte in der DSGVO größer nicht sein. [54] Die Einwilligung als Erlaubnistatbestand einer rechtmäßigen Datenverarbeitung gem. Art. 6 Abs. 1 Nr. 1 DSGVO ist nicht nur der zentrale Wirkmechanismus für die Gestattung der Datenverarbeitung, sondern zugleich auch der positive Ausdruck informationeller Selbstbestimmung der betroffenen Person durch die Entscheidungsmöglichkeit, „ob" und „wie" die personenbezogenen Daten verarbeitet werden dürfen.[55] Daneben trägt die Einwilligung aber nicht nur der Sicherung der grundrechtlichen Position des Betroffenen Rechnung, sondern gewährleistet auch aufgrund der umfangreichen Anforderungen hinsichtlich Bestimmtheit und Ausdrücklichkeit [56] die notwendige Rechtssicherheit für die Datenverarbeiter.

[53] So etwa *Herbst*, in: Kühling/Buchner, 3. Aufl. 2020, Art. 18 Rn. 1.
[54] Mit ähnlichem Urteil *Albrecht*: „entscheidender Grundpfeiler des Datenschutzes", CR 2016, 88 (91).
[55] *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253 (258); *Buchner/Petri*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 6 Rn. 17.
[56] *Buchner/Petri*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 6 Rn. 18 f.

Gemäß Art. 4 Nr. 11 DSGVO kann die Einwilligung (solange es nicht um sensible Daten geht, Art. 9 Abs. 2 lit. a) DSGVO) nicht nur ausdrücklich, sondern auch konkludent erfolgen. Auch konkludentes Handeln muss aber durch aktives Tun erfolgen (und auf die Einwilligung gerichtet sein).[57] Daraus wird die Schlussfolgerung gezogen, dass die betroffene Person beim Aufrufen einer Website aktiv in Form einer „Opt In-Erklärung" seine Einwilligung zur Verarbeitung personenbezogener Daten (insbes. Cookies) erteilen muss,[58] die bloße Untätigkeit (Nicht-opt out) reicht – im Gegensatz zur Rechtslage vor Inkrafttreten der DSGVO[59] – nicht mehr aus. Hintergrund ist nach der Rechtsprechung des EuGH, dass nicht ausgeschlossen werden kann, dass das Einwilligungsersuchen schlicht übersehen wurde;[60] das mag in Fällen, in denen beispielsweise jemand nach der Information über Fotoaufnahmen bei einer Veranstaltung anwesend bleibt, anders sein. Bei der Verarbeitung von sensitiven Daten ordnet Art. 9 Abs. 2 lit. a) DSGVO eine ausdrückliche Einwilligung an.

bb) When is the consent of the individual required under the personal data protection law?

Der Systematik des Art. 6 Abs. 1 S. 1 DSGVO folgend, stellt die Einwilligung einen von mehreren Erlaubnistatbeständen für eine rechtmäßige Verarbeitung personenbezogener Daten dar. Grundsätzlich bedarf es also jedenfalls der Einwilligung, wenn die Verarbeitung der personenbezogenen Daten nicht zur Erfüllung eines Vertrages mit der betroffenen Person (lit. b Alt. 1), oder zur Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person erforderlich ist (lit. b Alt. 2), oder der Erfüllung einer rechtlichen Verpflichtung (lit. c), dem Schutz lebenswichtiger Interessen (lit. d), der Wahrnehmung einer Aufgabe dient (lit. e), oder im überwiegenden Interesse des Verantwortlichen oder Dritter steht (lit. f.). Entgegen der systematischen Darstellung wird teils erwogen,[61] der Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. 1 DSGVO, aufgrund dessen, dass es sich dabei um ein milderes Mittel handele,[62] einen Vorrang gegenüber den vorgenannten Erlaubnistatbeständen einzuräumen.[63]

[57] EuGH, Urt. v. 01.10.2019, C 673/17, ECLI:EU:C:2019:801 – Planet 49, Rn. 52.
[58] ErwGr. 32 DSGVO; EuGH, Urt. v. 01.10.2019, C 673/17, ECLI:EU:C:2019:801 – Planet 49, Rn. 54 ff.
[59] Vgl. etwa BGH, NJW 2010, 864.
[60] EuGH, Urt. v. 01.10.2019, C 673/17, ECLI:EU:C:2019:801 – Planet 49, Rn. 55.
[61] Aufgrund dessen den pauschalen Vorrang auch ausschließend *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 7 Rn. 16; *Schulz*, in: Gola/Heckmann, DSGVO, 3. Aufl. 2022, Art. 6 Rn. 10.
[62] Vgl. *Schantz*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 6 Rn. 11.
[63] Ausdrücklich *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253 (258).

cc) Whether a business is required to obtain the consent of the individual (data subject) when acquiring personal data?

Wie ausgeführt braucht ein Unternehmen nicht zwingend die Zustimmung des Betroffenen, um dessen personenbezogenen Daten zu erlangen, soweit einer der sonstigen Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO vorliegt. Regelmäßig wird in Fällen einer Datenverarbeitung durch ein Unternehmen der Erlaubnistatbestand des Art. 6 Abs. 1 S. 1 lit. b) DSGVO in Frage kommen, je nach Konstellation kann auch Art. 6 Abs. 1 S. 1 lit. f) DSGVO relevant sein, etwa bei der Verarbeitung öffentlich zugänglicher Daten im Internet.

Obwohl mitunter empfohlen wird, wegen der teilweise vertretenen Auffassung des pauschalen Vorrangs der Einwilligung und zu Beweisgründen, etwa bei der Durchführung von vorvertraglichen Maßnahmen sicherheitshalber eine Einwilligung einzuholen, ist dies nicht unproblematisch, weil die Einwilligung gemäß Art. 7 Abs. 3 DSGVO jederzeit widerruflich ist und es dann doch einer anderen Rechtsgrundlage für die Verarbeitung bedarf.

dd) When personal data is provided to a third party, is the consent of the individual required to be obtained?

Jeder einzelne Datenverarbeitungsvorgang bedarf einer Rechtsgrundlage. Das bedeutet, dass sowohl derjenige, der die Daten weitergibt, als auch der Empfänger eine Rechtsgrundlage für die Datenverarbeitung benötigen; insoweit spricht man auch vom „Doppeltürmodell“,[64] dies meint, dass sowohl für die Datenübermittlung als auch für den Empfang und die Weiterverarbeitung eine Rechtsgrundlage notwendig ist. Eine Einwilligung kann sich grundsätzlich auf beides beziehen. Zu beachten ist aber, dass sie jeweils nur für den „bestimmten Fall“ (Art. 4 Nr. 11) erfolgt. Dies umfasst nicht nur die betroffenen personenbezogenen Daten (Art. 4 Nr. 1), sondern auch den Verantwortlichen (Art. 4 Nr. 7) und etwaige weitere Datenempfänger (Art. 4 Nr. 9). Willigt der Betroffene also explizit in eine Weitergabe an und in die Verarbeitung durch Dritte ein, bedarf es keiner erneuten Einwilligung;[65] umgekehrt ist eine Weitergabe an Dritte etwa von einer konkludenten Einwilligung regelmäßig nicht erfasst.[66] Einer Einwilligung bei der Datenübermittlung an Dritte bedarf es auch nicht, wenn diese gesetzlich vorgeschrieben ist (Art. 6 Abs. 1 lit. c DSGVO); etwa bei einer behördlichen Anordnung zur Offenlegung der personenbezogenen

[64] BVerfGE 141, 220 Rn. 305.
[65] Vgl. dazu *Klement*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019 Art. 7 Rn. 68.
[66] *Frenzel*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 6 Rn. 11.

Daten.[67] Auch im Falle des Art. 6 Abs. 1 lit. b DSGVO kann eine Einwilligung entbehrlich sein, da die Norm insoweit keine Aussage zum Vertragspartner der betroffenen Person trifft. Neben dem Wortlaut des Art. 6 Abs. 1 lit. b DSGVO legt dieses Ergebnis auch ein systematischer Vergleich zu Art. 49 Abs. 1 lit. b DSGVO nahe.[68] Schließlich kann auch ein berechtigtes Interesse zur Weitergabe bestehen, Art. 6 Abs. 1 lit. f DSGVO. Auch hier ist zu beachten, dass sich die Rechtsgrundlage jeweils auf alle Verarbeitungsvorgänge beziehen muss.

c) The Limit of the Notice and Consent model and the countermeasure:
Daniel J. Solove, an authority on privacy law, points out the limitations of the privacy self-management model in data protection law as follows; "[The U.S. privacy laws] provide[s] people with a set of rights to enable them to make decisions about how to manage their data. These rights consist primarily of rights to notice, access, and consent regarding the collection, use, and disclosure of personal data. The goal of this bundle of rights is to provide people with control over their personal data. ...As empirical and social science research demonstrates, cognitive problems impair individuals' ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data."

Thus, if there are limits to the self-management model in terms of the limitations of human cognitive abilities, how does your country's personal data protection law address these challenges? For example, is an effective notice required for businesses?

Die informationelle Selbstbestimmung verwirklicht sich nach deutschem Verständnis in abgestufter Form: Die höchste, bzw. beste Stufe ist die Einwilligung in eine Datenverarbeitung. Hier wird „selbst bestimmt", ob ein Dritter Daten verarbeiten darf. Basiert die Datenverarbeitung auf einer anderen Grundlage, tritt diese Form der Selbstbestimmung in den Hintergrund oder wird, wenn die Verarbeitung gegen den Willen der betroffenen Person erfolgt, sogar ignoriert. In diesen Fällen gewinnt ein anderer Aspekt der Selbstbestimmung an Bedeutung: Der Einzelne soll wissen, wer was bei welcher Gelegenheit über ihn weiß.[69]

Diese Idee ist auch in der DSGVO verwirklicht. Die in Art. 13 DSGVO geregelte Hinweispflicht ist in der Zusammenschau mit Art. 14, 15 DSGVO das Fundament für faire und transparente Verarbeitung von personenbezogenen Daten (vgl. Art. 5 Abs. 1 lit. a DSGVO: Transparenz); dies bringt bereits Art. 13 Abs. 2 DSGVO zum Ausdruck. Ziel der

[67] Dazu und auch hinsichtlich der Gegenansichten dieser Auffassung *Buchner/Petri*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 6 Rn. 78.
[68] Dazu *Schantz*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 6 Rn. 22.
[69] BVerfGE 65, 1 Rn. 146.

Hinweispflichten ist es, die betroffene Person zum einen über den Verarbeitungsvorgang zu unterrichten und daneben auch über weitere zusammenhängende Absichten und Rechtsfolgen aufzuklären.[70] Die in den Art. 13 ff. DSGVO geregelten Hinweispflichten erhalten durch Art. 12 DSGVO grundsätzliche Rahmenregelungen; so müssen die Mitteilungen präzise, transparent, verständlich und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden. Somit wird zumindest theoretisch der betroffenen Person auf möglichst einfache und zugängliche Art und Weise eine Übersicht verschafft, wer welche Daten und zu welchem Zweck hat. Zusätzlich zu diesen Informationen wird der Betroffene gem. Art. 13 Abs. 2 DSGVO unter anderem auch über seine Rechte zur Löschung und Beschwerde etc. aufgeklärt. Die Hinweispflicht gepaart mit den Rechten auf Auskunft, Löschung und Widerruf der Einwilligung stellt jedenfalls theoretisch einen ausreichenden Umfang an Transparenz und Rechtsschutzmöglichkeit für den Betroffenen dar. Die Hinweispflicht gem. Art. 13 DSGVO ist auch nicht dispositiv, sondern unterliegt lediglich den Öffnungsklausen des Art. 23, Art. 85 und Art. 88 DSGVO.[71]

Die größte Schwäche der Hinweispflicht ist das mangelnde Fachverständnis der Betroffenen und/oder das schlichte Desinteresse. Die nach Art. 13, 14 DSGVO mitzuteilende Informationen sind regelmäßig so umfangreich,[72] dass viele Betroffene die dafür nötige Zeit nicht aufbringen wollen oder können und sich so mit einem niedrigen Datenschutzniveau abfinden.[73] Umgekehrt sorgen sich viele Betroffene im großen Umfang um ein angemessenes Datenschutzniveau; in diesem Kontext spricht man häufig von dem „Privacy Paradox".[74] Neben dem bereits zuvor benannten Art. 12 DSGVO wird versucht dem Problem auch in Art. 7 Abs. 2 DSGVO zu begegnen. Dieser sieht vor, dass die Einwilligung zwar grundsätzlich Teil eines komplexen Gesamtgeschäfts sein darf, allerdings im Vergleich zu den anderen Regelung nicht in den Hintergrund geraten darf; mithin also leicht zugänglich und von den anderen Regelungen unterscheidbar sein muss.[75] An dem faktischen Problem der kognitiven Überladung der Betroffenen[76] ändert dies wohl trotzdem nichts. Immerhin möchte Art. 12 Abs. 7 DSGVO die informationelle Selbstbestimmung verbessern, indem er z.B. Piktogramme zur Erleichterung des Verständnisses der Informationen vorsieht. Trotzdem gelingt es dem geltenden

[70] *Paal/Hennemann*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 13 Rn. 4
[71] *Schmidt-Wudy*, in: BeckOK Datenschutz, Stand 01.05.2023, Art. 13, zur Dispositivität Rn. 33, zu den Öffnungsklauseln Rn. 8 f.
[72] Dazu umfassend *Ebner*, Weniger ist Mehr?, S. 104 ff.
[73] So *Ebner*, Weniger ist Mehr?, S. 44; *Pollmann/Kipker*, DuD 2016, 378.
[74] Dazu etwa *Specht*, in: Specht/Mantz (Hrsg.), 2019 § 9 Rn. 6.
[75] *Klement*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 7 Rn. 75.
[76] Dazu *Van Ooijen/Vrabec*, Journal of Consumer Policy 2019, 91 (95).

Datenschutzrecht nicht, das Problem zufriedenstellend zu lösen. Dementsprechend finden sich in der Literatur erste Vorschläge einer Änderung.[77]

Hinzu kommt, dass die Transparenzverpflichtungen eine gewisse Durchsetzungsschwäche aufweisen. Zwar können Verstöße gegen die Hinweispflicht gem. Art. 83 Abs. 5 lit. b DSGVO mit einer Geldbuße sanktioniert werden. Jenseits dessen ist aber unklar, ob es sich bei der Hinweispflicht um eine Ordnungsvorschrift oder um eine Rechtmäßigkeitsvoraussetzung für die Datenverarbeitung handelt.[78] Überwiegend wird davon ausgegangen, dass ein Verstoß gegen den Art. 13 DSGVO nicht pauschal zur Rechtswidrigkeit der gesamten Verarbeitung führt.[79] So wird insbesondere die Vorabinformation bei der Einwilligung getrennt von der im Rahmen der Datenerhebung mitzuteilenden Information betrachtet.[80] Erfolgt das Einwilligungsersuchen mit den Hinweisen zusammen, kann ein Fehler aber zur Unwirksamkeit der Einwilligung führen. Die potentielle Irrelevanz eines Verstoßes gegen die Hinweispflicht für die Rechtswidrigkeit der Datenverarbeitung schwächt insoweit auch den der Hinweispflicht zugedachten Schutzeffekt.[81]

d) How are devices or architectures such as a Personal Data Store (PDS) being utilized to assist with the person's controllability of their personal data?

Zur Vermeidung des unreflektierten Akzeptierens von Cookies („Cookie-Click-Fatigue“) hat der deutsche Gesetzgeber in § 26 Abs. 2 Nr. 3 lit. b) TTDSG erstmalig eine Regelung zu Personal Management Information Systems (PIMS) verabschiedet. Dies soll den Nutzern ermöglichen, durch ein voreingestelltes System, welches die Abfragemaske automatisch ausfüllt, Websites aufrufen zu können, ohne von einem Cookie-Banner belangt zu werden.[82] Durch die standardisierte Ausfüllung der Abfragen könnte man allerdings die für eine Einwilligung notwendige Zweckbestimmung insoweit als problematisch ansehen, als der Betroffene nicht individuell für den jeweiligen Zweck der Verarbeitung einwilligt. Allerdings ist dies im analogen Fall einer Stellvertretung auch nicht zwingend der Fall, vgl. dazu Art. 8 DSGVO.

---

[77] Einen Vorschlag unterbreitend *Ebner*, Weniger ist Mehr?, S. 314 ff.

[78] *Bäcker*, in: Kühling/Buchner, DSGVO, Art. 12 Rn. 13, 18, 27, Art. 13 RN. 61 ff., 80 ff.; *Schantz*, in: Schantz/Wolff, DatenschutzR, 2017, Rn. 1176; *Paal/Hennemann*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 13 Rn. 9a.

[79] *Paal/Hennemann*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 13 Rn. 9a. mwN.

[80] So *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 12 Rn. 5; a.A. *Bäcker*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 13 Rn. 66.

[81] Dazu *Bäcker*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 13 Rn. 61 ff.; ebenso *Dix*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 13 Rn. 26.

[82] Dazu *Kühling/Sauerborn*, ZD 2022, S. 596 f.

Insoweit erhalten Systeme wie das PIMS Einzug in die nationalen Datenschutzregelungen, allerdings ist noch nicht geklärt, ob und wie sich mit ihnen die Anforderungen des europäischen Datenschutzrechts erfüllen lassen.

e) Profiling regulations. E.g., the right to object to profiling (GDPR Article 21).

Der DSGVO liegt ausweislich des Art. 4 Nr. 4 ein weites Verständnis des Terminus „Profiling" zugrunde. Darunter wird jede Art der automatisierten Verarbeitung personenbezogener Daten verstanden, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Das Profiling stellt also eine besondere Art der Datenverarbeitung dar. Die DSGVO adressiert sie vor allem in zwei Bestimmungen: Im Widerspruchsrecht des Art. 21 und in den Anforderungen an automatisierte Entscheidungen in Art. 22.

Art. 21 DSGVO normiert ein Widerspruchsrecht für Datenverarbeitungen, die auf Art. 6 Abs. 1 lit. e) oder f) DSGVO gestützt sind. Dieses setzt im Regelfall Gründe voraus, die sich aus der besonderen Situation der betroffenen Person ergeben (Abs. 1 S. 1), im Fall der Direktwerbung ist der Widerspruch auch ohne solche Gründe, also voraussetzungslos möglich (Abs. 2). Beide Absätze erwähnen ausdrücklich, dass das Widerspruchsrecht auch für Profiling gilt. Insoweit handelt es sich allerdings nur um eine deklaratorische Ausführung, da das Profiling auch ohne den Zusatz von Art. 21 DSGVO erfasst wäre.[83] Die eigentlich redundante Ausführung ist wohl als Klarstellung der Erstreckung des Widerspruchsrechts auf den für die Persönlichkeitsrechte sehr sensiblen Fall des Profilings zu begreifen.[84]

Wichtiger ist Art. 22 DSGVO. Dieser räumt betroffenen Personen in Abs. 1 ein Recht ein, nicht einer ausschließlich auf einer automatisierten Verarbeitung basierenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. In der Vorschrift wird dabei explizit das Profiling als der wichtigste Fall[85] automatisierter Entscheidungsfindung hervorgehoben. Als bekanntes Beispiel für Profiling dienen Scoring-Verfahren, welche beispielsweise bei der Kreditvergabe zur

[83] Statt vieler *Caspar*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 21 Rn. 15.
[84] *Martini*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 21 Rn. 17.
[85] Diese Einschätzung teilend *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Aufl. 2019, Art. 22 Rn. 20.

Anwendung kommen. Ziel der Vorschrift ist es, rechtserhebliche Entscheidung nicht nur auf automatisierte Verarbeitungsprozesse zu stützen, sondern einer individuellen Kontrollinstanz durch einen Menschen zuzuführen.[86] Folglich soll also verhindert werden, dass der Betroffene zum bloßen Objekt einer algorithmenbasierten Bewertung persönlicher Daten wird.[87] Dass die DSGVO dem Vorgang des Profilings ein erhebliches Gefahrenpotential unterstellt, belegt auch Pflicht der Datenschutz-Folgenabschätzung, vgl. Art. 35 Abs. 1, 3 lit. a) DSGVO.

Allerdings wird die zunächst strenge Regelung des Art. 22 Abs. 1 DSGVO durch verschiedene Ausnahmetatbestände in Art. 22 Abs. 2 DSGVO aufgeweicht. Teile der Literatur sehen diese sogar als so umfassend, dass sie im Kontext des Art. 22 DSGVO nicht mehr von einem Verbot der automatisierten Einzelfallentscheidung sprechen.[88]

f) The right to data portability or the right to transmit personal data (e.g., GDPR Article 20) And in what situations are these rights implemented in practice?

Art. 20 DSGVO regelt das Recht auf Datenübertragbarkeit. Darin wird der betroffenen Person das Recht eingeräumt, die sie betreffenden personenbezogenen Daten, welche sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen zur Verfügung zu stellen. Einzige Voraussetzung dafür ist, dass die Verarbeitung auf einer Einwilligung gem. Art. 6 Abs. 1 lit. a) DSGVO oder Art. 9 Abs. 2 lit. a) DSGVO oder auf einem Vertrag gem. Art 6 Abs. 1 lit. b) DSGVO beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Durch diesen Anspruch wird versucht, einen Ausgleich zwischen der Marktmacht und der informationellen Selbstbestimmung herzustellen.[89] In den Erwägungsgründen wird der Datenportabilität die Ermöglichung bzw. Erleichterung des Anbieterwechsels zugeschrieben, als Beispiel wird die Übertragung von einem sozialen Netzwerk auf ein anderes genannt.[90] In der Literatur wird der Anwendungsbereich des Art. 20 DSGVO dabei unterschiedlich weit verstanden, so wird teils auch der Wechsel des Cloudspeicher-Anbieters bei großen Datenmengen als Anwendungsfall des Art. 20 Abs. 2 DSGVO angeführt.[91] Im Ergebnis soll letztlich die Abwanderung zu einem

[86] *Scholz*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 22 Rn. 3.
[87] *Martini*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Rn. 1.
[88] *Franzen*, in: Franzen/Gallner/Oetker, EuArbRK, 4. Aufl. 2022, Art. 22 Rn. 3.
[89] Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 8./9.10.2014, in: BBDI, Dokumente zu Datenschutz und Informationsfreiheit 2014, S. 23 f.
[90] ErwGr. 55.
[91] *Schantz*, NJW 2016, 1841 (1845).

anderen Anbieter erleichtert werden, insoweit kommen der Regelung also in erster Linie wettbewerbspolitische bzw. allgemein verbraucherschützende Ziele zu.[92]

[92] *Herbst*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 20 Rn. 4; *Schantz*, NJW 2016, 1841 (1845); *Kühling/Martini*, EuZW 2016, 448 (450).

③ Organization and authority of the supervisory body enforcing personal data protection law. Sanctions and complaint mechanisms.

a) Organization and authority

Neben der internen Kontrolle „im Hause“ des Verantwortlichen durch dessen Datenschutzbeauftragten (Art. 37-39 DSGVO) besteht eine externe Kontrolle durch unabhängige [93] Datenschutzaufsichtsbehörden. Diese hat im deutschen Datenschutzrecht Tradition seit dem Hessischen Datenschutzgesetz (die Aufsicht über öffentliche Stellen konnte nicht durch diese selbst erfolgen) und ist heute sowohl in Art. 8 Abs. 2 EuGRCh als auch in Art. 16 Abs. 2 AEUV verankert.

Auf europäischer Ebene wird die Aufsicht (über Stellen der EU) durch den Europäischen Datenschutzbeauftragten wahrgenommen, [94] außerdem besteht der Europäische Datenschutzausschuss (EDSA), dem eine zentrale Rolle im europäischen Verwaltungsverbund der Datenschutzaufsichtsbehörden zukommt (Art. 70 Abs. 1 S. 1 DSGVO, Art. 51 JI-RL). Primär zuständig sind aber für die Aufsicht – sowohl über öffentliche Stellen als auch über nichtöffentliche Stellen – die Datenschutzaufsichtsbehörden der Mitgliedstaaten, vgl. Art. 51 DSGVO. Die mitgliedstaatlichen Aufsichtsbehörden wird gem. Art. 52 DSGVO völlige Unabhängigkeit bei der Erfüllung ihrer Aufgaben eingeräumt. Art. 53 DSGVO regelt daneben die verfahrensrechtlichen als auch persönlichen Anforderungen an die Mitglieder der Aufsichtsbehörden.

Aufgrund des föderalen Systems der Bundesrepublik Deutschland wird die Verwaltungstätigkeit in weiten Teilen in und durch die Bundesländer ausgeübt. Dies zeigt sich auch im Datenschutzrecht. Das Bundesdatenschutzgesetz (BDSG) weist dem „Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“ (BfDI) primär die Aufsicht über die öffentlichen Stellen des Bundes zu (§§ 8 ff. BDSG). Die Aufsicht über öffentliche Stellen der Länder sowie über nichtöffentliche Stellen (also Unternehmen, Vereine, …) liegt bei den Bundesländern (§ 40 BDSG i.V.m. den Landesdatenschutzgesetzen).

[93] Dazu EuGH, Urteil vom 9. März 2010, Rs. C-518/07 – Kommission/Deutschland.

[94] Der europäische Datenschutzbeauftragte ist in erster Linie, ähnlich den Aufgaben des herkömmlichen Datenschutzbeauftragten, dafür zuständig, die Einhaltung des Datenschutzes innerhalb der EU-Verwaltung und der EU-Organe zu überwachen, Art. 41 Abs. 2 VO (EG) 45/2001. Neben sonstigen Aufgaben, wie die Beratung der Organe der EU (Art. 41 Abs. 2 iVm. Art. 46 lit. d VO 45/2001), oder der Bearbeitung von Beschwerden (Art. 46 lit. a VO 45/2001), ist der Europäische Datenschutzbeauftragte Mitglied im Europäischen Datenschutzausschuss, Art. 68 Abs. 3 DSGVO, grundsätzlich v. Lewinski/Rüpke/Eckhardt, DaSR, 2. Aufl. 2022, S. 353 ff.

Bereichsspezifische Ausnahmen bestehen für Gerichte, Kirchen und Religionsgemeinschaften und für Medien.[95]

Dementsprechend liegt ein Großteil der externen Kontrolle bei den Landesbehörden. Zwangsläufig geht mit dieser Aufgliederung eine gewisse uneinheitliche Handhabung einher, welche dadurch verstärkt wird, dass durch die Länder nicht nur die DSGVO und punktuell Bundesrecht vollziehen, sondern auch landesrechtliche Datenschutzregelungen. Als Gegenmittel fungiert die (informelle) „Datenschutzkonferenz" (DSK), in der die deutschen Datenschutzbehörden beispielsweise abgestimmte Stellungnahmen und Handlungsempfehlungen verabschieden.

Daneben verbleibt nur noch ein verhältnismäßig kleiner Aufgabenbereich für den BfDI.[96] Gleichwohl kommt dem BfDI die Vertretung im Europäischen Datenschutzausschuss zu, was vor dem Hintergrund des geringen Einflusses in nationaler Hinsicht zumindest als fragwürdig anmutet, regelungstechnisch und vor dem Hintergrund des Föderalismus aber naheliegend ist.

Die Zuständigkeit der Behörden ergibt sich aus Art. 55 Abs. 1 DSGVO: Grundsätzlich ist jede Behörde für den Datenschutz in ihrem Mitgliedstaat zuständig. Angesichts des Anwendungsbereichs der DSGVO und zahlreicher grenzüberschreitender Sachverhalte würde dies häufig zu Mehrfachzuständigkeiten führen; Verantwortliche müssten sich mit zahlreichen Datenschutzbehörden auseinandersetzen und es bestünde die Gefahr widersprüchlicher Entscheidungen. Daher etabliert Art. 56 DSGVO das Prinzip des „one stop shop" – hat ein Verantwortlicher eine Hauptniederlassung in einem Mitgliedstaat, ist dessen Aufsichtsbehörde federführend zuständig; die Mitwirkung andere Behörden erfolgt im Rahmen des europäischen Verwaltungsverbunds im Hintergrund, wo ggf. auch der EDSA im sog. Kohärenzverfahren (Art. 60, 63 ff. DSGVO) beteiligt wird.

Die Befugnisse der Datenschutzaufsichtsbehörden ergeben sich unmittelbar aus der DSGVO (Art. 58 DSGVO).

b) Sanctions and complaint mechanisms

Als Sanktion bei Verstößen gegen die DSGVO sieht diese selbst einen Bußgeldkatalog vor (Art. 83 Abs. 3-6 DSGVO) und verweist für potentiell weitere Sanktionen in Art. 84 DSGVO auf die Mitgliedstaaten. Die Bußgeldtatbestände des Art. 83 DSGVO lassen sich dabei grob in vier Kategorien einteilen: 1. Verstöße gegen Pflichten der Verantwortlichen bzw. der

[95] Ausführlicher v. Lewinski/Rüpke/Eckhardt, DaSR, 2. Aufl. 2022, S. 357 ff.
[96] Dazu etwa *Heil*, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, 2017, § 5.1 Rn. 45 ff.

Auftragsverarbeiter, 2. Verstöße gegen Pflichten der Zertifizierungs- und Überwachungsstellen, 3. Verstöße im Rahmen der konkreten Verarbeitung und 4. Behinderung der Aufsichtsbehörden.[97] Dabei können Bußgelder in Höhe von 20 000 000 Euro oder im Fall eines Unternehmens bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vor gegangenen Geschäftsjahres verhängt werden.

Die vorgenannten Sanktionen werden in nationaler Hinsicht durch die Regelung des § 43 BDSG flankiert, wobei es sich dabei wohl um keine Regelung im Sinne des Art. 84 DSGVO handelt.[98] Diese Ordnungswidrigkeit kann mit einer Geldbuße von bis zu 50 000 Euro geahndet werden, bleibt also im Umfang auch hinter der europäischen Regelung zurück.

Sowohl die DSK als auch der EDSA haben inzwischen Leitlinien für die Höhe der Bußgelder verabschiedet.[99]

Gemäß Art. 77 DSGVO hat jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde. Gemäß Art. 78 DSGVO hat zudem jede natürliche oder juristische Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde. Das gilt sowohl in dem Fall, dass die Aufsichtsbehörde belastende Maßnahmen gegen den Verantwortlichen oder Auftragsverarbeiter verhängt, als auch in dem Fall, dass die Behörde nicht auf die Beschwerde nach Art. 77 DSGVO reagiert.

[97] V. Lewinski/Rüpke/Eckhardt, DaSR, 2. Aufl. 2022, § 24 Rn. 25 ff.
[98] V. Lewinski/Rüpke/Eckhardt, DaSR, 2. Aufl. 2022, § 24 Rn. 36.
[99] Guidelines 04/2022 on the calculation of administrative fines under the GDPR (https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en); Bußgeldkonzept der DSK (https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf).

④ Judicial proceedings or judicial remedy (standing to sue. class action.)

Art. 79 DSGVO ergänzt den (ggf. gerichtlich eingeforderten) Schutz der betroffenen Personen durch Maßnahmen der Aufsichtsbehörden (Art. 77, 78 DSGVO) um einen Rechtsbehelf direkt gegen Verantwortliche und Auftragsverarbeiter. Grundsätzlich ist der Rechtsschutz bzw. die Gerichtsbarkeit im Datenschutzrecht abhängig vom jeweils zugrundeliegenden Rechtsverhältnis. So ist etwa das Verwaltungsgericht zuständig bei einer Unterlassungsklage gegen die Videoüberwachung eines öffentlichen Platzes.[100] Macht hingegen ein Betroffener seinem Anspruch auf Löschung seiner personenbezogenen Daten gegen eine private juristische oder natürliche Person geltend, ist die Zivilgerichtsbarkeit zuständig.[101] Handelt es sich um Arbeitnehmerdatenschutz, so eröffnet § 2 Abs. 1 ArbGG den Rechtsweg zu den Arbeitsgerichten[102] bzw. liegt die Verarbeitung von Sozialdaten dem Rechtsstreit zugrunde, dient § 51 SGG als Verweisung zur Sozialgerichtsbarkeit.[103]

Art. 80 Abs. 2 DSGVO ermöglicht es den Mitgliedstaaten, den in Art. 80 Abs. 1 DSGVO genannten Einrichtungen, Organisationen oder Vereinigungen ein Verbandsklagerecht einzuräumen. Dieses muss, auch wenn es ohne ein Zutun eines Betroffenen möglich ist, die Verletzung einer betroffenen Person gemäß der DSGVO infolge einer Verarbeitung zum Gegenstand haben. Ein Datenschutzverbandsklagerecht als Bestandteil der BDSG gibt es aktuell nicht. Allerdings wurde das verbraucher- bzw. wettbewerbsrechtliche UklaG auf bestimmte datenschutzrechtliche Sachverhalte erweitert.[104]

Gemäß Art. 82 hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller[105] Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Auch dieser ist vor den Gerichten der Mitgliedstaaten einzuklagen.

[100] VG Regensburg, ZD 2020, 601.
[101] Vgl. etwa OLG Bamberg, CR 2006, 274 f.
[102] BAG, CR 1987, 370.
[103] BSGE 130, 132.
[104] *V. Lewinski*, in: Auernhammer, DSGVO, 7. Aufl. 2020, Art. 80 Rn. 23.
[105] Dazu jetzt EuGH, Urt. v. 4.5.2023, Rs. C-300/21 – Österreichische Post, ECLI:EU:C:2023:370.

We have an additional question related to the question ③ (c) in Question List.

Article 9 (2) (g) of GDPR provides that “the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person [and] data concerning health” are permitted if “ [such a] processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject”.

We have a question about the relationship between this provision and the utilization of health data for research purposes.

Is the consent of the patient required for the use of his/her medical record or biometric data for research purposes or drug development? What legal obligations, other than consent, do research institutions have when collecting and utilizing patient health data for research purposes?

And we would like to know about a recent development in European Health Data Space (EHDP).

Regarding your questions concerning the use of health data for research purposes (3), the situation is as follows:

First, it should be noted that the GDPR contains a "privilege" for research purposes (Article 89). However, this does not mean that data processing for research purposes is exempt from the GDPR. In fact, the GDPR applies, as can be read in Article 89 (1) GDPR, but in accordance with EU or MS law some rights may not apply, Article 89 (2).

Article 5 (2) GDPR states that research pursposes are not incompatible with other purposes. This provision is related to Article 6 (4) GDPR, according to which the original purpose may be amended if the purpose is not incompatible. The interpretation of the latter provision is controversial: A few scholars think that a change of purpose is possible without any other prerequisites, but the overwhelming opinion is that the controller still needs a legal basis according to article 6 (1) GDPR.

With regard to health data, Article 9 GDPR applies, which, in its paragraph 1, prohibits the processing of health data (also for research purposes), but there are numerous exceptions in Article 9 (2) GDPR:

One way to use a medical record or biometric data for research purposes or drug development would be consent (lit. a). If I understand your question correctly, you want to know if any of the other litera in Article 9 (2) can be used as a basis for processing a medical record or biometric data for research purposes or drug development, in particular lit. g, if there is no consent.

In my view, four provisions need to be considered in this regard:

As you mention, Art. 9 (2) (g) GDPR could apply. Public interest is understood to mean an interest that affects the entire population or at least large parts of it. This includes, for example, processing for humanitarian purposes such as monitoring epidemics. The public interest does not contain any thematic specifications, but can extend to everything that serves the community. However, Art. 9 (2) (g) GDPR is not a legal basis in and of itself, but an empowerpent for EU or MS legislators to balance the public interest with the needs of data protection. In Germany, we make use of this empowerment in § 22 (1) (1) (d) BDSG. However, it is questionable if this provision, which merely copies the GDPR text without specifying cases of public interest, is in line with the GDPR, and in any case, I would not consider this provision to be applicable to health data for research purposes.

Art. 9 (2) (h) GDPR could be relevant, at least prima facie, (purposes of preventive or occupational medicine ... medical diagnosis). It is also an empowerment for national legislators, and Germany has made use of it in § 22 (1) (1) (b) BDSG. However, for research purposes, Art. 9 (2) (j) GDPR is considered lex specialis, see below.

Art. 9 (2) (i) GDPR could be relevant: ("necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices").In

contrast to lit. g) and h), Art. 9 (2) (i) GDPR specifically refers to the public health interest. This regularly concerns cases in which consent of the data subjects cannot be obtained at all. "Public health" is understood as in Regulation (EC) No. 1338/2008. According to this, public health includes "all elements related to health, such as health status, including morbidity and disability, the determinants affecting that health status, the need for health care, the resources allocated to health care, the provision of health care services and universal access to them, as well as the corresponding expenditure and financing, and finally the causes of mortality [...]". In this respect, Art. 9(2)(i) GDPR is intended to prevent threats to public health; in contrast, Art. 9(2)(h) GDPR is intended to take into account healthcare. Germany has made use of it in § 22 (1) (1) (c) BDSG.

Art. 9 (2) (j) deals with research. Research is understood broadly, in line with Recital 159. "The processing of personal data for scientific research purposes within the meaning of this Regulation should be interpreted broadly to include processing for, for example, technological development and demonstration, fundamental research, applied research and privately funded research [...]". This very generous understanding is also underlined by the lack of a public interest reservation for processing for research purposes. However, Art. 9 (2) (j) also needs to be implemented by a provision in EU or MS law.

In Germany, § 27 BDSG applies, which reads "By way of derogation from Article 9(1) of Regulation (EU) 2016/679, the processing of special categories of personal data within the meaning of Article 9(1) of Regulation (EU) 2016/679 shall also be permitted without consent for scientific or historical research purposes or for statistical purposes where the processing is necessary for those purposes and the interests of the controller in the processing significantly outweigh the interests of the data subject in not having the processing carried out. The controller shall provide for appropriate and specific measures to safeguard the interests of the data subject pursuant to the second sentence of Section 22(2)."

As often in data protection law, the provision requires a balancing of interests, which is why a lot of research is still based on volunteers.

Regarding obligations for research institutions (other than consent), Article 89 GDPR gives some guidance: In general, they are treated as any other controller and need to fulfil all obligations the GDPR imposes on controllers. Additionally, the processing is subject to appropriate safeguards for the rights and freedoms of data subjects pursuant to Article 89 (1) of the GDPR. According to Article 89 (1) (2) GDPR, these safeguards must include technical and organizational measures to ensure respect for the principle of data minimization (Article 5 (1) (c) of the GDPR). This is achieved, for example, by reducing the amount of data collected and the scope of processing to the extent necessary for the purpose, setting a storage period, and regulating the accessibility of the data. The requirement of data minimization (Article 5 (1) (c) of the GDPR) and the requirement of storage limitation (Article 5 (1) (d) of the GDPR) are taken into account by the provision on anonymization and pseudonymization in Article 89 (1) (3) and (4) of the GDPR. However, in view of the general provisions of Article 25 (1) of the GDPR, there is doubt whether the increase in the minimum standards for data processing for research purposes pursued in Article 89 (1) of the GDPR actually adds any value. The same applies to § 27 (3) BDSG.

Finally, the European Health Data Space (EHDS) is part of the European Health Union and represents the first common EU data space in a specific area. Current developments include e-prescribing and e-administration as well as patient summary records, which are gradually being introduced in all EU countries.

※This work was supported by JST [Moonshot R&D][Grant Number JPMJMS2293]

III. Switzerland

Florent Thouvenin （Professor, Faculty of Law, University of Zurich)

Question List

1. The Relationship between Constitutional Law and Personal Data Protection Law

①Constitutional Status of the Right to Privacy or the Right to Informational Self-Determination

Is the right to privacy or the right to informational self-determination (i.e., the right to self-determination in the management of personal data; das Recht auf informationelle Selbstbestimmung) guaranteed as a constitutional right? If so, is the right to privacy interpreted to be different from the right to informational self-determination?

***

Answer:

The right to privacy is protected under article 13 (1) of the Federal Constitution of the Swiss Confederation (hereinafter "Cst."). It states that "[e]very person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications".

The right to informational self-determination is protected under article 13 (2) Cst. Albeit not named directly, it has been recognized as such by the Federal Supreme Court of Switzerland (hereinafter "FSC"). Article 13 (2) Cst. states that "[e]very person has the right to be protected against the misuse of their personal data". The right to informational self-determination is thus a subset of the broader right to privacy as stated in article 13 (1) Cst. Notably, article 13 (2) Cst. is interpreted by the FSC and parts of the doctrine in a broad sense according to which the provision does not only protect against the *misuse* of personal data but provides a right to informational self-determination. The FSC has consistently held that the constitutional right to informational self-determination guarantees that, "in principle, regardless of how sensitive the information in question actually is, every person must be able to determine vis-à-vis the processing of personal data by federal bodies and private persons whether and for what purpose the data is processed" (cf. Decision of the FSC 147 I 280, consideration 7.1; own translation). The FSC therefore does not only state that article

13 (2) Cst. contains a right to informational self-determination but it also interprets the right to informational self-determination very broadly. This view, however, is challenged by parts of the doctrine: Federal bodies in Switzerland are bound by the principle of legality and thus may only process personal data if a legal basis for such processing exists. As the processing of personal data by federal bodies is always based on a legal basis, there is no need for these bodies to request data subjects' consent for such processing. As a consequence, data subjects have no right to decide on the processing of personal data about them by federal bodies. As it turns out, a right to information self-determination does not exist with regard to federal bodies.

The situation is different for the processing of personal data by private parties. They are generally allowed to process personal data as long as they comply with data protection principles, such as the principle of transparency, purpose limitation, and proportionality. In contrast to the GDPR, the DPA is based on general permission to process personal data, subject to a prohibition. In the event of a breach of a data protection principle, private parties must justify the processing by asking for consent, claiming an overriding interest in the processing, or referring to a legal basis that allows such processing (see below for more details). As a result, in the vast majority of cases, private parties do not need to obtain the data subject's consent. Accordingly, there is not much left of the right to informational self-determination.

***

② Constitutional Significance of the Personal Data Protection Law

If the right to privacy or the right to informational self-determination is constitutionally protected in any sense, is such right defined or stipulated as a purpose or guiding principle of the personal data protection law? In other words, is the personal data protection law characterized as a statute that implements constitutional values or norms such as the right to privacy?

↓

Cf; While the Act on Protection of Personal Information in Japan has, as is seen in the purpose provision, no explicit reference to the words of the right to privacy or the right to informational self-determination, the GDPR declares that it is established on the constitutional basis of the right to the protection of personal data, which has been guaranteed as a fundamental right of the Charter of Fundamental Rights of the European Union.

***

Answer:

The Swiss Federal Act on Data Protection (hereinafter "DPA") applies to both Swiss federal bodies and private persons, namely businesses. The purpose of the DPA is to "protect the personality and the fundamental rights of natural persons whose personal data are being processed" (article 1 DPA).

However, the concrete requirements for data processing differ for federal bodies and private persons. Unlike federal bodies, private persons are not generally bound by fundamental rights. However, fundamental rights can also have third-party effects on private individuals. In data protection law in particular, the legislator is obliged to enact legislation that takes account of the right to informational self-determination between private parties. This has been done with the DPA and its provisions regulating the processing of personal data by federal bodies and private parties.

***

2. The Overview of Personal Data Protection Law

① The Influence of other countries' legal systems

Are there any countries that you have referred to as models in enacting your country's personal data protection law?

***

Answer:

The initial Swiss Federal Act on Data Protection of 1992 and its origin do not contain explicit reference to particular countries which have modeled for the Swiss DPA. Its preparation, however, began during or shortly after the enactment of data protection acts in Germany, France, and Austria and it is safe to assume that the Swiss DPA has been influenced by the laws of these countries. The FSC has, however, made explicit reference to the so-called "Volkszählungsurteil" judgment by the German Federal Constitutional Court (hereinafter the "FCC") and recognized the right to informational self-determination as inferred by the German FCC in the afore-mentioned judgment.

The recently revised DPA of 2020, which entered into force on 1 September 2023 was heavily influenced by the General Data Protection Regulation (hereinafter "GDPR") of the European Union and by the Protocol amending the Council of Europe Convention for

the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) of the Council of Europe (hereinafter the "Amending Protocol"). The revision aimed at harmonization with the GDPR to ensure that Switzerland continues to be qualified as a country with an adequate level of protection within the meaning of article 45 GDPR. The revision also aimed at ensuring the compatibility of the Swiss law with the Amending Protocol so that the latter could be signed and ratified.

***

②Definition and Scope of "personal data"

Are cookies and other online identifiers included among personal data under the personal data protection law? What is the definition of personal data under the personal data protection law?

↓

Cf; GDPR provides that " "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In contrast, the Act on Protection of Personal Information in Japan defines the scope of personal information more narrowly than GDPR; the Act provides that the personal information in this Act is the information by which "a specific individual can be identified". Thus, in principle, cookie information by itself does not constitute personal information, since the *identifiability* of a *specific* person is strictly required in order for any information to fall in the category of personal information. This regulation scheme has been criticized as a factor that hinders effective profiling regulation.

***

Answer:

The Swiss DPA defines personal data similarly to the GDPR as "all information relating to an identified or identifiable natural person" (article 5 (a) DPA). Under GDPR, a person is considered identifiable if the combination of (other) data available to the controller leads to the identity of the person without an unreasonable effort. Accordingly, cookies and other online identifiers can be considered personal data under Swiss law. The Swiss Telecommunications Act (hereinafter "TCA") furthermore stipulates that the processing

of data on external equipment by means of transmission using telecommunications techniques is permitted only if users are informed about the processing and its purpose and about their right to refuse such processing (article 45c (b) TCA). This provision applies to the use of cookies as well.

***

③ The Rights of Data Subjects and the Obligations of those who process personal data

a) The right to erase personal data (e.g., GDPR Article 17) or the right to utilization cease

***

Answer:

Article 32 (2) DPA states that actions relating to the protection of personality rights are governed by the Swiss Civil Code (hereinafter "CC"). Particularly, article 32 (2) (c) DPA states that a claimant may request that personal data be deleted or destroyed. In contrast to the GDPR, the right to erasure is designed as a remedy against the violation of personality rights and is not construed as a data subject right that may be asserted at any time. Consequently, a right to the erasure of personal data exists in Switzerland in line with general personality rights but it must be pondered on a case-by-case basis which interest prevails.

***

Is there any correlation between the right of personality under civil law or the right to erasure and the provisions of the DPA? For example, if a data controller violates the provisions of the DPA regarding consent or purpose binding, may a request for erasure be permitted under the Civil Code? Could you please tell us the conditions under which a request for deletion or erasure will be permitted?

***

Answer:

There is a close correlation between the protection of the personality in civil law and data protection law as the DPA aims to protect the personality of data subjects. In addition, the DPA refers to the provisions in the CC for the remedies a data subject may invoke in case of a violation of the DPA. As the DPA refers directly to the provisions of the CC, a request for erasure is given under the CC. In addition, article 32

para 2 lit. c of the DPA explicitly mentions a right to erasure as one of the remedies that can be invoked. A violation of the provisions of the DPA, in particular the data protection principles set forth in article 6 DPA, constitutes a violation of the data subjects' personality. Such violation is unlawful unless it is justified (see below for more details). In case of an unlawful violation of the data subjects' personality, the remedies under the CC are available. Particularly, the data subject may request by way of legal action that the violation of the personality cease (article 28*a* (1) (2) CC). In addition, the data subject may invoke the remedies explicitly mentioned in the DPA such as the right to erasure. Whether a request for erasure will be permitted is subject to a decision by the competent civil court. Such request will only be permitted if the unlawful violation of the personality is not merely imminent but current and ongoing at the time of the decision.

***

b) The Status and Significance of Consent in Personal Data Protection Law (opt-in or opt-out?): When is the consent of the individual required under the personal data protection law? Whether a business is required to obtain the consent of the individual (data subject) when acquiring personal data? When personal data is provided to a third party, is the consent of the individual required to be obtained?

***

Answer:

Whereas data processing under GDPR is built upon a general prohibition with the reservation of permission (cf. article 6 (1) (a) GDPR: "Processing shall be lawful only if and to the extent that at least one of the following applies (…):"), the processing under the DPA is built upon a general permission with the reservation of prohibition. Article 30 (1) DPA states that "anyone who processes personal data must not unlawfully violate the data subjects' personality." Private persons may therefore generally process personal data as long as they comply with the data protection principles. For example, processing must be carried out in good faith, must be proportionate and data may only be collected for a specific purpose (purpose limitation). If the data is processed in contravention of these principles, it is considered a violation of the data subjects' personality (article 30 (2) (a) DPA). Such violation is unlawful unless it is justified (1) by the consent of the data subject, (2) by an overriding private or public interest, or (3)

by statutory law (article 31 (1) DPA). Some examples of an overriding interest of the controller are mentioned in article 31 (2) DPA. Consequently, a business may, for example, assert an overriding private interest to process personal data of a contractual party in direct connection with the conclusion or the performance of a contract (article 31 (2) (a) DPA) and is therefore not required to obtain consent for the processing of these data.

If the processing of personal data is justified by consent it must be carried out on the basis of free, specific, informed, and unambiguous consent (cf. article 5 (2) of the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data). However, implied consent is generally sufficient, unless sensitive personal data are being processed, in which case explicit consent is required (article 6 (7) (a) DPA). In this regard, it can be added that an express declaration of intent against the data processing also constitutes a violation of personality (cf. article 30 (2) (b) DPA), which must subsequently be justified. Thus, generally, the possibility of opt-out exists as well.

Businesses therefore need not regularly obtain consent from the data subject when acquiring and processing personal data. Rather, they can justify the processing of personal data in other ways, namely based on their overriding interest. A (rather informal) survey by the Swiss Association for Corporate Data Protection in Winter 2022/2023 has found that only roughly 15 % of data processing by the participating 45 companies is based on consent. The remaining 85 % are based on other justifications, namely an overriding interest or a legal basis, or need no justification at all as the processing complies with the data protection principles.

When personal data is provided to a third party, no consent is required but as part of the duty of information, the recipients or the categories of recipients of personal data must be disclosed at the time of the collection of data.

***

c) The Limit of the Notice and Consent model and the countermeasure: Daniel J. Solove, an authority on privacy law, points out the limitations of the privacy self-management model in data protection law as follows; “[The U.S. privacy laws] provide[s] people with a set of rights to enable them to make decisions about how to manage their data. These rights consist primarily of rights to notice, access, and consent regarding the collection, use, and disclosure of personal data. The goal of this bundle of rights is to provide people with control over their personal data. …As empirical and social science research demonstrates, cognitive problems impair individuals’ ability to make informed, rational

choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data."
Thus, if there are limits to the self-management model in terms of the limitations of human cognitive abilities, how does your country's personal data protection law address these challenges? For example, is an effective notice required for businesses?

***

Answer:
Enforcement of the DPA is primarily carried out by the Federal Data Protection and Information Commissioner (hereinafter "FDPIC" or "the Commissioner"), who has the power to initiate investigations (see below). In this way, the Swiss DPA partly tackles the challenges coming from the limitations of the privacy self-management model by entrusting a dedicated third party. The DPA is, however, based on the assumption of the rational choice by the data subjects. The DPA therefore does not address these challenges in a convincing way. The DPA merely stipulates that consent is only valid if it has been given freely and for one or several specific processing activities and after adequate information (article 6 (6) DPA). If sensitive personal data is processed or a profiling by a private person is high-risk or a federal body is conducting profiling at all, consent must be given explicitly (article 6 (7) DPA).

***

d) How are devices or architectures such as a Personal Data Store (PDS) being utilized to assist with the person's controllability of their personal data?

***

Answer:
While there are projects to assist with the person's controllability of their personal data in Switzerland, none have established themselves so far and are being (broadly) utilized.

***

e) Profiling regulations. E.g., the right to object to profiling (GDPR Article 21).

***

Answer:

There are some specific regulations regarding profiling in the DPA. As mentioned above, if profiling is considered "high risk", explicit consent must be given (article 6 (7) (b) DPA). However, this only applies if consent is required with regard to the justification scheme (see above). High-risk profiling is profiling involving a high risk to the personality or fundamental rights of the data subject, as it creates a pairing between data that enables an assessment of essential aspects of the personality of a natural person (article 5 (g) DPA). In such cases, a data protection impact assessment is mandatory due to the high risk for the data subject's personality or fundamental rights (article 22 (1) DPA).

Explicit consent is also required for any profiling conducted by a federal body (article 6 (7) (c) DPA). For any such profiling by a federal body, a formal law must exist as a statutory basis (article 34 (2) (b) DPA).

***

f) The right to data portability or the right to transmit personal data (e.g., GDPR Article 20)

***

Answer:

The right to data portability was added to the DPA in the revision of 2020. Article 28 DPA is based on the GDPR and closely aligned with article 20 GDPR. According to article 28 (1) DPA, any person may request from a controller, free of charge, the disclosure of personal data that they have disclosed to him in a standard electronic format if the data is processed in an automated manner and it is processed with the consent of the data subject or in direct connection with the conclusion or performance of a contract between the controller, and the data subject. As with article 20 (2) GDPR, under the DPA the data subject may also request the controller to transfer their personal data directly to another controller, if the general requirements are met and the transfer does not involve a disproportionate effort (article 28 (2) DPA).

Article 29 DPA furthermore foresees possible restrictions to the right to data portability if the relevant conditions are met.

***

And in what situations are these rights implemented in practice?

***

Answer:

As the revised DPA has just entered into force on 1 September 2023, it is too early to tell.

***

④Organization and authority of the supervisory body enforcing personal data protection law. Sanctions and complaint mechanisms.

***

Answer:

Under the DPA the FDPIC is the supervisory body (article 43 et seqq. DPA). Its head is appointed by the Swiss Parliament for a duration of four years and exercises his duty independently from other authorities (articles 43 (4) and 44 (1) DPA).

The Commissioner may initiate investigations against federal bodies or private persons if there are sufficient indications that data processing violates the data protection regulations (article 49 (1) DPA). The federal body or the private person is required to provide the FDPIC with all information and to make available all documents which are necessary for the investigation (article 49 (3) DPA). If they do not comply, the FDPIC may access all information and documents that are required for the investigation, access premises, and facilities, question witnesses, and order evaluations by experts (article 50 (1) DPA).

By means of administrative measures, the FDPIC may further order that the processing of data is fully or partially adjusted, suspended, or terminated and that the personal data is fully or partially deleted or destroyed if data protection regulations are violated (article 51 (1) DPA). The Commissioner may furthermore defer or prohibit a transfer of data to a foreign country if the provisions on the transfer to a foreign country are violated (article 51 (2) DPA).

The FDPIC furthermore informs, trains and advises both the federal bodies and the private persons, raises public awareness, provides persons with information on how to exercise their rights and provides an opinion on draft federal legislation (article 58 (1) DPA).

Under the DPA, the sanctions are designed as criminal offenses, as opposed to administrative offenses. Unlike under the GDPR, the sanctions target the individual persons, e.g., the employees of a business and not the business itself. While the fines are lower than under GDPR, the impact may be stronger because the fines cannot be factored

in by the (large) companies and employees will have strong incentives to avoid the fines and criminal proceedings, possibly resulting in a criminal record. In terms of procedural law, the cantons are responsible for the prosecution and the judgment of criminal acts under the DPA, in line with general Swiss criminal law.

Article 60 (1) DPA stipulates that private persons are criminally liable to a fine of up to 250,000 Swiss Francs (approx. ¥ 42,000,000) if they breach their obligations regarding the duty of information and regarding the access right. They are further liable if they willfully fail to inform data subjects appropriately about the collection of personal data or about an automated individual decision or if they willfully fail to provide to the data subject all information that is required in order for the data subject to assert his rights as per article 19 (2) DPA. These liabilities apply only if a complaint is filed.

Private persons are further liable to a fine of up to 250,000 Swiss Francs if they willfully provide false information to the FDPIC in the context of an investigation or willfully refuse to cooperate (article 60 (2) DPA).

Additionally, article 61 DPA stipulates a fine of up to 250,000 Swiss Francs for a violation of duties of diligence: Upon complaint, private persons are liable if they willfully disclose personal data abroad in violation of other provisions of the DPA, if they assign the data processing to a processor without ensuring that relevant provisions of the DPA are met or if they fail to comply with the minimum data security requirements.

Furthermore, according to article 62 DPA, a private person is, upon complaint, liable to a fine of up to 250,000 Swiss Francs if they willfully breach their professional confidentiality obligations. Lastly, article 63 DPA states that private persons are liable to the same fine if they willfully fail to comply with a decision issued by the FDPIC or an appellate authority, which contains reference to the criminal penalty of article 63 DPA.

The statute of limitations for these acts is five years (article 66 DPA).

***

⑤Judicial proceedings or judicial remedy (standing to sue. class action.)

***

Answer:

If personal data is processed by a private person, a data subject may generally request that incorrect data be corrected (article 32 (1) DPA). For other actions relating to the protection of the personality of the data subjects the DPA refers to the CC, which contains the relevant provisions. Particularly, a claimant may request that a specific data processing be prohibited, a specific disclosure of personal data to third parties be

prohibited and that personal data be deleted or destroyed (cf. article 32 (2) DPA). The judicial proceedings may be directed against any party that causes the infringement of the personality rights, such as controllers, processors or auxiliary persons.

For judicial proceedings between private parties, the Swiss Civil Procedure Code applies. The data subject has the right of action against the controller and may sue at the courts at the domicile or registered office of either of the parties. Material and functional jurisdiction is governed by cantonal law.

If personal data is processed by a federal body, the procedure is governed by general provisions of the Federal Act on Administrative Procedure (cf. article 41 (6) DPA). Persons requesting the responsible federal body to (1) refrain from unlawfully processing personal data, (2) eliminate the consequences of unlawful processing or (3) ascertain the unlawfulness of the processing, have a right to receive a ruling from the federal body (cf. article 41 (1) DPA). The ruling may then be contested by appeal to the Federal Administrative Court (hereinafter "FAC") and, finally, to the FSC.

Investigations by the FDPIC also result in a ruling by the FDPIC. They may also be contested by appeal to the FAC. The data subject is not a party to the investigation but must be informed by the FDPIC about the results of the investigation (article 49 (4) DPA).

***

⑥Article 9 (2) (g) of GDPR provides that "the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person [and] data concerning health" are permitted if "[such a] processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".
We have a question about the relationship between this provision and the utilization of health data for research purposes.
Is the consent of the patient required for the use of his/her medical record or biometric data for research purposes or drug development? What legal obligations (such as anonymization) do research institutions have when collecting and utilizing patient health data for research purposes?
And we would like to know about a recent development in European Health Data Space

(EHDP).

***

Answer:

Under Swiss law, the use of a patient's medical record or biometric data for research purposes or drug development most often falls within the scope of the Human Research Act (hereinafter "HRA"). The HRA applies to all research concerning human diseases and/or the structure and function of the human body, involving, *inter alia*, the use of health-related personal data for such purposes (article 2 (1) (e) HRA). For research falling within the scope of the HRA, informed consent is required for the (primary) collection of health-related personal data (article 16 et seq. HRA). A person may thus only be involved in a research project if they have given their informed consent in writing. To be duly informed, they must receive comprehensible oral and written information on (i) the nature, purpose, and duration of, as well as the procedure for, the research project, (ii) the foreseeable risks and burdens, (iii) the expected benefits of the research project, in particular for themselves or for other people, (iv) the measures taken to protect the personal data collected and (v) their rights (article 16 (2) HRA). The persons concerned are to be given an appropriate period for reflection before deciding whether they are willing to consent (article 16 (3) HRA). In addition, any research project must be authorized by the responsible ethics committee (article 45 (1) (a) HRA).

Special rules apply to the further (secondary) use of genetic data (and biological material). These materials and data may be used in uncoded form for a particular research project if informed consent has been given by the person concerned (article 32 (1) HRA). They may furthermore be used for research purposes in general in coded (i.e. pseudonymized) form if informed consent has been given by the person concerned (article 32 (2) HRA). In addition, biological material and genetic data may be anonymized for research purposes if the person concerned has been informed in advance and has not dissented from the anonymization. If anonymized, biological material and genetic data no longer fall within the scope of the HRA or the DPA.

A similar cascade exists for non-genetic health-related personal data. These data may be further used in uncoded form for research purposes in general if informed consent has been given by the person concerned (article 33 (1) HRA). In coded (i.e. pseudonymized) form, the data may be further used if the person concerned has not dissented (article 33

(2) HRA). As anonymously collected or anonymized data does not fall within the scope of the HRA (cf. article 2 (2) (c) HRA) the further use of such data is allowed without restrictions.

Additionally, article 34 HRA contains an exception clause that allows for biological material and health-related personal data to be processed for research purposes without the data subjects' consent if three conditions are met. First, it must be impossible or disproportionately difficult to obtain consent or to provide information on the right to dissent; the same applies if this would impose an undue burden on the person concerned. Second, no documented refusal must be available. Third, the interests in carrying out the research must outweigh the interests of the persons concerned in deciding on the further use of his or her biological material or health related personal data. While designed for exceptional cases only, article 34 HRA has become the rule in practice.

In Switzerland, there are currently no plans to participate in a European Health Data Space. Swiss Parliament has, however, mandated the Swiss Federal Council to create a framework law for the secondary use of data in strategically relevant areas such as health care. A proposal for such a law is not to be expected before 2024 or 2025.

***

Disclaimer: As English is not an official language of Switzerland, the wording of the DPA was taken from the unofficial translation of https://datenrecht.ch/gesetzestexte/ndsg-en/.

***

※This work was supported by JST [Moonshot R&D][Grant Number JPMJMS2293]

IV. France

Yukiko Ogawa
(Assistant Professor, Faculty of Law, Teikyo University)

1. 個人情報保護法制と憲法的価値の実現

（1） 情報プライバシー権

フランスは、1978 年に制定した「情報処理、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（Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés）」（以下、「情報と自由法」という）によって、国のデータ保護機関 CNIL（Commission Nationale de l'Informatique et des Libertés、情報処理と自由に関する国家委員会）を創設し、中央集権型の個人情報保護を図ってきた。本法律の起草時点において、既に、フランス国内だけではなく、先進諸国において多くの大規模データベースが実際に運用されていた。かかる状況に鑑み、市民の私生活の秘密（le secret de la vie privée）を保護するために、諸情報へのアクセス条件を厳格に規制する目的で、本法律が制定された[1]。

フランスでは、いわゆるプライバシー権は、私生活の尊重を受ける権利（droit au respect de la vie privée）として保障される。もともとは、ヨーロッパ人権条約 8 条を具体化するために、「すべての人は私生活を尊重される権利を有する」と規定する民法 9 条（loi n° 70-643 du 17 juillet 1970）として法制化され、以来、法律上の権利として司法裁判所によって保護されていた。1999 年の 2 つの憲法院判決[2]が、私生活の尊重を 1789 年人権宣言 2 条に根拠づけたことで、憲法上の権利としての位置づけが明確になったとされている。なお、1958 年のフランス第五共和国憲法は、私生活の尊重を受ける権利に関する直接的な規定を置いていない。

私生活の尊重を受ける権利の内容は、未だ発展途上にあるが、一般に、私生活の尊重は、私生活の秘密（住居、自動車、通信、個人情報等）と、私生活の自由（自己決定権や社会生活上のつながり）とに分けられ、憲法院判決にみられるのは主として前者の側面に限定されている[3]。

個人データの保護と私生活の尊重との関係については、2012 年の憲法院判決[4]は、「個人

---

[1] Texte n° 1004 (1973-1974) de M. Pierre-Bernard COUSTE, déposé à l'Assemblée Nationale le 4 avril 1974, Proposition de loi tendant à créer une Commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens.

[2] Décision n° 99-419 DC du 9 novembre 1999（齊藤笑美子「婚姻外カップル立法化の合憲性―パックス（PaCS）判決」フランス憲法判例研究会編『フランスの憲法判例 II』91-94 頁）, Décision n° 99-422 DC du 21 décembre 1999.

[3] 馬場里美「私生活の尊重」同書 87-90 頁

[4] パスポート作成時の個人情報処理に際する指紋や目の色等の生体認証データの取得について規定するアイデンティティの保護に関する法律について、法律審署前に憲法適合性が争われた事案。Décision

データの収集、記録、保存、閲覧および通信」が私生活の尊重への権利に対する制約にあたることを前提に、当該処理が、「一般利益（intérêt général）によって正当化され、その目的に適切かつ比例した方法で実施されなければならない」と判示した。

（２）　情報自己決定権

情報自己決定権（le droit à « l'autodétermination informationnelle »）は、フランス憲法（憲法ブロック）に明文の規定はなく、憲法院も未だ憲法上の権利として真正面から承認しているものではないが、今日、実定法上の概念としては、「すべての人は、この法律に定める条件の下で、自分に関する個人データの使用を決定し及び管理する権利を有する」と規定する2016年10月7日のいわゆる「デジタル共和国法」(loi n° 2016-1321 du 7 octobre 2016 pour une République numérique）54条にあらわれている。この規定は、1983年12月15日のドイツ連邦憲法裁判所判決（国勢調査法判決（1983年12月15日：BVerfGE 65, 1 ））の影響を受け、政府提出法律案の最初の段階から提案されていた[5]。法律案に付された影響評価書によれば、自分のデータを自由に処分する権利(le droit à la libre disposition de ses données)ないしは〔自分の〕個人データ自由処分の原則(principe de libre disposition de ses données)の実現は、個人データ保護の新たな局面として認識されている。すなわち、単なる私生活の保護から、オンライン上の生活をコントロールしようとする個々人の保護へと、新しいパラダイムが提示された。アクセス権やデータポータビリティ権は、後者の権利として位置づけられる。他方で、データ処理が、デジタル共和国法や、後に言及する2018年の「個人データの保護に関する法律」等、法令の規定に従ってなされる場合、個人の自己決定よりも、悪用を避けるためにデータ管理者に課される条件が重視されており、情報自己決定権の主観的権利としての保障は十分には達成されていない、との指摘もある[6]。

2.　個人情報保護法制の現状と課題

（１）　1978年「情報と自由法」制定

フランスが、1978年に、情報と自由法（Loi Informatique et Libertés :LIL）[7]を制定し、データ保護機関CNILを創設するに至った大きなきっかけは、Safari事件であった。フランスでは、出生時に、フランス国立統計経済研究所（Institut National de la Statistique et des Études Économiques : INSEE）によって割り当てられる個人台帳登録番号（Numéro

---

n° 2012-652 DC du 22 mars 2012.

[5] 政府提出法律案に付された影響評価書（Étude d'impact）96-97頁および立法理由（ecposé des motifs）参照

[6] Audrey BACHERT-PERETTI, « France », *Annuaire international de justice constitutionnelle (2021),* ECONOMICA/PUAM, 2022, pp. 324.

[7] 正式名称は、情報処理、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（Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés）

d'Inscription au Répertoire :NIR）が、全国個人識別台帳（Répertoire National d'Identification des Personnes Physiques : RNIPP）に登録される。ジョルジュ・ポンピドゥ政権下のフランス政府は、警察署や行政機関など 400 以上の組織で分散して保有している 1 億近くの全ファイル（état-civil、租税、地籍台帳、健康データなど）を、国民に付与された単一の強制識別子（NIR）を用いて相互接続し、内務省（内務大臣ジャック・シラク）において一元管理する計画――Safari（Systeme Automatise pour les Fichiers Administratifs et le Repertoire des Individus、行政ファイルと個人台帳の自動システム）計画――を予定していたところ、1974 年 3 月 21 日のル・モンド紙が、「« Safari » あるいはフランス人狩り」という挑発的な見出しをつけて、この計画を暴露した[8]。これを受けて、ピエール・メスメル首相の同年 3 月 29 日付け通達により、予防措置として、異なる省庁に属する情報システム間の新たな相互接続が禁止され、1974 年 11 月 8 日のデクレにより、国務院副院長のベルナール・シュノと破毀院初代院長のモーリス・アイダロを委員長とする情報と自由委員会が設立された。この委員会は、政府当局による IT ツールの使用に関する規制についての検討を目的とするもので、総報告者の名前にちなんで命名されたトリコ報告書が、1975 年 6 月 27 日、首相に提出され、1977 年 11 月に、のちに情報と自由法となる法案に関する議会審議が開始された[9]。

情報と自由法制定に際しては、スウェーデンのデータ保護法（1973 年）、アメリカのプライバシー法（1974 年）、ドイツのヘッセン州データ保護法（1970 年 10 月 7 日）など、既に個人データ保護に関する法制を有する諸国の例のほか、イギリスの政府データベース創設に関する法律や私人の秘密の自由の保護に関する法律など、成立には至らなかった法案や政策も広く参照されている[10]。IT 技術の進展に伴って、こと先進国の公的機関が大規模なデータベースを保有し始めるなか、データ保護法の整備が急務として認識されるようになり、フランスもその潮流のなかで本法制定に至ったものである。

1978 年法によって設置された CNIL が、フランスで初めて「独立行政機関」としての法的性格を付与されたという事実は、SAFARI 事件を契機に露呈した公的機関による IT 利用の危険性と、公的機関から独立した組織設立の必要性の証左ともいえよう。行政機関による大規模な集中情報システムの実装に対応して、国民に新たな権利を認めることは、情報と自由法制定の最大の目的であった[11]。1978 年法のその先駆的な性格は、第 108 号条約として

---

[8] « Safari » ou la chasse aux Français, Le monde, 21 mars 1974, https://www.cnil.fr/sites/default/files/atoms/files/le_monde_0.pdf （最終閲覧日：2023 年 9 月 24 日）

[9] Audrey BACHERT-PERETTI, « France », *Annuaire international de justice constitutionnelle (2021)*, ECONOMICA/PUAM, 2022, pp. 314.

[10] Texte n° 1004 (1973-1974) de M. Pierre-Bernard COUSTE, déposé à l'Assemblée Nationale le 4 avril 1974.

[11] もっとも、情報と自由委員会は、「公共、半公共及び民間の各部門における IT の発展が、私生活、個人の自由及び公的自由を尊重して行われることを保証する措置を政府に提案する」（1974 年のデクレ第 1 条）ことをその任務としており、当初から、公共部門と民間部門に同一の法律を適用することを想定して

知られる、個人データの自動処理に関する個人の保護に関する条約に大きな影響を与えたと評されている[12]。

なお、NIR は、社会保障の分野で利用されてきた経緯があり、社会保障番号とも呼ばれているが、今日、NIR を税、教育、警察など、他の行政サービスに関するファイルと統合して管理することは認められておらず、セクターごとに ID が割り当てられている[13]。ファイルの相互接続や個人情報の利用が、それが正当化される目的以外の目的でなされることを回避するために、CNIL は統一番号の使用には一貫して否定的な立場を示しており、SAFARI 計画への反動として CNIL が設置されたことを踏まえると、フランスは、「日本のような“統一番号制”は絶対に採用しない」ことが確実とも評されている[14]。2019 年には、「加盟国は、国民識別番号又はそれ以外の一般に利用されている識別子の取扱いのための特別の条件を別に定めることができる」と規定する EU 一般データ保護規則（以下、「GDPR」という）87 条を受けて、NIR の利用目的を制限するデクレ（Décret n° 2019-341 du 19 avril 2019、通称 « cadre NIR » ）が制定された。« cadre NIR »では、社会保護、健康、雇用、租税、裁判、統計・国政調査、教育の分野ごとに NIR の利用が可能な目的を限定列挙し、これに該当しない目的での NIR 利用は禁止している。

（２） 2018 年「個人データの保護に関する法律」による「情報と自由法」改正

2016 年、GDPR（GDPR の立法過程については、第 8 章 II 参照）が採択されたことを受け、フランスは、GDPR に準拠する国内法の整備を迫られた。GDPR は「規則」である以上、加盟国の国内法に優先して、加盟国の政府や企業、個人等に直接適用される性質を有する。他方、規則には、その実施にあたり加盟国に判断・裁量の「余地」を認める部分が多かれ少なかれ存在するのが通例である。GDPR 上の「自然人」（4 条 1 号）に死者が含まれるか、「監督機関」（4 条 21 号、51 条）を新たに創設するのか、既存の機関を当てるのか、

いた点は、諸外国との比較において際立った特徴といえる。

[12] Audrey BACHERT-PERETTI, op.cit., p. 314.

[13] 個人 ID 管理のモデルをセパレートモデル（行政サービス分野ごとに異なる ID を管理し、それぞれの情報は相互に利用できない方式）、フラットモデル（一つの共通 ID を全ての分野で利用し、効率的に情報連携できる方式）、セクトラルモデル（行政サービス分野ごとに ID を管理する一方で、業務別の個別 ID が分野共通 ID と紐付けられ、分野間での情報連携の際には分野共通 ID を他の分野共通 ID に変換して情報を連携する方式）に分類する見解によれば、フランスは、セパレートモデルに分類される。株式会社国際社会経済研究所「国家情報システム（国民 ID）に関する調査研究報告書―英国、フランス、イタリア等における番号制度の現状―」（2011）20 頁 https://www.i-ise.com/jp/report/pdf/rep_it_201010.pdf （最終閲覧日：2023 年 9 月 24 日）、鈴木尊巳「日本がモデルにしたオーストリア電子政府と今後の ID 連携」Fujitsu 68（4）（2017） 80-87 頁 https://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol68-4/paper02.pdf （最終閲覧日：2023 年 9 月 24 日）参照。

[14] 自治体国際化協会「平成 17 年度海外比較調査　各国の電子自治体の推進状況」（2006）77 頁［坂尻昇太担当執筆］

同意年齢を何歳にするか（8 条 1 項)、「削除権（忘れられる権利)」(17 条）や「データポータビリティ権」(20 条）などこれまでの情報と自由法には規定のなかった新しい権利をどう実効的に保障するか、プロファイリング等の自動処理に基づく決定をされない権利に関して加盟国に独自の措置を定めるか（22 条 2 項 (b))、規則違反に対して損害賠償を請求する集団訴訟の可能性（21 世紀に向けた司法の近代化に関する 2016 年 11 月 18 日の法律によって導入した集団訴訟の対象に含むか、その訴訟要件等)、データ処理事業者が従うべきルールの標準化・簡素化（特に、CNIL による許可等の事前手続きの軽減とリスクベースの事後手続きの導入）など、適用条件につき加盟国に選択の「余地」が与えられている 50 以上の部分については国内での議論が強いられた。とりわけ、加盟国に判断の余地が与えられた部分については、加盟国間での調整・調和が求められる。なぜなら、加盟国間で適用するルールやその条件が異なる場合、どのルールが適用されるかは、データ管理者やその下請け業者の所在地によって異なりうるからである。たとえば、同意年齢を 13 歳と定めるスウェーデンの法律は、スウェーデンを所在地とするデータ管理者等に適用されるため、当該データ管理者等がフランス国内において情報提供サービスを行う場合には、たとえフランスが同意年齢を 16 歳に設定していたとしても、フランス居住者はスウェーデンの法律の適用を間接的に受けることになる。なお、法改正に際しては、アイルランドに主要拠点を置く Google と Facebook を念頭に議論が進められた[15]。

（3）　「個人データ」の定義

情報と自由法は、「個人データ」を次のように定義している（第 2 条第 2 項第 1 文)。

個人データとは、識別された自然人又は識別番号若しくはその者に固有の一若しくは複数の要素を参照することによって、直接的または間接的に識別しうる自然人に関するあらゆる情報から構成される。

Cookie は、それ単体では、自然人を識別できないが、他の情報と組み合わせることにより自然人を識別しうるときは「個人データ」にあたる。自然人を識別しうるか否かの判断は、「自然人の識別を可能にするすべての手段又はデータ管理者若しくはその他の者がアクセスしうるすべての手段を考慮に入れなければならない」(同第 2 条第 2 項第 1 文）とされている。Cookie に関しては、情報と自由法 82 条によって、e プライバシー指令を国内法化しており、「個人データ」に該当するか否かに関わらず、同条の適用を受ける。

なお、GDPR の発効を受けて、CNIL が 2019 年に、Web サイト発行者によってユーザーのコンピューターに配置される「Cookie」およびその他のトラッカー接続ファイルに関する新しいガイドラインを策定したところ、さまざまな専門家団体から、ガイドラインの廃止を求める要望書が提出されたことを受け、国務院は、Cookie ウォールを法的に禁止する部分について無効と判断する一方で、Cookie の使用目的の明示、Cookie への同意の拒否ま

[15] Etude d'impact, Projet de loi relatif à la protection des données personnelles, 12 décembre 2017, p.75.

たは撤回の容易さ、Cookie の推奨保持期間など、他の推奨事項の合法性を確認した[16]。

（４）　個人データの処理が合法であるための要件

フランスにおいては、GDPR が直接適用されるため、データ主体の権利と事業者の義務について、基本的には、GDPR と同様のルールが適用される。

個人データの処理（traitements）は、以下に掲げる条件のうち少なくとも一つを満たしている場合に合法とされる（法 5 条）

①処理が、GDPR に規定する個人データ保護制度の対象となる処理にあたる場合は、GDPR4 条 11 号及び 7 条に規定する条件の下で、データ主体の同意を得ている場合

②処理が、データ主体が当事者である契約の履行又はデータ主体の要求に応じてとられる契約前の措置を実行するために必要な場合

③処理が、データ管理者が従うべき法的義務を遵守するために必要な場合

④処理が、データ主体又は他の自然人の重大な利益を保護するために必要な場合

⑤処理が、公共の利益のための役務遂行のために必要又はデータ管理者に与えられた公権力の行使の下で必要な場合

⑥公的機関がその役務を遂行するために行うものを除き、処理が、データ管理者又は第三者が追求する正当な利益の目的に照らして必要な場合。ただし、特にデータ主体が子どもである場合など、個人データの保護を必要とするデータ主体の利益、自由及び基本的権利が優先される場合はこの限りでない。

なお、GDPR8 条 1 項を受けて、フランスは、単独で有効に同意できる年齢を、15 歳としている（法 7-1 条、45 条）[17]。15 歳未満の者は、その親権者（le ou les titulaires）が共同で同意したときにのみ、個人データの処理が有効となる。

（５）　データ主体の権利と事業者の義務

①情報提供を受ける権利（droit à l'information）

GDPR12 条から 14 条に規定する条件の下で行使される（法 48 条 1 項）

---

[16] Conseil d'État n° 434684, lecture du 19 juin 2020.

[17] 同意年齢について、フランス政府案は GDPR に規定する 16 歳を維持していたが、国民議会（下院）では、13 歳を同意年齢とするスペインやチェコ共和国、14 歳とするエストニアなど、独自の選択をしている加盟国の法案がフランス社会に与える影響が考慮され、青少年のインターネット利用の実情、親権者からの同意取得可能性等を検討した上で、最終的には 15 歳を同意年齢とすることになった。なお、実際には、オンライン上で親権者の同意を得るのは簡単ではない。CNIL デジタルイノベーションラボラトリー（Laboratoire d'Innovation Numérique de la CNIL: LINC）では、ゼロ知識証明による「プライバシーを尊重した年齢認証システム」を開発中である。Jérôme Gorin, Martin Biéri et Côme Brocas, Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée, 21 juin 2022, https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee（最終閲覧日：2023 年 9 月 24 日）

15 歳未満の者への情報提供は、明確かつわかりやすい言語で提供する（同条第 2 項）

必要な範囲で、情報と自由法 48 条〜56 条に規定する権利を死後に行使することができる（法 85 条）。したがって、死後の個人データの処理についての指示を定める権利についても情報提供を受ける（同条第 3 項）

②アクセス権（droit d'accès）

GDPR15 条に規定する条件の下で行使される（法 49 条 1 項）

個人データの隠匿又は消失のおそれがある場合、裁判官は、略式手続含め、隠匿又は消失を回避しうるあらゆる措置を命ずることができる（同条第 2 項）

ただし、統計の確立又は科学的若しくは歴史的研究の実施のみを目的として必要な期間を超えない期間、関係者のプライバシー及びデータ保護の侵害のリスクを明確に排除する形式で保管される場合並びに国内安全保障法 L. 863-2 条に基づいて専門諜報機関に送信された情報には適用されない（同条第 3 項）

③訂正権（droit de rectification）

GDPR16 条に規定する条件の下で行使される（50 条）

④削除権（droit à l'effacement）

GDPR 1 7 条に規定する条件の下で行使される（法 51 条第 1 項）

データ主体の請求に応じて、特に、当該データ主体が未成年だったときに、データ管理者がサービス提供に関連して収集した個人データは、できる限り早く消去しなければならない。当該データを第三者に送信した場合は、データ管理者は合理的な措置をとるとともに、データ主体から削除請求がなされている旨等を当該第三者に伝えなければならない（同条第 2 項）。

個人データが消去されない場合、又は請求から 1 ヶ月以内にデータ管理者から応答がない場合は、データ主体は、CNIL に苦情（réclamation）を申し立てることができる。CNIL は、苦情の申立てを受けた日から 3 週間以内に判断する。

⑤利用制限権（droit à la limitation du traitement）

GDPR 18 条に規定する条件の下で行使される（法 53 条）

利用制限権については、フランス法に固有の規定は置かれていない。

⑥個人データの訂正若しくは削除又は利用の制限に関する義務の通知

GDPR19 条に規定する条件の下で行使される（法 54 条）

⑦データポータビリティ権（droit à la portabilité des données）

GDPR20 条に規定する条件の下で行使される（法 55 条）

データポータビリティ権については、デジタル共和国法 48 条で規定され、消費法典に編纂されていたが（消費法典第 2 編第 2 章第 4 節第 3 款第 4 目「データの回収とポータビリティ（Récupération et portabilité des données）」）、GDPR 準拠法制定に伴い削除された[18]。

アルザス及びモーゼルの商工会議所議員選挙における電子投票システム開設にあたり、データポータビリティ権（削除権、利用制限権及び意義申立て権も）を放棄するアレテ[19]がある。

CNIL は、データポータビリティ権の行使を促進するための方策として、①データ主体が認証されたアカウント/スペースから標準的な機械可読形式（CSV、XML、JSON など）でデータを直接ダウンロードできる機能を提供すること、②許可された第三者（組織またはその他）がデータを自動的に取得する機能を提供すること、③そのための安全な API を提供すること、を提案している[20]。

⑧異議申立て権（droit d'opposition）

GDPR21 条に規定する条件の下で行使される（法 56 条）

ただし、個人データの処理が法的義務を満たしている場合又は GDPR23 条に規定する条件の下で、これらの権利と義務に関する規定の適用が、法律の明示的な条項によって除外される場合には、本条は適用されない。

⑨プロファイリングを含む自動処理に基づく決定をされない権利

個人の行動に関する評価を含む裁判所の決定は、その人の人格の特定の側面を評価することを目的とした個人データの自動処理に基づいてはならない（法 47 条第 1 項）。

個人に関して法的効果を生ずる、又は個人に重大な影響を与えるその他の決定は、その個人に関する特定の個人的側面を予測または評価することを目的としたデータの自動処理のみに基づいて行うことはできない（同法第 2 項）。

ただし、GDPR22 条 2 項 (a) 及び (c) に規定する場合並びに公共行政関係法典 L. L. 311-

---

[18] デジタル共和国法のもとにおいて、すでに、データを送信する権利だけではなく、データを取得する権利についても規定しており、取得データの形式や取得可能性についての情報提供など、サービスプロバイダ等のデータ管理者に課される義務については、2016 年法制定に際してとられたオンライン協議プロセスにおいて、事業者等も関与しながら活発に議論された。

[19] Arrêté du 25 septembre 2021 portant création d'un système de vote électronique en vue des élections des membres des chambres de métiers d'Alsace et de la Moselle devant se dérouler du 1er octobre au 14 octobre 2021

[20] CNIL, « Professionnels : comment répondre à une demande de droit à la portabilité ? », 7 avril 2021, https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-la-portabilite

3-1 条及び第 4 編第 1 章第 1 節に基づいて行われた個別の行政上の決定で、その処理が情報と自由法第 6 条 I に記載するデータ（いわゆるセンシティヴデータ）に関わらない場合は、適用しない。これらの決定に関して、データ管理者は、処理がどのように実装されたかをデータ主体に詳細かつわかりやすい形式で説明できるように、アルゴリズム処理とその展開を確実に制御する。

情報と自由法第 6 条 I に規定する特別なカテゴリーの個人データに基づく自然人に対する差別をもたらすプロファイリングは禁止される（法 95 条第 3 項）。なお、情報と自由法第 6 条 I は、GDPR9 条 1 項に対応している。

⑩集団訴訟

フランスでは、2014 年に、消費に関連する 2014 年 3 月 17 日の法律第 2014-344 号によって初めて集団訴訟が法的救済手段の一つとして導入された。そして、2018 年法では、GDPR 違反の損害賠償請求（GDPR82 条）につき、集団訴訟の道を開いた。同様の状況に置かれた複数の自然人が、個人データ管理者またはその下請け業者の GDPR 違反または GDPR と性質を同じくする法律の規定違反を共通の原因として損害を被った場合、違反状態の解消または損害賠償（精神的損害の賠償を含む）を求めて、管轄権を有する民事裁判所または行政裁判所に集団訴訟を提起することができる。原告適格は、私生活の保護または個人データの保護を目的とすることを少なくとも 5 年間定期的に宣言している団体、個人データの処理が消費者に影響を与える場合には、消費法典に基づき承認された全国を代表する消費者保護団体、および、個人データの処理が国民の利益や公務員の権利義務に関する場合には、労働法典に規定する従業員または公務員の労働組合に認められる。

（6） 情報銀行、PDS

CNIL が 2013 年 8 月に取りまとめた IP（innovation and foresight）レポートは、イギリスの MiData、フランスの MesInfos[21]に言及し、顧客と企業との間でデータを相互に共有することに、新たなイノベーションの道を見出している。また、PDS の具体例としては、MyDex, Privowny, personal.com を挙げている。個人が消費者データを「再利用」する方法としては、自分の移動や二酸化炭素排出量から、消費に対して環境に配慮した対応について考える、といった例が示されている（Daniel Kaplan）。他方で、一回の簡単な同意で、あらゆる企業が保有する取引データにアクセスできるようになると、個人のアクセス権を一種の一般化されたオープンデータに変換することになりかねない、といった懸念も示されている（Meryem Marzouki）[22]。

医療データに関しては、これを公益のために利用するという観点から、2016 年 1 月に

[21] 野村敦子「個人起点のデータ流通システムの形成に向けて ―イギリスの midata の取り組みから得られる示唆―」JRI レビュー9 巻 70 号（2019）199-201 頁

[22] CNIL, PRIVACY TOWARDS 2020 EXPERT VIEWS, aug 2013, pp.16-17.

医療システムを近代化するための法律により National Health Data System（SNDS）が設立された。SNDS は、公的機関によって収集された匿名化された健康情報を収集し、公益目的の調査、研究および評価のための利用を促進するためのシステムで、健康保険データ(SNIIRAM データベース)、病院データ(PMSI データベース)、医学的死因(Inserm の CépiDC データ)、障害関連データ（MDPH-CNSA データ)および補完的な健康保険組織からのデータのサンプルで構成される。公的・私的、営利・非営利を問わず、あらゆる個人・法人は、保健政策の実施、健康および医療社会的ケアの分野における革新等、公益に関する調査、研究、評価を実施する目的で、CNIL の許可を得て、2017 年 4 月から SNDS データにアクセスできる。

さらに、健康データについては、医療システムの組織化と変革に関する 2019 年 7 月 24 日の法律によって、健康データを共有するためのプラットフォームである Health Data Hub が設立された。主な目的は、国民の医療データを一元化して管理したうえで、研究者や企業によるそのデータへのアクセスを容易にし、データの利活用を促進することにある。フランスには、SAFARI 事件以降、データの集中管理／一元管理に対する拒否反応が強かったことから、健康データに特化しているとはいえ、一元管理を可能にしたのは、大きな転機といえる。

（7） 個人情報保護法を執行する監督機関の組織と権限

情報と自由法制定の目的の一つは、個人情報保護のための独立行政機関を創設することであった。今日では、GDPR 上の独立監督機関としても機能しており、データ保護基準・行動規範等の規則制定権、議会による諮問への答申（法 8 条Ⅰ)、データ処理者・下請け業者に対する立入調査、勧告、警告、許可等の取消し、命令（データ処理の適正化・停止等)、急速審理の申立て、制裁金の賦課等（法 19 条－23 条)、苦情処理の権限を有する。

以下では、GDPR 違反に対する制裁の概略について説明する。

CNIL の委員長は、想定されるデータ処理が GDPR に違反するおそれがあるという事実について、データ管理者又はその下請け業者に警告する（avertir）ことができる（法 20 条Ⅰ)。データ管理者又は下請け業者が、GDPR 又はこの法律に基づく義務を遵守していない場合、委員長は、期限を定めて、命令する（mettre en demeure）ことができる（同Ⅱ)。それでも是正されない場合は、罰金、許可・認証等の取消、就業規則を承認する決定の停止等の制裁を課す（同Ⅲ)。

情報と自由法 1 条に規定する権利や自由が重大かつ即時に侵害された場合は、権利と自由を保護するために必要なあらゆる措置を求めて、急速審理手続を裁判所に申立てることができる。必要に応じて罰則を求めることもできる（法 21 条Ⅳ)。

CNIL は、違反行為を検察官に告訴する権限も有しており（法 8 条Ⅰ)、刑事罰を科す場合は、そこから行政刑罰として科された金額を差し引くことができる。

3. 研究・医薬品開発を目的とした診療データの二次利用

健康データとは、「医療サービスの提供を含め、本人の健康状態に関する情報を明らかにする、自然人の身体的又は精神的な健康に関連する個人データ」と定義されている（GDPR4条15号）。診療データは、これに含まれる。「健康データ」はセンシティヴデータにあたるため、原則として、データ処理は禁止されるが（GDPR9条1項）、データの利用について本人の同意がある場合のほか、予防医学、健康・社会ケア治療の提供等に必要な場合、公衆衛生分野における公益のために必要な場合など、本人の同意なくしてデータ処理が例外的に認められる場合もある[23]。

情報自由法は、健康データの処理は、公益目的を考慮する場合にのみ実施できるとしており（66条第1項）、公益目的かどうかの認可権限はCNILにある。さらに、個人の自由や権利にとって「ハイリスク」な処理の場合、データ管理者はデータ保護影響分析を実施しなければならない（法90条）。医薬品開発などの研究目的で利用する場合には、公益目的と評価されるとしても、情報自由法の枠内で利用することになるため、データ主体の同意は原則として要請される。

より厳密には、診療データの利用に必要な手続き上の要請は、二段階で検討されなければならない。第一に、データウェアハウスの構築に関するルール、第二に、同一のデータ管理者又は他の組織によってウェアハウスに保存されたデータを使用して実施される調査、研究、または評価プロジェクトの実施に関するルールである[24]。

また、データ主体である患者以外の者から間接的に収集する場合の情報提供については、特に、科学研究目的で処理する場合にまで患者本人の同意を要するとすると、不相応な労力を強いることになるため、データ管理者において、情報を一般に公開する（例: Web サイトで公開される一般情報）など、データ主体の権利、自由、正当な利益を保護するための適切な措置を講ずればよいとされる。

以上

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

[23] 宮下紘『EU一般データ保護規則』（勁草書房、2018年）74頁参照。

[24] CNIL, Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ?, 2 mars 2023. CNIL, Quelles formalités pour les traitements de données de santé à caractère personnel ?, 8 janvier 2018.

Ⅴ. Thailand

Report on Right to Informational Self-Determination under Thai Law

Thitirat Thipsamritkul[1]

1. The Relationship between Constitutional Law and Personal Data Protection Law

1.1 Constitutional Status of the Right to Privacy or the Right to Informational Self-Determination

The terms "privacy" did not appear in the text of Thailand's constitution[2] until the 15th Constitution B.E. 2534 (1991), Section 44, *"A person's family rights, dignity, reputation or the right of privacy shall be protected."* Before that, there were only the protection of secrecy in communications and the right to family in the Constitution B.E. 2492 (1949).

The similar provision with Section 44 under Constitution B.E. 2534 (1991) appeared again with the clause prohibiting the circulation of image or statement that violate privacy was included in the following Constitution B.E. 2540 (1997), so called "the people's constitution".[3] The protection against unlawful exploitation of personal information was also added¥ in the Constitution B.E.2550

---

[1] Lecturer at Faculty of Law, Thammasat University, served as consultant to the Drafting Committee for Personal Data Protection Bill in 2019, and was selected Member of Personal Data Protection Commission (withdrawn later). Some parts of information in this report were gained from the author's own experience.

[2] Since the democratic revolution in B.E. 2475 (1932), there has been 20 Constitutions in Thailand including the temporary Constitutions. The main reasons for these changes were 13 military coups. The chapter of fundamental rights remains in similar structure and have evolved overtime. Distinctively, the Constitution B.E. 2540 (1997) was the only one called "people's constitution" since it was drafted by civilian government with a broad civic participation.

See more, Andrew James Harding , Rawin Leelapatana, "Constitution-Making in 21st-Century Thailand:The Continuing Search for a Perfect Constitutional Fit", The Chinese Journal of Comparative Law, Volume 7, Issue 2, September 2019, Pages 266–284, https://doi.org/10.1093/cjcl/cxz009.

[3] Thailand Constitution B.E.2540 (1997), Section 34.

A person's family rights, dignity, reputation or the right of privacy shall be protected.

The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which is beneficial to the public.

(2007).[4]

The current Constitution B.E. 2560 (2017) maintains similar protection but the restriction to such right is expanded to include personal information in general.

> *"**Section 32.** A person shall enjoy the rights of privacy, dignity, reputation and family.*
>
> *An act violating or affecting the right of a person under paragraph one, or an exploitation of personal information in any manner whatsoever shall not be permitted, except by virtue of a provision of law enacted only to the extent of necessity of public interest."*

This change reflects the broader understanding of personal data in modern day that goes beyond image and statement. It is worth to note that the drafting of this constitution was done in parallel with the initiative to introduce a set of new digital economy law including the Cyber Security Bill and the Personal Data Protection Bill.

Constitution B.E. 2534 (1991)	**Constitution B.E. 2540 (1997)**	**Constitution B.E. 2550 (2007)**	**Constitution B.E. 2560 (1997)**
Simple recognition of the right to privacy in separation from the liberty of dwelling	Recognition of right to privacy + Prohibition of the circulation of image or statement that may violate privacy.	Recognition of right to privacy + Prohibition of the circulation of image or statement that may violate privacy. + Protection against unlawful exploitation of data	Recognition of right to privacy + General prohibition of unlawful processing of personal information.

Generally, In Thai law, the right to privacy is not interpreted to be different from the right to informational self-determination. There are also other provisions that relate to right to privacy in the

[4] Thailand Constitution B.E.2550 (2007), Section 35.

A person's family rights, dignity, reputation and the right of privacy shall be protected.

The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which is beneficial to the public.

A person shall be protected from the unlawful exploitation of personal information in relation to oneself as provided by law.

classic sense, such as the liberty of dwelling.[5]

Apart of the constitutional protection, the Civil Code[6] and the Criminal Code[7] have always prescribed the tort liability. It is general understanding that these provisions include the infringement of privacy but both Civil and Criminal Code impose the burden of proof on data subjects.[8] There were very few court cases referred to the right to privacy or privacy. The most well-known civil case is the supreme court judgment No.4893/2558[9] referring to the right to privacy under both B.E.2540 (1997) and B.E. 2550 (2007) Constitutions that must not be violated by mass media.

1.2 Constitutional Significance of the Personal Data Protection Law

The main purpose of Personal Data Protection Act (PDPA) is to protect rights. It also includes the clause providing basis for processing of personal data which is explained as restriction of fundamental rights under constitutional law, provided by Section 26.[10] Therefore, the following preamble of PDPA specifically referred to section 32 of the B.E.2560 (2017) Constitution that guarantee the right to privacy.

> *"This Act contains certain provisions in relation to the restriction of rights and freedom of a person, which section 26, in conjunction with section 32, section 33 and section 37 of the*

---

[5] Thailand Constitution B.E.2560 (2017)

Section 33. *A person shall enjoy the liberty of dwelling.*

Entry into a dwelling without the consent of its possessor or a search of a dwelling or private place shall not be permitted, except by an order or a warrant issued by the Court or where there are other grounds as provided by law.

[6] Civil Code, Section 420, 422, and 423.

[7] Criminal Code, Section 326-333.

[8] Janjira Iammaruya, 'Laws relating to Personal Information in Thailand' in the Research Report submitted to the Official of Information Act (2003), p 6 [in Thai].

[9] Supreme Court Judgment No.4893/2558, 11 May 2015.

[10] Thai Constitution B.E. 2560 (2017)

*"**Section 26.** The enactment of a law resulting in the restriction of rights or liberties of a person shall be in accordance with the conditions provided by the Constitution. In the case where the Constitution does not provide the conditions thereon, such law shall not be contrary to the rule of law, shall not unreasonably impose burden on or restrict the rights or liberties of a person and shall not affect the human dignity of a person, and the justification and necessity for the restriction of the rights and liberties shall also be specified.*

The law under paragraph one shall be of general application, and shall not be intended to apply to any particular case or person."

Constitution of the Kingdom of Thailand so permit by virtue of the law.

The rationale and necessity to restrict the rights and freedom of a person in accordance with this Act are to efficiently protect personal data and put in place effective remedial measures for data subjects whose rights to the protection of personal data are violated. The enactment of this Act is consistent with the criteria prescribed under section 26 of the Constitution of the Kingdom of Thailand. "

The reference to Section 26 reflects the preamble of PDPA also refers to the liberty of dwelling under Section 33, and the right to property in Section 37.[11] The reference to the right to property reflects the idea that sees ownership of data as part of economic rights.

It is common for Thai legislators to include a remark at the end of an act to briefly remind the main research of lawmaking. The PDPA has the following remark.

"The reason to enact this act is that there have been so many violations of rights to privacy in relation to personal data protection that caused suffering and damages to data subjects. Moreover, the advance of technology has enabled and accelerated the collection, use or disclosure of personal data that may amount to such violations and eventually caused damage to the economy. Therefore, it is necessary to issue a law protecting personal data in general to set rules, mechanisms or measures regulating the use of personal data."

This remark reflects both the importance of privacy rights and economic incentives that Thai lawmakers had in mind. Scholarly work uniformly mentioned PDPA as protecting right to privacy.

2. The Overview of Personal Data Protection Law

2.1 The Influence of other countries' legal systems

Influence on legislations before PDPA

Following the global trend of anti-corruption, governmental transparency and the rise of media freedom, the Official Information Act B.E.2540 (1997) was enacted to enhance the people's right to access government information. Chapter 3 of this legislation contains provisions on personal information protection. The principles of necessity, purpose limitation, direct collection of data, and

[11] Thai Constitution B.E. 2560 (2017)

"***Section 37.*** *A person shall enjoy the right to property and succession.*

The extent and restriction of such right shall be as provided by law. …."

transparency were presented. The following Credit Information Business Act B.E.2546 (2003), which contains more detailed provisions of personal data protection, was influenced by both the UK Data Protection Act 1998 (which follows European Union Directive 95/46/EC) and the US Fair Credit Reporting Act 1970, even though these two models have different principles and legislation styles, especially regarding data subject consent.[12]

Personal Data Protection Act (PDPA)

The attempts to draft and pass personal data protection law started right after the enactment of the Official Information Act B.E.2540 (1997).[13] The early versions of PDPA draft were influenced by legislations of different countries including EU, UK, Australia and Singapore. The drafting work was initiated by the Office of Official Information and the National Electronics and Computer Technology Center (NECTEC).

However, after the 2014 coup d'état, the military government declared 'Thailand 4.0' policy that led to the digital economy law reform.[14] Following with the amendments of copyright laws, electronic transactions, computer crime and telecommunication regulations, the drafting of cybersecurity bill and personal data protection bill was carried out by the collaboration between the Electronic Transaction Development Agency (ETDA) and the Ministry of Digital Economy and Society (MDES).

In 2017, three years after the 2014 military coup, following the controversial referendum that gave birth to the new Constitution B.E. (2560) 2017, the military amended the Computer Crime Act B.E. 2550 (2007) amidst the widespread resistance from academic community, civil societies, and general citizens. The amendment was domestically and internationally criticized for persisting oppression of online freedom, allowing arbitrary enforcement, and induced self-censorship amidst the

---

[12] Chalaware Chusap, *Problems of the application of The Credit Information Business Act 2002: Study on the issue of data suject's consent* (Thammasat University Master of Law Thesis, 2009). [in Thai]

[13] Nakorn Serirak, *Privacy*, (Faham Publishing 2nd edn, 2020), p 265-289. [in Thai]

[14] Rumana Bukht & Richard Heeks, 'Digital Economy Policy: The Case Example of Thailand', Paper No. 7 Development Implications of Digital Economies**,** 2018, p 12-13 <https://diode.network/publications/>.

overdue promise of a democratic election.[15] At that time, the Cybersecurity Bill was seen as another tool for the government to intrude on people's privacy as similar legislations do in other countries.[16]

> "*Growing public backlash against the bill is causing tremors both online and offline because of concerns over the abuse of power and data privacy breaches. The bill has been condemned as too far-reaching, impossible to implement and potentially infringing on individual and juristic person rights."*[17]

With this background, the demand that the Cybersecurity Bill must be considered together with the Personal Data Protection Bill became the main narrative. Therefore, both ETDA and MDES tried to engage more with civil societies in revising the draft of both laws. The fact that GDPR came into force in 2018 hugely influenced the drafters at ETDA, MDES and the Council of State to change the personal data protection bill from structure and principles.[18] Dr. Pichet Durongkaveroj, the Minister of Digital Economy and Society in the first cabinet of the military government referred to the enforcement of GDPR as an important push for Thailand to accelerate its drafting process of the personal data protection bill in order to enable its participation in the global digital economy.[19]

---

[15] 'Thailand passes amendment to cyber law despite opposition' (Reuters, 16 December 2016) <https://www.reuters.com/article/us-thailand-cyber-idUSKBN14513I> ; Danny O'Brien and Gennie Gebhart, 'The Amended Computer Crime Act and the State of Internet Freedoms in Thailand' (Electronic Frontier Foundation, 21 December 2016) <https://www.eff.org/deeplinks/2016/12/amended-computer-crime-act-and-state-internet-freedoms-thailand> ; Article19, *Thailand Computer Crime Act 2017: Legal Analysis*, (Article19, 2017) <https://www.article19.org/data/files/medialibrary/38615/Analysis-Thailand-Computer-Crime-Act-31-Jan-17.pdf>.

[16] 'Thai proposal for all-powerful cyber agency alarms businesses, activists'(Reuters, 16 November 2018) <https://www.reuters.com/article/us-thailand-cyber-idUSKCN1NL0JP>. See also, 'Deputy PM insists cyber security bill still subject to change' (National News Bureau of Thailand, 17 October 2018) <https://thainews.prd.go.th/en/news/detail/WNPOL6110170010018>.

[17] 'The Cybersecurity Balancing Act: A draft law is positioned to give the state unprecedented power over the digital arena' (Bangkok Post, 22 October 2018) <https://www.bangkokpost.com/thailand/politics/1562230>.

[18] 'Thailand: MDES publishes revised draft data protection bill' (Data Guidance, 26 February 2018) <https://www.dataguidance.com/news/thailand-mdes-publishes-revised-draft-data-protection>.

[19] The Nation, "Government Fast Tracks Personal Data Protection Law", 18 May 2018, https://www.nationthailand.com/in-focus/30345749 .

GDPR influence via academic guideline

"Thailand Data Protection Guideline (TDPG) 1.0",[20] an academic-led guideline produced in collaboration with law firms and business in digital and banking sectors, embraced EU principles and other international data protection practices. Though some companies did express worries that GDPR would require too high standards for Thai business, the TDPG 1.0 became a reference for lawyers who helps Thai businesses that transact with European companies to comply with GDPR and prepare the domestic-focused business to be ready for the new personal data protection bill.

The National Legislative Assembly's commission[21] that reviewed the personal data protection bill (together with the cybersecurity bill) also took TDPG 1.0 as a reference and referred several times to the possibility of Thailand being included in the EU's "whitelist". Moreover, civil societies also supported the GDPR model since it is seen to protect privacy rights more than the previous drafts and have the potential to stop the abuse of personal data by governmental agencies since it applies to both private and public organizations.

The final version of PDPA followed important principles of GDPR. Research and statistic purpose was added as an additional lawful basis. A similar set of data subject rights was included except for the right to intervene in automatic decisions. Unlike GDPR, criminal punishment was also introduced despite the fierce disagreement from academics. This later caused unnecessary misunderstanding about PDPA and contributed to the delay in enforcement.[22]

Between the push to follow international practice and the local pull to be exempted

It is evident that PDPA was motivated by economic appetite following GDPR and other high-income countries' practices. The privacy rights-friendly reputation of GDPR also allowed MDES to respond to the backlash from the Computer Crime Act amendment and avoid criticism against the Cybersecurity Act.

However, Section 4 of PDPA provided broad exemptions for various governmental entities that may dilute these advantages. The drafting of new law tends to include the exemption of PDPA. The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566

---

[20] Piyabutr Boonaramruang et al, Thailand Data Protection Guideline 1.0 (Chulalongkorn University Press, 2018) [in Thai]. The author of this report is also part of this academic group.

[21] The National Legislative Assembly is body appointed by the military government after the 2014 coup that functions as legislative branch.

[22] Various organizations tried to debunk the misunderstanding. For example [in Thai]; university <https://www.chula.ac.th/news/75005/>, 'CoFact' a fact-checker agency <https://blog.cofact.org/digital-thinkers22/ >, consultation provider <https://pdpathailand.com/knowledge-pdpa/7things-misleading-about-pdpa/ >.

(2023), include Section 12[23] that exempts obligations under the Personal Data Protection Act (PDPA) for this purpose of data processing. This is clearly the case where Thai officials saw PDPA and other personal data protection laws, including the Official Information Act, as obstacles to pursuing public interest such as cybercrime and scam prevention, even though PDPA provides clear lawful basis for authorities to process personal data protection for public tasks prescribed by law. Many scholars and civil societies are worried that this general exemption may be abused to collect more information of citizen without means to oversee the processing data by authorities. The principle of transparency is hugely compromised in this context since it involves the personal data processing by the two data-intensive industry; banks and telecommunications.

In June 2023, the interim cabinet approved a new decree that exempts more governmental entities and exempts private sectors from several duties of data protection when providing personal data to comply with governmental requests, such as the Anti-Corruption related request.[24] This new decree was issued under the open language of PDPA Section 4(2) provision that allows for the expansion of exemptions by the executive branch without the parliamentary check.

> *"The exceptions to apply all or parts of the provisions of this Act to any Data Controller in any manner, business or entity, in a similar manner to the Data Controller in paragraph one, or for any other public interest purpose, shall be promulgated in the form of the Decree."*

This increase and expansion of exemption is expected to cause chaos in private companies' data governance systems and obviously derails Thai PDPA from GDPR model. This may also result in lower level of constitutional protection for the right to privacy. However, it is unlikely to see a strategic litigation that challenges the constitutionality of such exemptions in the Constitutional Court. The legal text of Section 32 of Constitution B.E. 2560 (2017) would allow the interpretation that such exemption would probably be explained as falling into "public interest". A lot of civil societies are afraid that if such decision is to be made, it will set the precedents for governmental agencies to expand more exemptions.

2.2 Definition and Scope of "personal data"

[23] *Section 12. The disclosure, exchange, access as well as the storage, the collection, or the use of personal data under this Royal Decree is not under the enforcement of personal data protection law. However, the person who receives or possesses data may not disclose this personal data to those who have no related duties.*

[24] Royal Thai Government, Press Release 11 July 2023, at https://www.thaigov.go.th/news/contents/details/70221

The scope of "personal data" is defined by Section 6 of PDPA as follow.

> *"Personal Data" means any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular"*

Under the Official Information Act, "Personal Information" is defined as follow.

> *"personal information" means "an information relating to all the personal particulars of a person, such as education, financial status, health record, criminal record or employment record, which contain the name of such person or contain a numeric reference, code or such other indications identifying that person as fingerprint. tape or diskette in which a person's sound is recorded, or photograph, and shall also include information relating to personal particulars of the deceased."*

Comparing to the Official Information Act, the PDPA has a broader definition, though exclude the deceased person's data. The inclusion of indirectly identifiable data expands the scope of protection. This broad definition includes cookies and other online identifiers. It is generally viewed that processing cookies and other online identifiers requires some assessment and measures under PDPA personal data protection measures.[25]

2.3 The Rights of Data Subjects and the Obligations of those who process personal data

The protection of data subjects' rights in PDPA is much more comprehensive manner, especially comparing with mechanism under Official Information Act where the committee has very limited power in enforcement. The list of data subjects' rights are right to be informed,[26] right to access,[27] right to rectification,[28] right to erasure,[29] right to restrict,[30] and right to data portability.[31]

---

[25] Piyabutr Boonaramruang et al, *Thailand Data Protection Guideline 3.0* (Chulalongkorn University Press, 2020), p 85 [in Thai].

[26] PDPA Section 25 and 27.

[27] PDPA Section 30.

[28] PDPA Section 35.

[29] PDPA Section 33.

[30] PDPA Section 34.

[31] PDPA Section 31.

The list is similar to GDPR, except that data subject does not have right not to be subject to automated individual decision-making, including profiling under the PDPA.

a) The right to erase personal data or the right to cease utilization

The right to erase, destroy and anonymize personal data or to is included in Section 33 of PDPA. This right can be invoked when (1) the necessary purposes ceased to exist, (2) the consent is withdrawn, (3) when the data subject successfully objected that the data processing lacked the lawful basis of a public task or legitimate interest, or (4) when the data was processed unlawfully. PDPA obliges the data controller to act when the data was disclosed to the public and to inform other relevant data controllers.

The right to restrict the use of personal data is also included in Section 34 of PDPA.[32] This right is expected to be invoked as a temporary measure before the data subject or data controller pursues other action.

b) The Status and Significance of Consent in Personal Data Protection Law

[32] ***Section 34.*** *The data subject shall have the right to request the Data Controller to restrict the use of the Personal Data, where the following applies:*

(1) when the Data Controller is pending examination process in accordance with the data subject's request pursuant to section 36;

(2) when it is the Personal Data which shall be erased or destroyed pursuant to section 33 (4), but the data subject requests the restriction of the use of such Personal Data instead;

(3) when it is no longer necessary to retain such Personal Data for the purposes of such collection, but the data subject has necessity to request the retention for the purposes of the establishment, compliance, or exercise of legal claims, or the defense of legal claims;

(4) when the Data Controller is pending verification with regard to section 32 (1), or pending examination with regard to section 32 (3) in order to reject the objection request made by the data subject in accordance to section 32 paragraph three.

In the event that the Data Controller does not take action in accordance with paragraph one, the data subject shall have the right to complain to expert committee to order the Data Controller to take such action.

The Committee may prescribe and announce rules regarding the suspension of use in accordance with paragraph one.

Section 24 of Thailand's PDPA integrates the necessity principle and prescribes 7 grounds for lawful and fair processing[33] for legitimate purposes, which are consent, historical archive and research/statistic,[34] vital interest, contractual obligation (or to enter into contract), public task or official authority, legitimate interest,[35] and legal obligations of data controller.

Except for the ground of historical archive and research/statistic which must be conducted in accordance with the later announced rules of Data Protection Committee, other 6 grounds are almost identical to GDPR. Despite the acknowledgement of drafting commission that consent cannot be and should not the only main ground considering current digital environment, unlike GDPR, the ground of consent is written as general principle and other grounds are put as exceptions. This was a default formula of law-drafting insisted on by the Council of State. It is no surprise that this provision has led to the over-prioritization of consent in practice.

Reading together with the drafting history and taking into consideration other related provisions that clearly did not put consent as the primary ground of processing,[36] consent is only required when the main grounds cannot be relied on. The main grounds are "contract" in normal business operation, "public task/official authority" in normal governmental operation, and "legal obligations" in both contexts. Like GDPR, consent is not the best ground for data controllers to rely on since Section 19 requires several strict conditions that prioritize data subjects' autonomy and rights to control their data. Since opt-in consent is required and data subjects can withdraw consent in most circumstances, "legitimate interest" is a more practical ground.

In conclusion, "consent" is suitable for marketing purposes and additional services. It shall not be relied on in normal operations. However, many data controllers are still confused that "consent"

---

[33] The term used in Section 24 is "collection". However, taking into consideration the context of other provisions that linked to the grounds specified in Section 24, this provision shall be read to cover all data processing activities, including using, disclosing, storing and deletion.

[34] Nevertheless, Section 9 of the National Health Act B.E. 2550 (2007) requires consent for the use of medical service receiver as subject of experiment. Reading in conjunction with Section 3(1) of PDPA, consent remains a lawful basis for medical experiment. Other sectoral regulators may also set similar conditions in addition to PDPA.

[35] Though the term used in Thai is "lawful interest", the preparatory work and followed description by the PDPC and other experts show that it is equivalent to "legitimate interest" of GDPR.

[36] Piyabutr Boonaramruang et al, *Thailand Data Protection Guideline 3.0* (Chulalongkorn University Press, 2020) p 65-94 [in Thai].

is required for most situations. This myth came from different reasons such as the reference to consent in previous laws both that related [37] and not directly related to data protection, [38] and the miscommunication by officials during the launch of PDPA in June 2022.

The disclosure of personal data to the third parties does not require consent if such disclosure was necessary for the initial scope of processing purposes. Section 23 and 25 requires a proper notice, while Section 27 and 39 requires the record of such disclosure.

c) The Limit of the Notice and Consent model and the countermeasure

The requirement of valid consent under Section 19 addresses some of the limitations of the self-management model due to limited human cognitive abilities. It follows GDPR to demand that.

> *"Such request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an easily accessible and intelligible form and statements, using clear and plain language, and does not deceptive or misleading to the data subject in respect to such purpose."*

Section 19 also grants discretion to the PDPC to prescribe standard forms and wordings for data controllers to use when obtaining consent. However, the PDPC did not issue a standard form by itself but referred to compulsory standard forms under other laws which prescribe additional duties to data controllers according to Section 3. [39] It has also recommend data controllers follow some

---

[37] For example, Credit Information Act B.E. 2550 (2007).

[38] For example, patient's informed consent for medical service and research in National Health Act B.E. 2550 (2007), parents' consent for private transaction by minors in the Civil Code.

[39] Section 3 prescribes the overlapping with other laws as follows.

"In the event that there is any sector-specific law governing the protection of Personal Data in any manner, any business or any entity, the provisions of such law shall apply, except:

(1) for the provisions with respect to the collection, use, or disclosure of Personal Data and the provisions with respect to the rights of data subjects including relevant penalties, the provisions of this Act shall apply additionally, regardless of whether they are repetitious with the above specific law;

(2) for the provisions with respect to complaints, provisions granting power to the expert committee to issue an order to protect the data subject, and provisions with respect to the power and duties of the Competent Official, including relevant penalties, the provisions of this Act shall apply in the following

voluntary standard forms existing in industries and also comply with the PDPC guideline issued on September 7, 2022.[40] This guideline offers similar suggestions to the European Data Protection Board's guidelines and Thai scholars' guidelines called TDPG 3.0. Another PDPC's guideline on notice issued on September 7, 2022, also follows GDPR and ICO's recommendations.[41] Though these guidelines do not have legal binding power, the Expert Committee and Courts are expected to take them into consideration when interpreting the law.

The use of patient medical record or biometric data for research purposes or drug development

Section 24 of PDPA prescribes historical archive and research/statistic as a separate legal basis for processing general personal data (non-sensitive data).[42] Not many relies to this lawful basis since its interpretation direction is not known. There is no specific guidelines issued on the safeguard measure from the PDPC yet.

Section 26, which governs sensitive data, including medical record or biometric data, also provides exception of strict consent conditions, mostly relating to medical profession, health care and welfare arrangements. Similar to Article 9(2)(i) of GDPR, Section 26(5)b[43] provides the legitimate

---

circumstances:

(a) in the event that such law has no provision with respect to complaints;

(b) in the event that such law has the provisions giving the power to the competent official, who has the power to consider the complaints under such law, to issue an order to protect the data subject, but such power is not equal to the power of the expert committee under this Act; and either the competent official who has power under such law makes a request to the expert committee, or data subject files a complaint with the expert committee under this Act, as the case may be."

[40] Available [in Thai] <https://www.mdes.go.th/uploads/tinymce/source/สคส/แนวทางการดำเนินการในการขอความยินยอมฯ.pdf>.

[41] Available [in Thai]<https://www.mdes.go.th/uploads/tinymce/source/สคส/แนวทางการดำเนินการในการแจ้งวัตถุประสงค์ฯ.pdf>.

[42] Nevertheless, Section 9 of the National Health Act B.E. 2550 (2007) requires consent for the use of medical service receiver as subject of experiment. Reading in conjunction with Section 3(1) of PDPA, consent remains a lawful basis for medical experiment. Other sectoral regulators may also set similar conditions in addition to PDPA.

[43] **Section 26.** Any collection of Personal Data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the Committee, is prohibited, without the explicit consent from the data subject, except where;

aim to use health data for public health interest defined by law. That means the patient's consent is not required for research project that is conducted under a specific law. The members of PDPC also recognized that this may create undue disadvantages for private research institutes since they can only rely on patient's consent to conduct research that are not in a collaboration with government agencies. In any event, the duty to anonymize or pseudonymize data is not directly required by PDPA but maybe required by other profession ethics or other regulations related to medical and research professions.

The sub-paragraph (e) of the Section 26(5) also provides public interest defined by law as another exemption of consent; *"the substantial public interest by providing the suitable measures to protect the fundamental rights and interest of data subject."*

The obligation to provide "suitable measures" in each sub-paragraph reflects the attempts to balance between the public interest that may be gained from personal data processing and its effects on individual data subjects' rights and freedom.

d) Devices or architectures such as a Personal Data Store (PDS) to assist with the person's controllability of their personal data

There are no specific provisions relating to devices or architectures such as a Personal Data Store (PDS) being utilized to assist with the person's controllability of their personal data. Such utilization is not prohibited.

This topic has not been widely discussed in Thailand. Such utilization may be done with "contract" or "legitimate interest" as a lawful basis under Section 24 of PDPA. The operator of such PDS shall be considered data the controller. The processing of sensitive data shall be subject to stricter conditions under Section 26 of PDPA.

e) Profiling regulations

There is no specific provision prescribing the right to object profiling as provided in GDPR,

---

(5) it is necessary for compliance with a law to achieve the purposes with respect to;

(b) public interest in public health, such as protecting against cross-border dangerous contagious disease or epidemics which may be contagious or pestilent, or ensuring standards or quality of medicines, medicinal products or medical devices, on the basis that there is a provision of suitable and specific measures to safeguard the rights and freedom of the data subject, in particular maintaining the confidentiality of Personal Data in accordance with the duties or professional ethics;

Article 21. However, this topic has been discussed before and after the enactment of PDPA such as in the discussion of Data Protection Impact Assessment (DPIA) and the guidelines for marketing department in TDPG 3.0.[44] If the profiling increases the risk to data subjects, the data controller shall adopt some measures to safeguard data subjects and record the impact assessment to prove its good faith. The data subject may also invoke the right to access and the right to restrict against the data controller to retrieve the transparency of profiling process and object the unfair use of their personal data.

f) The right to data portability or the right to transmit personal data (e.g., GDPR Article 20) And in what situations are these rights implemented in practice?

Section 31 prescribes the right to access and receive his/her own personal data from the data controller. The right to data portability is included in Section 31 (2) PDPA as follow.

> *(2) request to directly obtain the Personal Data in such formats that the Data Controller sends or transfers to other Data Controllers, unless it is impossible to do so because of the technical circumstances.*

The National Legislative Assembly's commission discussed this provision at length in the draft reviewing process. Many representatives from public sectors consider this right as enabling open government initiatives rather than seeing it as facilitating market competition as seen in countries. In contrast to such intention of the drafters and commentators at the lawmaking process, PDPA has been referred to on many occasions as a primary obstacle to the open data initiatives.

The implementation of this right has not yet been seen in practice. It is unlikely that a complaint based on this provision will be successful since this right is conditioned with the technical circumstances that data controller may easily prove to exist.

2.4 Organization and authority of the supervisory body enforcing personal data protection law. Sanctions and complaint mechanisms.

Organization Structure and relation with government

The Personal Data Protection Commission (PDPC) is the principal supervisory body enforcing PDPA. The qualified members of this commission must be selected by an independent Select Committee, which is appointed by the Prime Minister, the President of the Parliament, the Ombudsman

[44] Piyabutr Boonaramruang et al, *Thailand Data Protection Guideline 3.0* (Chulalongkorn University Press, 2020), p 213-222, p 353-366 [in Thai].

and the National Human Rights Commission. The current members of PDPC are 10 experts in law and related fields, including the health industry, securities exchange, law enforcement and military. Permanent Secretary of MDES, Permanent Secretary of the Office of the Prime Minister, Secretary General of the Council of State, Secretary General of the Consumer Protection Board, Director General of the Rights and Liberties Protection Department, Attorney General and the Secretary General of the PDPC Office serve as ex officio members. The Qualified members of PDPC have 4 years terms and can be appointed no more than 2 terms.[45] The Cabinet can discharge a PDPC member due to his/her actus reus.[46]

Under Thai public law, PDPC has a status of "Independent Administrative Organization". It is a neutral governmental body that may be managed by different rules from normal governmental body and must not be politically interfered.[47] Section 46 of PDPA provides that the government shall provide seed fund and annual budget as proper.

Authority

The PDPC is responsible for overseeing laws relating to personal data protection and making relevant proposals to the Cabinet. PDPC is responsible for planning the promotion and protection of personal data, prescribing guidelines and measures, and issuing various rules, codes and sub-regulations, among others. The PDPC is also responsible for regulating personal data protection in accordance with the policy formulated by the National Committee for Digital Development for Economy and Society and in turn for making the master plan for the Committee.[48] It also has duties to provide advice and collaborate with other governmental agencies, especially those with the power to regulate personal data protection of specific sectors since PDPA adds new standards to apply together with their existing legislations.

Sanctions and Complaints Mechanisms

The PDPC can appoint expert committees to consider complaints, investigate non-compliance and settle disputes, as it sees fit.[49] Currently, it has appointed 2 Expert Committees, one

---

[45] PDPA, Section 12.

[46] PDPA, Section 13.

[47] This categorisation of governmental entity as "Independent Administrative Organization" follows the principles and practice of the Office of the Public Sector Development Commission available [in Thai] at <https://webdev.excise.go.th/act2560/images/files/กฎหมายอนๆ/_แก้ไข_เพิ่มเติม.pdf>. The updated list of each categories can be found at <https://po.opdc.go.th/> [in Thai].

[48] PDPA, Section 16(1).

[49] PDPA, Section 72.

on finance and economic-related complaints, and another one on digital technology-related complaints.

Sections 71-76 of PDPA prescribe a complaint mechanism for data subjects. Complaints can be submitted to the PDPC directly or via email. The template of the complaint requires data subject to clarify whether the complaint(s) has been made to 1) data controller, or to 2) other governmental bodies (expert committee under PDPC, administrative courts or other courts, other governmental bodies).[50] This is consistent with Section 73, paragraph 2 that requires the Expert Committee to consider other complaint mechanisms under other supervisions of other governmental bodies.

> *"The filing, refusal of acceptance, dismissal, consideration, and timeframe for the consideration of the complaints shall be in accordance with the Committee's rule by taking into account the refusal of acceptance of the complaints or dismissal of the matter in the event that there has been the authority to consider such matter under other laws."*

The interpretation of this Section 73, together with Section 3 that prescribes the overlapping issues under different laws, may cause a problem of jurisdiction between the PDPC and other governmental bodies that regulate privacy-related issues over specific sectors such as banking, insurance, telecommunications, etc.

If the complaint cannot be settled, the Expert Committee has the power to order the data controller or the data processor 1) to perform or to rectify, and 2) to prohibit an act or to carry an act to cease damage.[51] In case of failure to comply, the expert committee to proceed further with administrative action[52] and the administrative penalty.[53] The administrative actions include notice, subpoena, investigation, seizure and confiscation. The administrative penalties can be charged a maximum of THB 5,000,000.[54] The objection to the administrative action and penalty can be made to the Administrative Court.[55]

In addition, Section 79-81 of PDPA prescribe criminal penalties of a 1-year sentence maximum and Section 78 also allows punitive damages for not greater than 2 times the actual damages. These provisions open for the Court of Justice (both civil and criminal courts) to decide PDPA-related disputes.

---

[50] See more https://www.mdes.go.th/mission/detail/6408-ประกาศและคำสั่งของสำนักงาน.

[51] PDPA, Section 74, paragraph 3.

[52] PDPA, Section 74, paragraph 4.

[53] PDPA, Section 90.

[54] PDPA, Section 85 and 87.

[55] For more information on Thai Administrative Court system, see also https://www.admincourt.go.th/admincourt/en/structure.php

2.5 Judicial proceedings or judicial remedy

Apart from the administrative sanctions that are the main enforcement measures under the power of PDPC, PDPA also prescribes civil[56] and criminal liability.[57] Data subjects may also submit their complaints to the civil and criminal court. The specific provision of civil liability can be helpful when the data subject discharges the burden of proof.

PDPA does not provide a specific provision on standing or class action. The general principles of Thai procedural laws shall apply.[58] The class action on data breach may fall into the permitted types of case under Thai Civil Procedural Code Section 222/8.[59] However, there are still general doubt about the knowledge of the Court of Justice's judges would be sufficient to tackle technicality matters in the PDPA related disputes.

※*This work was supported by JST [Moonshot R&D][Grant Number JPMJMS2293]*

[56] PDPA, Section 77-78.

[57] PDPA, Section 79-81.

[58] For more information on class action procedure in Thailand, see also Tanaporn Farungsang, 'Summary of Class Action under the Civil Procedure Code' (SEC, 2019) <https://www.sec.or.th/EN/Documents/LawsandRegulations/ClassAction-appendix-EN.pdf.

[59] Thai Civil Procedural Code Section 222/8.

For the following cases where there are numerous members of a class, the plaintiff who is a member of the class may request for a class action:

(1) tort cases;

(2) breach of contract cases;

(3) cases claiming various legal rights such as the law concerning the environment, the protection of consumers, labour, stocks and stock markets, trade competition.

Ⅵ. Taiwan

Research project：Freedom of Mind and Value Co-Creation through Decentralized Data Management— The Taiwan Report

Chien-Liang Lee
Institutum Iurisprudentiae, Academia Sinica, Taiwan

1. The Relationship between Constitutional Law and Personal Data Protection Law

① Constitutional Status of the Right to Privacy or the Right to Informational Self-Determination

(1) The right to privacy or the right to informational self-determination are constitutional rights of Taiwan's Constitution.

There is no explicit stipulation of the right to privacy or informational self-determination in Taiwan's Constitution, which is then recognized and practiced through the constitutional interpretations of the Grand Justices of Judicial Yuan (Taiwan Constitutional Court, hereinafter referred to as TCC).

TCC referred to the right to privacy in Judicial Yuan (J.Y.) Interpretation No. 293 (1992) for the first time. The reasoning of J.Y. Interpretation No. 585 (2004) indicated explicitly that the right to privacy is a fundamental right guaranteed by Art. 22 of the Constitution[1], which covers the protection of personal life and private living space from interference and the autonomy of personal data. According to the holding of J.Y. Interpretation No. 603 (2005), the term "*the right to informational privacy*" or "*the right to personal informational privacy*" was coined, which guarantees the right to decide whether, to what extent, when, in what manner and to whom to disclose the personal data, the right to know and control the use of personal data and the right to rectify the errors in the personal data. Judging from the development of the J.Y. interpretations, the right to privacy defining the autonomy of personal information keeps being adjusted and corrected.

In view of the development of technology, the above protection meaning of the right to informational privacy was later not only inherited but also further extended by the Constitutional Court established in 2022. The Judgment 111-Hsien-Pan-13 rendered by the TCC on August 12, 2022, emphasizes the ex-post right of control, e.g. the right to information privacy guarantees that the affected persons have the ex-ante

[1] Art. 22 of the Constitution: "All other freedoms and rights of the people that are not detrimental to social order or public welfare shall be guaranteed under the Constitution."

right of control to decide whether the data are utilized or not before the utilization of the data and the ex-post right of control during and after the utilization of the data. The affected persons have the ex-post right regarding the personal data collected, processed and utilized with or without their consent under certain prerequisites. In addition, the ex-post right of control includes the right to delete personal data and the right to stop or limit the utilization of personal data.

(2) The right to informational self-determination or the right to privacy

There is no term for informational self-determination in US-American Constitutional Law. It uses the concept of the right to privacy, which covers the protection of the right to informational self-determination. The German Constitutional Court invented the term *the right to informational self-determination* in the Census Judgment of 1983 and derived it from the general personality right and human dignity.

In Taiwan, the TCC has used the term "the right to informational privacy" as an inferior type of the right to privacy and labeled its dimension as the right to informational self-determination. It is especially worth noting that the TCC derives the right to privacy from the ideas that the core values of a free and constitutional democracy are to protect human dignity and respect the free development of personality, so it protects the private sphere of personal life from intrusion and self-determination of personal information (the holding of J.Y. Interpretation No. 603).

Some Taiwanese scholars argue that the right to informational self-determination and the right to informational privacy have different content, character and scope of protection. The former protects the external freedom of personal behaviors, guaranteed as long as the right to dispose of personal information is not externally oppressed, limited or hindered; that is, the consent of the persons concerned exists. The latter protects the flexible space of internal personality formation and attaches more importance to the tight connection between specific personal information and its personality and subjectivity. However, in my opinion, there is no essential difference between the right to informational privacy and the right to informational self-determination. It matters how we interpret the content and the scope of the application. Judging from the interpretations of the Constitutional Court of Taiwan, the term privacy contains the meaning of self-determination. To differentiate between informational privacy and informational self-determination is to restrict the meaning of privacy and self-determination. In this context, the right to informational self-determination shall be included in the scope of the right to informational privacy in this article.

② Constitutional Significance of the Personal Data Protection Law

The Computer Processed Personal Data Protection Act was amended and renamed Personal Data Protection Act.

Taiwan's current Personal Data Protection Act (hereinafter referred to as PDPA) was enacted in 2010, replacing the Computer Processed Personal Data Protection Act of 1995 (hereinafter referred to as CPDPA). The amended articles came into force on October 1, 2012. Neither CPDPA nor PDPA does refer to the right to privacy or the right to informational self-determination. The legislature's explanations of the amended articles frequently refer to "privacy." This shows that the privacy of personal data is a main consideration of PDPA.

Protecting personality right is one of the stated goals of the PDPA. It enriches the interpretation of the personality right when the PDPA contains informational privacy and informational self-determination. According to the CPDPA, the predecessor of the PDPA, the consent of the persons concerned was one of the legal bases of the personal data collection by government agencies and non-government agencies, and the use of the personal data was limited in principle to the original purpose of collection. This shows that the autonomy of personal data took shape at that time. The current PDPA emphasizes informed consent and ensures control by the subjects of personal data. This also reflects the legislative thought that informational self-determination is the principle of the PDPA.

2. The Overview of Personal Data Protection Law

① The Influence of other countries' legal systems

The enactment of the CPDPA, the predecessor of the PDPA, referred to the eight principles of the "Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data" adopted by OECD in 1980, that is, Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle and Accountability Principle.

The amendment of some articles of PDPA referred to the requirements of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the predecessor of GDPR), that is, data quality, the lawfulness of data processing, processing of sensitive data, informing of the persons concerned, rights of the persons concerned, objection of the persons concerned, automated individual decisions, confidentiality and security of data, register, publicizing of processing operations and international data transfer.

② Definition and Scope of "personal data"

Generally speaking, the definition of personal data in Taiwan's PDPA is similar to that of GDPR. The criterion is whether a natural person can be directly or indirectly

identified. The personal data of deceased persons are excluded. Whether encrypted[2] or de-identified[3] data are within the scope of the PDPA depends on whether a person can be identified after the data are compared, combined or connected. Whether cookies are personal data depends on whether a person can be directly or indirectly identified by the collected data in specific cases. The comparison between PDPA and GDPR regarding the definition and scope of "personal data" is listed below :

GDPR	Personal Data Protection Act
Art. 4 (1) GDPR: 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. ▪ GDPR does not apply to the personal data of deceased persons. (Recital 27)	Art. 2 subpara. 1 PDPA: "Personal data" refers to a natural person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other information that may be used to directly or indirectly identify a natural person. ▪ Art. 3 Enforcement Rules of the PDPA: The circumstances where a data subject can be "indirectly identified", as referred to under Subparagraph 1, Paragraph 1, Article 2 of the PDPA, shall mean the circumstances where a government or non-government agency possessing such

[2] See the administrative provision of National Development Council fa-fa-zi No. 1090004500: "Encrypted data cannot be used to directly identify a specific person, but they are personal data in the sense of the Personal Data Protection Act if a person can be identified after comparation, combination or connection."

[3] See the administrative provision of National Development Council fa-fa-zi No. 1080081030: "Whether Personal Data Protection Act applies to the data which have passed the certification of personal data de-identification by the Electronics Testing Center depends on whether the de-identified data can be used to directly or indirectly identify a specific person. Controversies are decided by judicial judgments."

	data cannot directly identify the data subject, unless it compares, combines or connects such data with other data. ▪ Personal data means the data of living natural persons. Data of deceased persons are outside the protection scope of the PDPA. (National Development Council fa-fa-zi No. 1090021610)

③ The Rights of Data Subjects and the Obligations of those who process personal data

A. Rights of the persons concerned:

According to Article 3 of PDPA, the data subject shall be able to exercise the following rights with regard to his/her personal data and such rights shall not be waived or limited contractually in advance: 1. the right to make an inquiry of and to review his/her personal data; 2. the right to request a copy of his/her personal data; 3. the right to supplement or correct his/her personal data;4. the right to demand the cessation of the collection, processing or use of his/her personal data; and 5. the right to erase his/her personal data. Based on this, it can be understood that the data subject has at least the following rights regarding their personal data under this law:

1. The right to inquire or request access.
2. The right to request copies.
3. The right to request correction or supplementation.
4. The right to request cessation of collection, processing, or utilization.
5. The right to request erasure.

The specific content of each right based on the provisions of PDPA is as follows:

1. Right to inquire or request access: The data subject may request the government or non-government agency to respond to inquiries and allow the data subject to review the personal data collected (Article 10, para. 1).
2. Right to request copies: The data subject may request the government or non-government agency to provide a copy of their collected personal data (Article 10, para. 1).
3. Right to request correction or supplementation: The data subject may request the government or non-government agency to ensure the accuracy of their personal data in the agencies' possession and correct or supplement such data (Article 11, para. 1).
4. Right to request cessation of collection, processing, or utilization:

(1) In the event of a dispute regarding the accuracy of the personal data, the data subject may request the government or non-government agency to cease processing or using the personal data (Article 11, para. 2).
(2) When the specific purpose of data collection no longer exists, or upon expiration of the relevant time period, the data subject may request the government or non-government agency to erase or cease processing or using the personal data (Article 11, para. 3).
(3) The data subject may request the government or non-government agency to erase the personal data collected or cease collecting, processing or using the personal data in the event where the collection, processing or use of the personal data is in violation of the PDPA (Article 11, para. 4).

5. Right to request erasure:
(1) When the specific purpose of data collection no longer exists, or upon expiration of the relevant time period, the data subject may request the government or non-government agency to erase or cease processing or using the personal data (Article 11, para. 3).
(2) The data subject may request the government or non-government agency to erase the personal data collected or cease collecting, processing or using the personal data in the event where the collection, processing or use of the personal data is in violation of the PDPA (Article 11, para. 4).

In contrast to GDPR, Taiwan's PDPA has no norms of the right to data portability, the right to consent to a decision based solely on automated processing, or the right to erase personal data which are no longer necessary in relation to the purposes for which they were collected or otherwise processed (like the right to be forgotten in Art. 17 GDPR).

B. Obligations of government agencies:

Except for the personal data specified under Paragraph 1, Article 6 PDPA (Data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records), the collection or processing of personal data by a government agency shall be for specific purposes and on one of the following bases:

1. Where it is within the necessary scope to perform its statutory duties;
2. Where consent[4] has been given by the data subject; or

[4] "Consent", as referred to in Subparagraph 2, Paragraph 1, Article 15, means a declaration of agreement given by a data subject after he/she has been informed by the data collector of the information required under the PDPA. (Art. 7 para. 1) The data subject's consent may be presumed given pursuant to Subparagraph 2, Paragraph 1, Article 15 and if the data subject does not indicate his/her objection and affirmatively provides his/her personal data after the government or non-

3. where the rights and interests of the data subject will not be infringed upon. (Art. 15 PDPA)

A government agency shall expressly inform the data subject of the following information when collecting their personal data in accordance with Article 15 or 19 of the PDPA:

1. The name of the government or non-government agency;
2. The purpose of the collection;
3. The categories of the personal data to be collected;
4. The time period, territory, recipients, and methods of which the personal data is used;
5. The data subject's rights under Article 3 and the methods for exercising such rights; and
6. The data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. (Art. 8 para. 1 PDPA)

A government or non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19, which was not provided by the data subject, inform the data subject of its source of data and other information specified in Subparagraphs 1 to 5, Paragraph 1 of Article 8. (Art. 9 para. 1 PDPA)

A government agency shall make public the following information online or allow the public to make inquiries thereof via other appropriate means; the foregoing also applies when any changes are made to the following information:

1. The names of the personal data files;
2. The name and contact information of the agency that is in possession of the personal data files;
3. The legal basis and purpose of keeping the personal data files; and
4. The category of personal data. (Art. 17 PDPA)

A government agency in possession of personal data files shall assign dedicated personnel to implement security and maintenance measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed. (Art. 18 PDPA)

C. Obligations of non-government agencies：

Except for the personal data specified under Paragraph 1, Article 6 (Data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records), the collection or processing of personal data by a non-government agency shall be for specific purposes and on one of the following bases:

---

government agency has informed the data subject of the relevant information specified in Paragraph 1, Article 8 of the PDPA. (Art. 7 para. 3)

1. Where it is expressly required by law;
2. Where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject and proper security measures have been adopted to ensure the security of the personal data;
3. Where the personal data has been disclosed to the public by the data subject or has been made public lawfully;
4. Where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;
5. Where consent has been given by the data subject[5];
6. Where it is necessary for furthering public interest;
7. Where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or
8. Where the rights and interests of the data subject will not be infringed upon. (Art. 19 para. 1 PDPA)

A non-government agency shall expressly inform the data subject of the following information when collecting their personal data in accordance with Article 15 or 19 of the PDPA:

1. the name of the government or non-government agency;
2. the purpose of the collection;
3. the categories of the personal data to be collected;
4. the time period, territory, recipients, and methods of which the personal data is used;
5. the data subject's rights under Article 3 and the methods for exercising such rights; and
6. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. (Art. 8 para. 1)

A non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19, which was not provided by the data subject, inform the data subject of its source of data and other information specified in Subparagraphs 1 to 5, Paragraph 1 of Article 8. (Art. 9 para. 1)

---

[5] "Consent", as referred to in Subparagraph 5, Paragraph 1, Article 19, means a declaration of agreement given by a data subject after he/she has been informed by the data collector of the information required under the PDPA. (Art. 7 para. 1) The data subject's consent may be presumed given pursuant to Subparagraph 5, Paragraph 1, Article 19 if the data subject does not indicate his/her objection and affirmatively provides his/her personal data after the government or non-government agency has informed the data subject of the relevant information specified in Paragraph 1, Article 8 of the PDPA. (Art. 7 para. 1)

A non-government agency possessing personal data files shall implement proper security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed. (Art. 27 para. 1)

④ Organization and authority of the supervisory body enforcing personal data protection

Taiwan has yet to have a single competent authority for personal data protection. That is to say, the personal data protection is decentralized. Administrative agencies are responsible for data protection in respect of their respective affairs. The Executive Yuan laid down a list of the central governing authorities for the supervision of non-government agencies in terms of personal data protection.[6]

The Constitutional Court of Taiwan held in Judgment 111-Hsien-Pan-13 (2022) that the PDPA lacks an independent supervisory mechanism for personal data protection. The protection of informational privacy is insufficient. This may be unconstitutional. The relevant mechanism should be established within three years.

The Executive Yuan introduced on April 13, 2023, a draft amendment to the PDPA, in which the new Art. 1-1 sets up the Personal Data Protection Commission as the competent authority for the PDPA. The new Art. 1-1 of the PDPA was passed by the Legislative Yuan on May 31, 2023, but is still not in effect. The Executive Yuan was authorized to assign the date Art. 1-1 takes effect.

⑤ Judicial proceedings or judicial remedy (standing to sue. class action.)

The issue of remedies for personal data protection is closely related to the rights of the data subject mentioned earlier, forming a mutual and interdependent relationship. Under Taiwan's remedial system, when the obligor is a government agency, the remedy shall be pursued through administrative litigation procedures; when the obligor is a non-government agency, the remedy shall be sought through civil litigation procedures. These remedies are not directly stipulated in the Personal Data Protection Act (PDPA). However, they are based on the nature of the violation and are brought forward according to the Administrative Appeal Act, Administrative Litigation Act, and Civil Procedure Code provisions. In addition, the PDPA has specific provisions regarding compensation for damages that are summarized as follows:

A. Basis of Claims and Principle of Liability:

1. Government agency:

(1) A government agency shall be liable for the damages arising from injury caused

[6] https://www.moj.gov.tw/media/16809/542114375377.pdf?mediaDL=true

by any unlawful collection, processing or use of personal data, or other infringement on the rights of data subjects due to such government agency's violation of the PDPA, unless such injury was caused by any natural disaster, emergency or other force majeure event (Article 28 para. 1).

→Government agencies bear almost non-negligence liability.

(2) If an injury suffered by the victim is a non-pecuniary damage, he/she may request an appropriate amount of monetary compensation; if the injury suffered by the victim is damage to his/her reputation, the victim may request appropriate corrective measures to restore his/her reputation (Article 28 para. 2).

2. Non-government agency:

(1) A non-government agency shall be liable for the damages arising from any injury caused by any unlawful collection, processing or use of personal data, or other infringement on the rights of data subjects due to such non-government agency's violation of the PDPA, unless the non-government agency can prove that such injury is not caused by its willful act or negligence (Article 29, para. 1). → The burden of proof is shifted to the non-government agencies.

(2) If an injury suffered by the victim is a non-pecuniary damage, he/she may request an appropriate amount of monetary compensation; if the injury suffered by the victim is damage to his/her reputation, the victim may request appropriate corrective measures to restore his/her reputation (Article 29, para. 2 applied mutatis mutandis to Article 28, para. 2)

B. Compensation Limitation:

1. Government agencies:

(1) Under the circumstances identified in the preceding two paragraphs, if it is difficult or impossible for the victim to prove the monetary value of the actual damage, he/she may ask the court to award the compensation in the amount of not less than NT$500 but not more than NT$20,000 per incident, per person based on the severity of the damage (Article 28 para. 3).

(2) Where the rights of multiple data subjects have been infringed upon due to the same incident, the total amount of compensation awarded to such data subjects shall not exceed NT$200 million. However, if the interests involved in the incident exceed NT$200 million, the compensation shall be up to the value of such interests (Article 28 para. 4).

2. Non-governmental organizations, the same as above (PDPA, Article 29, para. 2).

3. Aside from the provisions of the PDPA, the legal basis for damages compensation (Article 31):

(1) The State Compensation Law may be applied to a government agency

(2) The Civil Code may be applied to a non-government agency.

4. Class action lawsuits (Article 32 to Article 40):

(1) Where the rights of multiple data subjects have been infringed upon due to the same incident, the incorporated foundation or incorporated charity may file a lawsuit with the court in its own name after obtaining a written delegation of litigation rights of at least 20 data subjects (Article 34 para. 1).

(2) In Taiwan, state compensation lawsuits are heard by civil courts and are to be applied to the provisions of the Code of Civil Procedure (National Compensation Act, Article 12). Therefore, the provisions mentioned above of class action lawsuits also apply to state compensation lawsuits filed against government agencies. The comparison between PDPA and GDPR regarding remedies is listed below :

GDPR	Personal Data Protection Act
● Art. 77 (1) GDPR: Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. ● Art. 79 (1) GDPR: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge	● Remedies[7] ■ Art. 28 para. 1 (government agencies): A government agency shall be liable for the damages arising from injury caused by any unlawful collection, processing or use of personal data, or other infringement on the rights of data subjects due to such government agency's violation of the PDPA, unless such injury was caused by any natural disaster, emergency or other force majeure event. →A government agency can be exempt from liability only when injury was caused by natural

[7] Where the rights of multiple data subjects have been infringed upon due to the same incident, the total amount of compensation awarded to such data subjects shall not exceed NT$200 million. However, if the interests involved in the incident exceed NT$200 million, the compensation shall be up to the value of such interests. (Art. 28 para. 4, Art. 29 para. 2)

a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. ● Art. 82 (1) GDPR: Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. ● Art. 82 (2) GDPR: Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. ● Art. 82 (3) GDPR: A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. ● Art. 80 (1) GDPR:	disaster, emergency or other force majeure event. This is stricter than GDPR. ■ Art. 29 para. 1 (non-government agencies): A non-government agency shall be liable for the damages arising from any injury caused by any unlawful collection, processing or use of personal data, or other infringement on the rights of data subjects due to such non-government agency's violation of the PDPA, unless the non-government agency can prove that such injury is not caused by its willful act or negligence. →A non-government agency can be exempt from liability when it can prove that injury is not caused by its willful act or negligence. This is similar to GDPR. ■ Art. 34 para. 1 sentence 1 (class action): Where the rights of multiple data subjects have been infringed upon due to the same incident, the incorporated foundation or incorporated charity may file a lawsuit with the court in its own name after obtaining a written delegation of litigation rights of at least 20 data subjects.

The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.	

An additional question: Utilization of health data for research purposes

Is the consent of the patient required for the use of his/her medical record or biometric data for research purposes or drug development? What legal obligations (such as anonymization) do research institutions have when collecting and utilizing patient health data for research purposes?

According to Art. 6 para. 1 proviso subpara. 4 PDPA, data pertaining to a natural person's medical records, healthcare, genetics and physical examination can be collected, processed or used where it is necessary for statistics gathering or academic research by a government agency or an academic institution for the purpose of healthcare, public health, or crime prevention, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject. In other words, the health data can be collected, processed or used without patient's consent when the data subject cannot be identified.

The Constitutional Court held in Judgment 111-Hsien-Pan-13 (2022)[8] that the PDPA and other pertaining regulations lack independent supervisory instruments on

[8] Background of the case: The insured of the National Health Insurance receive the medical care services of the Contracted Healthcare Providers, which according to Article 80 of the National Health

data protection. The competent authority shall, within three years from the announcement of the judgment, ensure relevant legal mechanisms be established.

According to Art. 79 National Health Insurance Act, the National Health Insurance Administration, Ministry of Health and Welfare, may require relevant agencies to provide the necessary information it needs to carry out the business of the Insurance. According to Art. 80 National Health Insurance Act, the Competent Authority may ask the insured, the group insurance applicants, the premium withholders, and contracted medical care institutions to provide relevant documents, such as account records, receipts, medical history, diagnosis records, or cost of medical expenses, and other documents or relevant information.

The Constitutional Court held in the said judgment that Articles 79 and 80 of the National Health Insurance Act lack explicit regulations on the subject, aims, legal elements, scope, and measures on how the National Health Insurance data, as a database, may be preserved, processed, transmitted externally, and provided externally by the National Health Insurance Administration. The stated provisions also fail to provide explicit regulations on important subjects, such as supervisory instruments regarding organizational and procedural data protection matters. They violate the right to informational privacy guaranteed by Article 22 of the Constitution. The competent authority shall amend pertaining provisions or establish special acts within three years.

In addition, the Constitutional Court held in the said judgment that in terms of the usage of personal health insurance data beyond its original collecting purpose, transmitted from the National Health Insurance Administration to other government agencies or academic research institutes, the existing legal regime lack regulations allowing the data subjects to opt-out, consequently violating the right to informational privacy guaranteed by Article 22 of the Constitution. The competent authority shall

---

Insurance Act (NHIA) provide the relevant medical records and prescription data to the National Health Insurance Administration to claim the medical costs.
Over the years, the National Health Insurance Administration has collected a huge number of health insurance data, including personal health insurance data. It gave the data to the National Health Research Institute to establish the "National Health Insurance Research Database," which is accessible to the public. It also transmitted the health insurance data, which is accessible to the public, to the Health and Welfare Data Science Center, Ministry of Health and Welfare (MHW).
The petitioners were of the opinion that the said actions are illegal because their personal health insurance data protected by the constitutional right to privacy are used for the purposes outside the business of the National Health Insurance. They argued that the National Health Insurance Administration shall not provide their personal health insurance data to others for the purposes outside the business of the National Health Insurance.
The National Health Insurance Administration rejected the argument. The petitioners initiated administrative litigations. After losing the case in the final court decision, the petitioners filed for constitutional review, arguing that Article 6 Paragraph 1 Proviso Subparagraph 4 of the Personal Data Protection Act and Article 79 Paragraph 1 and Article 80 Paragraph 1 of the National Health Insurance Act are unconstitutional.

amend or establish relevant acts stipulating the subject, basis, procedure and effect of opt-out or denying opt-out within three years. If the amendment or establishment of said acts is past due, the data subject shall request to stop the data use outside of original purposes.

Points to criticize:

1. The judgment does not clarify the question if Article 6 Paragraph 1 Proviso Subparagraph 4 of the Personal Data Protection Act can be the legal basis for the provision of the health insurance data by the National Health Insurance Administration to the National Health Research Institutes to establish the National Health Insurance Research Database.
2. It seems contradictory that the judgment asks the legislature to enact the regulations of the right of the affected persons to stop the utilization but recognizes the constitutionality of Article 6 Paragraph 1 Proviso Subparagraph 4 of the Personal Data Protection Act, which allows the compulsory collection, process or utilization without the consent of the affected persons (limitation to the right of the affected persons to control the personal data with the ex ante consent arising from the right to personal information privacy). The right to stop the utilization, or the right to opt-out, presupposes the ex ante consent of the affected persons. It is a contrast to the right to opt-in. How can the affected persons exercise the right to stop the utilization when under legal prerequisites the public authorities can compulsorily collect, process or utilize the personal data without their consent? On the contrary, how can the public authorities compulsorily collect, process or utilize the personal data when the affected persons enjoy the right to stop the utilization of their personal data?

※This work was supported by JST [Moonshot R&D][Grant Number JPMJMS2293].

The following is a summary page of the report.

Ⅶ. South Korea

Jiyoung Sang
(Visiting Researcher, Keio University & South Korea Attorney at law)

韓国法における個人情報自己決定権の保護

I. はじめに

韓国法上の個人情報の主体は、自己の個人情報に関して憲法上の基本権として「個人情報自己決定権」を有する。本稿では、韓国憲法上の個人情報自己決定権の意味について述べ、さらに、その個人情報自己決定権が具体的な法律（「個人情報保護法」）を通じて如何に保護されているかについて取り上げる。

II. 情報主体の憲法上の基本権としての個人情報自己決定権

1. 個人情報自己決定権の意義

韓国の憲法には、明文の条項として個人情報自己決定権が示されていない。しかしながら、２００５年、個人の指紋情報を収集・保管・電算化してそれを犯罪捜査のために利用されるようにした旧住民登録法の関連条項などが違憲かどうかが問題になった事件において、憲法裁判所が個人情報自己決定権を憲法上の独自の基本権として認めた以来（憲法裁判所２００５年5月２６日宣告９９憲マ５１３、２００４憲マ１９０（併合）決定[1]、以下「指紋情報事件」）、かかる権利は憲法上の基本権として認められている。

上記の指紋情報事件の判示で定義された個人情報自己決定権とは、「自己に関する情報が、いつ、誰に、どの範囲まで知られ、また利用されるようにするかをその情報主体が自ら決める権利、すなわち情報主体が個人情報の開示・利用に関して自ら決める権利」をいう。このような個人情報自己決定権の概念は、ドイツ連邦憲法裁判所が１９８３年「人口調査事件（BVerfGE 65,1）」で最初に判示した情報自己決定権（die Recht auf informationelle Selbstbestimmung）、すなわち「自己の個人的情報のどれを第三者に開示して利用させるかを自ら決める権利」の影響を受けたものと評価されている[2]。

---

[1] 憲法裁判所は、審判対象条項は、個人情報である指紋を収集してそれを犯罪捜査などに利用することで個人情報自己決定権を制限するものであるが、これは法律留保原則及び過剰禁止原則に反しないため、個人情報自己決定権を侵害したとはいえないと判断した。

[2] クォン・ヨンジュン、「個人情報自己決定権と同意制度に対する考察」、法学論叢第３６巻第１号、２０１６、６７７頁；チェ・ソンヒ、「個人情報自己決定権と忘れられた憲法裁判所決定などのための弁明」、情報法学第２０巻第3号、２０１７、３０６頁

憲法裁判所は、上記の指紋情報事件で「新しい独自的基本権としての個人情報自己決定権を憲法的に承認する必要性」が台頭した背景について、現代の情報通信技術の発達によって国の個人情報の収集・処理力量が強化されたことに注目した。また、このような社会的状況のもとで個人情報自己決定権を憲法上の基本権として承認することは、「現代の情報通信技術の発達に内在する危険性から個人情報を保護することで、窮極的には個人の決定の自由を保護し、さらに自由民主体制の根幹が総体的に損ねられる可能性を遮断するうえで必要な最小限の憲法的保障装置」であると判示した。

個人情報自己決定権が初めて認められた２００５年の指紋情報事件以降にも情報通信技術の発達は一層加速化しており、かかる技術を基に、国に限らず、私人（各種企業や団体など）が個人情報を収集・処理しようとする需要や力量も共に急速に高まっている。また、情報主体にとっても、発達された情報通信技術によってその力量が強化された個人情報処理者が情報主体の権利を侵害しないように防ぐなど、個人情報自己決定権を防御的に行使するだけでなく、一方では発達した技術を基に様々な方面に分散している自己の個人情報を能動的に活用して管理するなど、個人情報自己決定権を積極的に行使しようとする需要もますます増えていくことが見込まれる。

結局、「自己に関する情報がいつ、誰に、どの範囲まで知られ、また利用されるようにするか」を自ら決める個人情報自己決定権は、今後の現代社会でより重要な意味を持つようになると考えられる。

2. 憲法に示されていない独自的基本権としての個人情報自己決定権

ア. 個人情報自己決定権の憲法上の根拠

前述のとおり、韓国の憲法には明文の条項として個人情報自己決定権が基本権として示されていない。そうであれば、個人情報自己決定権の憲法上の根拠は何か？

憲法第１０条第１文
すべての国民は、人間としての尊厳と価値を持ち、幸福を追求する権利を有する。

憲法第１７条
すべての国民は、私生活の秘密と自由を侵害されない。

憲法裁判所は、２００５年の指紋情報事件で、個人情報自己決定権の理念的基礎として、憲法第１０条第１文（人間の尊厳と価値及び幸福追求権に基づく一般的人格権）、憲法第１７条（私生活の秘密と自由）、憲法の自由民主的な基本秩序ルールや国民主権原理と民主主義の原理などを考慮することができるとしながらも、個人情報自己決定権により保護しようとする内容をこのような各基本権など及び憲法原理などの一部に完全に取り込ませることは不可能なので、個人情報自己決定権の憲法的根拠を敢えて一部に限定することは望ましくないとし、結局、個人情報自己決定権とはこれらを理念的基礎とする「独自的基本権であって、憲法に示されていない基本権」と認めた。

ちなみに、指紋情報事件以降の憲法裁判所による決定例などによれば、個人情報自己決定権の憲法的根拠として「自由民主的な基本秩序や国民主権原理など」に触れずに、憲法第１０条第１文と第１７条のみに触れている傾向がある（憲法裁判所２０１５年6月２５日宣告２０１４憲マ４６３決定など）。この点に関して、憲法裁判所がその後の判示などで自由民主的な基本秩序や国民主権原理などに触れなくても、指紋情報事件決定に同じ説示を繰り返したり、そのまま引用していることなどに照らし、憲法裁判所の個人情報自己決定権の捉え方について従来の指紋情報事件決定の説示から逸脱したりその見解を変えたとは言い難いという意見がある[3]。

イ．プライバシー権との関係

個人情報自己決定権の憲法的根拠ないし理念的基礎になる憲法第１７条における私生活の秘密と自由は、プライバシー権（Right to privacy）にも密接な関わりがある。プライバシー権の意義や脈絡は、様々な観点によって理解されることができ、各観点によって韓国憲法上のプライバシー権の意味もそれぞれ別に理解されると考えられる。

まずプライバシー権を狭く理解する場合（狭義説）、これは私生活の平穏が侵害されず私生活の秘密がむやみに開示されない権利であるといえる。これは初期に米国で認められた概念であり、私生活の領域から派生される各種の事実が他人に露出しない消極的権利（right to be alone）にあたると考えられる。一方、このような消極的な性格の権利に加え、積極的な性格の権利として自己に係る私的な生活や情報を管理・統制する権利もプライバシー権に含まれるという見解があり、これは近来学界の多数説（広義説）と捉えられている[4]。

憲法裁判所は、多くの決定例で、憲法第１７条の私生活の秘密や自由について、私生活の秘密とは「私生活に関わりのある、自分だけの私的な領域が本人の意思に反して他人に知られないようにする権利」であり、私生活の自由とは「社会共同体の一般的な生活ルールの範囲内で私生活を自由に形成していき、その設計や内容について外部から干渉されない権利」であるとしている[5]。案ずるに、この憲法裁判所の判示は、憲法第１７条を基本的に消極的な性格の権利と捉えながらも、その中で積極的に「私生活を自由に形成できる権利」があることを認めたものであり、このような流れから憲法第１７条は前述の広義のプライバシー権の概念に相応しいものと考えられる。

ところで、このようなプライバシー権の概念を前提とすれば、プライバシー権の保護法益は、自己の私生活の秘密に係る事項を自由に形成・維持し、それをむやみに他人に開示されない法的利益であ

---

[3] チェ・ソンヒ、「個人情報自己決定権と忘れられた憲法裁判所決定などのための弁明」、情報法学第２０巻第３号、２０１７、２９４～２９６頁。

[4] プライバシー権に関する韓国の諸学説を分類した内容は、パク・ソンヨン、「プライバシー権の比較憲法的研究」、西江大学校一般大学院、２０１６、３１～３３頁参照。

[5] 憲法裁判所２００２年3月２８日宣告２０００憲マ５３決定、憲法裁判所２００１年8月３０日宣告９９憲バ９２決定など。

るといえる。このような私生活に係る情報は、個人の社会的評価を低下させ得る情報や隠密な私生活情報であり、かかる情報の外部開示による名誉などの人格権を保護するためのものであるといえる[6]。一方、個人情報自己決定権については、情報主体が自己の個人情報が如何に利用されるかについて同意し、個人情報が如何に利用されているかを閲覧して確認するなど、個人情報に対する統制権限をその内容とするものと捉えるべきであり、個人に関する情報開示などによって私生活（プライバシー）が侵害されるかどうかは、その権利の一部に該当すると考えられる[7]。

そうであれば、個人情報自己決定権は自己に関する情報を自ら統制することができる権利であることから、上記のプライバシー権の概念範囲の一部と重なるといえるが、個人情報自己決定権とプライバシー権は基本的に権利保護の対象や目的が異なるといえる。憲法裁判所もこれらの点を考慮し、指紋情報事件で、個人情報自己決定権により保護しようとする内容を第１７条の私生活の秘密や自由など一部の基本権や憲法原理の一部に完全に取り込ませることができないとし、個人情報自己決定権を憲法に示されていない独自的基本権と認めたのではないかと考えられる。

III. 韓国の個人情報保護法上の個人情報自己決定権の保護

憲法上の基本権である個人情報自己決定権を具体的に実現する個別法としては、「個人情報保護法」がある[8]。個人情報保護法は２０１１年制定当時、「情報主体の権利を明確に定めることにより、情報主体がより容易に個人情報に対する自己統制権を実現」できるようにするために制定された（２０１１年3月２９日法律第１０４６５号に制定された個人情報保護法の制定理由を参照）。さらに、個人情報保護法第１条の目的規定には、このような制定目的に限らず、個人情報自己決定権の憲法的根拠になる憲法第１０条第１文（人間の尊厳と価値及び幸福追救権に基づく一般的人格権）の内容も入っていることがわかる。

個人情報保護法第１条（目的）
この法は、個人情報の処理及び保護に関する事項を定めることにより、個人の自由と権利を保護し、さらに個人の尊厳と価値を具現することを目的とする。

このような個人情報保護法は、個人情報の処理及び保護に関する事項を定める一般法の地位を有する（個人情報保護法第６条[9]）。個人情報の中でも、一部の個人情報（個人信用情報、個人位置情報

[6] イ・インホ、「第２世代プライバシー保護法としての個人情報保護法に対する理解」、司法第８号、２００９年６月、５６～６４頁。
[7] カン・ダルチョン、「個人情報自己決定権保護の限界の観点から見た「個人情報保護法」改正の問題点」、中央法学第２２集第３号、２０２０年９月、１５頁。
[8] クォン・ヨンジュン、「個人情報自己決定権と同意制度に対する考察」、法学論叢第３６巻第１号、２０１６年、６７８頁；カン・ダルチョン、「個人情報自己決定権保護の限界の観点から見た「個人情報保護法」改正の問題点」、中央法学第２２集第３号、２０２０年９月、２０～２１頁；キム・ヘウォン、「個人情報に対する憲法的検討」、公法学研究第２０巻第４号、２０１９年、８２頁。
[9] 個人情報保護に関しては、他の法律に特段の規定がある場合を除き、この法の定めによる。

など）においては優先して適用される特別法など（「信用情報の利用及び保護に関する法律」、「位置情報の保護及び利用などに関する法律」など）が存在するが、本稿では一般法である個人情報保護法を基準に情報主体の個人情報自己決定権が韓国の法制を通じて具体的に保護される態様について述べる。

1. 情報主体による権利行使

韓国の個人情報保護法は、次のように第４条に情報主体の権利を概括的に明示し、その権利などは「個人情報の開示と利用に関して自ら決める権利」である個人情報自己決定権の内容を要諦としている。

個人情報保護法[10]第４条（情報主体の権利）
情報主体は、自己の個人情報処理に関して次の各号の権利を有する。
1. 個人情報の処理に関する情報の提供を受ける権利
2. 個人情報の処理に関する同意の有無、同意の範囲などを選択して決める権利
3. 個人情報の処理有無を確認し、個人情報に対して閲覧（写し発給を含む）を要求する権利[11]
4. 個人情報の処理停止、訂正・削除及び破棄を求める権利
5. 個人情報の処理によって発生した被害が迅速且つ公正な手続によって救済される権利

本１.項（情報主体による権利行使）では、個人情報処理が通常的に行われる過程で情報主体が行使できる権利として個人情報保護法第４条第１号ないし第４号の各権利が如何に保障されるかについてまず取り上げる。また、異常な個人情報処理による被害に関し、情報主体が行使できる権利を項目を分けて２.項（司法的救済システムによる情報主体の被害救済）で取り上げる。

ア. 個人情報処理者への義務付与による間接的な権利保障

1) 個人情報処理に関する情報の提供を受ける権利

個人情報保護法は、個人情報処理者をして個人情報を収集・利用するなど個人情報を処理することに関する情報を情報主体に知らせることを義務づけている。詳しくは、個人情報処理者は個人情報の収集・利用・（第三者への）提供のために、その目的・範囲などを情報主体にあらかじめ告知して同

[10] 以下に引用する個人情報保護法の条文は、基本的に２０２３年７月施行されている現行法（２０２０年８月５日施行法律第１６９３０号）を基準とする。２０２３年３月１４日公布され、２０２３年９月１５日又は２０２４年３月１５日施行される改正個人情報保護法（法律第１９２３４号）条文の関連内容は、別途の注釈などに説明を加える。

[11] ２０２３年９月１５日施行される改正個人情報保護法のもとでは、第３号の「閲覧を求める権利」が「閲覧及び転送を求める権利」に改正され、「完全に自動化した個人情報処理による決定を拒否したり、それに対する説明などを求める権利」が第６号に新設された。この点、本１.項の「ウ.最近の改正により一層能動的な自己情報統制権を実現」の項目で詳述する。

意を得なければならない（個人情報保護法第１５条第２項、第１７条第２項、第３９条の３第１項[12]）。さらに、個人情報処理者が情報主体以外から収集した個人情報を処理するときは、その収集・出処・処理目的などをテキストメッセージ、電子メールなど情報主体がわかりやすい方法で情報主体に知らせなければならない（個人情報保護法第２０条第１項及び第２項[13]）。

一方、個人情報処理者は、個人情報の処理目的、保有・利用期間などを盛り込んだ個人情報処理方針（Privacy Policy）を策定して開示し（個人情報保護法第３０条第１項）、一定規模以上の情報通信サービスプロバイダーは、利用者に個人情報利用内訳を周期的に通知しなければならない（個人情報保護法第３９条の８第１項[14]）。

2) 個人情報処理に関する同意の有無、範囲などを選択して決める権利

個人情報自己決定権で重要なのは、情報主体が、個人情報処理者の個人情報処理に対して実質的な統制権を有することである。したがって、情報主体に個人情報処理の有無及び同意範囲などを選択できる権利を与えるとしても、個人情報処理者が事実上同意を強要すれば、情報主体の権利が形式化されてしまう恐れがある。個人情報保護法は、このような問題を解決するために、情報主体の個人情報自己決定権を保障すべく、その同意方法を法律で具体化して包括的な同意を禁止している（個人情報保護第２２条）[15]。

例えば、個人情報処理に関する重要事項は、字の大きさなどを別々にして明確に表示し、契約の締結などのために情報主体の同意なく処理できる（必須の）個人情報と、情報主体の同意を要する（選択的な）個人情報とを区分するなど、個人情報保護法第２２条は同意を得る方法をかなり詳しく規律している。大法院もまた、個人情報処理者が情報主体から適法な同意を得るためには、「利用者（情

---

[12] 情報通信サービスプロバイダー（オンライン上、利用者の個人情報を収集及び利用する個人情報処理者など）に対する特例規定である第３９条の３は、２０２３年９月１５日施行される改正個人情報保護法のもとでは削除され、情報通信サービスプロバイダーも一般個人情報処理者と同様、個人情報収集・利用に関する規定が適用される。
ちなみに、過去の情報通信サービスプロバイダーに対する個人情報保護関連規定は「情報通信網の利用促進及び情報保護等に関する法律」で定められたが、当該内容が現行個人情報保護法（２０２０年２月４日法律第１６９３０号に改正されたもの）において特例規定である第３９条の３ないし第３９条の１５に移された。

[13] 個人情報処理者が規模などにおいて一定の基準に満たなければ、情報主体の要求があるときに限って関連情報を告知することができる（第２０条第１項）。

[14] 情報通信サービスプロバイダーに対する特例規定である第３９条の８は、２０２３年９月１５日施行される改正個人情報保護法のもとでは削除される。当該内容は、同日施行される改正法に新設される第２０条の２に移され、当該通知義務は情報通信サービスプロバイダーにとどまらず、個人情報処理者一般に拡大して適用される。このとき、一定基準以上の個人情報処理者（５万人以上の情報主体の敏感情報又は固有識別情報を処理する者、又は１００万人以上の情報主体の個人情報を処理する者）は、収集した個人情報の利用・提供の内訳や利用・提供の内訳がわかる情報システムに接続する方法を周期的に情報主体に通知しなければならない。

[15] 個人情報保護委員会、「個人情報保護法令及び指針・告示解説」、２０２０年１２月、３４頁及び１４７頁。

報主体）が個人情報の提供に関する決定権を十分自由に行使できるよう、情報通信サービスプロバイダーがあらかじめ当該インターネットサイトに通常の利用者に法定告知事項[16]の詳細がわかりやすいよう法定告知事項の全部を明確に掲載しなければならない」と判示しました（大法院２０１６年6月２９日宣告２０１４ドゥ２６３８判決[17]）。

もっとも、２０２３年9月１５日施行される改正個人情報保護法のもとでは、上記第２２条の内容の多くが緩和され、これは従来の個人情報保護法における「同意万能主義」の問題[18]を解消しようという改正の趣旨が反映されたものとみられる[19]。これを補足すれば、韓国の個人情報保護法は、欧州連合のGeneral Data Protection Regulation（ 以下「ＧＤＰＲ」）に類似して個人情報の収集・利用の正当な根拠として、同意、法令上の根拠、公的業務の遂行、契約の締結・履行、重大な利益、正当な利益を並列的に並べているが（個人情報保護法第１５条第１項など）、多くの個人情報処理者は、同意なく個人情報処理が可能であるという点に対する立証責任を負わないために（同意がなくても個人情報を収集・利用することができる場合までも）一概に同意を通じて個人情報を収集・利用している。

これに対して、前述のとおり、規制機関や司法機関が「明確な告知による適法な同意を得なければならない」という立場を取るほど、個人情報処理者としては、却って法令上の基準に相応しい同意さえあれば個人情報の収集・利用は適法であるという認識が蔓延することになる一方、情報主体としては、同意書式の語句をきちんと確認せずに習慣的に同意したり、同意しなくては関連サービスを利用できないため仕方なく同意することが頻繁になる。

これらの点を踏まえ、２０２３年9月１５日施行される改正個人情報保護法は、個人情報の収集・

---

16 個人情報の収集・利用・提供をするために情報主体から同意を得る前に情報主体に必ず告知しなければならない事項である。例えば、個人情報の収集にあたり、個人情報の収集・利用目的、収集しようとする個人情報の項目、個人情報の保有及び利用期間、同意を拒否する権利があるという事実及び、同意拒否による不利益がある場合には、その不利益の内容が法定告知事項に該当する（個人情報保護法第１５条第２項）。

17 Webサイトのバナーやイベント広告のポップアップ画面を通じて個人情報の収集項目及び目的、保有期間に対する案内なく「確認」をクリックすれば同意したものとみなす方法であり、明示的な同意を得ずに利用者の個人情報を収集して保険会社などに提供した行為について、適法な同意のない個人情報提供行為であると判断したケース。

18 チョ・スヨン、「個人情報保護法における情報主体の同意と基本権保障に関する研究」、法学研究第１８巻第1号、２０１８年、３３１頁；個人情報保護委員会も、現行の同意制度に関して「複雑で硬直的な同意制度の運用により企業・機関などの個人情報処理者は合理的な個人情報の処理及び活用に制約を受け、情報主体も複雑な告知事項と手続などにより「同意の形式化」が蔓延」しているとした（個人情報保護委員会２０２３年3月7日付けプレスリリース１１頁）。

19 個人情報保護委員会の２０２３年3月7日付けプレスリリースによれば、２０２３年9月１５日施行される改正個人情報保護法は、「これまで情報主体の「同意」に過度に依存していた個人情報処理慣行から脱し、相互契約など合理的に予想できる範囲内では同意がなくても個人情報の収集・利用が可能になるよう整備」されたものである（個人情報保護委員会２０２３年3月7日付けプレスリリース３頁）。

利用の正当な根拠のうち「契約の締結・履行」要件を緩和[20]して不必要な同意徴求の慣行の解消を図り、前述の個人情報保護法第２２条もまた情報主体の同意なく処理できる個人情報に対しては、同意ではない関連する個人情報処理根拠に従ってこれを個人情報処理方針に開示しなければならないことを明確にする方向に改正された。

イ．情報主体が自ら行使できる権利の明示

1)　個人情報の処理有無の確認及び閲覧を求める権利

個人情報保護法第３５条（個人情報の閲覧）

① 情報主体は、個人情報処理者が処理する自己の個人情報の閲覧を当該個人情報処理者に求めることができる。

② 第１項にも拘わらず、情報主体が自己の個人情報の閲覧を公共機関に求めようとするときは、公共機関に自ら閲覧を求め、又は大統領令の定めによって保護委員会を通じて閲覧を求めることができる。

③ 個人情報処理者は、第１項及び第２項による閲覧を求められたときは、大統領令に定める期間内に情報主体が当該個人情報を閲覧できるようにしなければならない。この場合、当該期間内に閲覧することができない正当な事由があるときは、情報主体にその事由を知らせて閲覧を延期することができ、その事由が消滅すれば遅滞なく閲覧させなければならない。

④ 個人情報処理者は、次の各号の一にあたる場合には、情報主体にその事由を知らせて閲覧を制限・拒絶することができる。

1. 法律に基づいて閲覧が禁止・制限される場合
2. 他人の生命・身体を害する恐れがあり、又は他人の財産その他の利益を不当に侵害する恐れがある場合
3. 公共機関が次の各目の一にあたる業務を行うにあたり、重大な支障をもたらす場合
   - ア．租税の賦課・徴収又は還付に関する業務
   - イ．「小・中等教育法」及び「高等教育法」による各級学校、「生涯教育法」による生涯教育施設その他の法律に基づいて設置された高等教育機関での成績評価又は入学者の選抜に関する業務
   - ウ．学歴・技能及び採用に関する試験、資格審査に関する業務
   - エ．補償金・給付金の算定などについて行われている評価又は判断に関する業務
   - オ．その他の法律に基づいて行われている監査・調査に係る業務

⑤ 第１項から第４項までの規定による閲覧要求、閲覧制限、通知などの方法並びに手続に関して必要な事項は大統領令に定める。

[20] 現行の個人情報保護法上の関連要件は、「情報主体との契約の締結及び履行のためにやむを得ず必要な場合」となっているが（個人情報保護法第１５条第１項第４号）、２０２３年９月１５日施行される改正個人情報保護法は、当該規定を「情報主体と締結した契約を履行したり契約を締結する過程で情報主体の要請による措置を履行するために必要な場合」に改正し、「やむを得ない」という要件を削除した。

情報主体は、個人情報処理者が処理する自己の個人情報に対する閲覧を当該個人情報処理者に求めることができる。かかる閲覧要求権は、個人情報処理者による無分別な個人情報の収集・利用の提供を防ぐ機能を果たすことができる。

個人情報処理者が情報主体の閲覧を拒絶できる事由は、法律に基づいて閲覧が禁止・制限される場合、他人の生命・身体を害する恐れがあったり他人の財産その他の利益を不当に侵害する恐れがある場合、又は公共機関による特定業務の遂行に重大な支障をきたす場合に限られるため、個人情報処理者は情報主体の閲覧を任意に拒絶する余地がほとんどない。さらに、個人情報処理者は、情報主体から閲覧を求められたときは、１０日以内に情報主体が当該個人情報を閲覧できるようにしなければならない。

一方、情報主体は自己の個人情報の閲覧を求めるためには、個人情報処理者が設けた方法や手続に従って求めなければならない（個人情報保護法第３５条第５項、同法施行令第４１条第１項）。これは、一方的で非効率的な閲覧要求の濫用により、個人情報処理者の利益が不当に侵害されないようバランスをとったものと思われる。このとき、個人情報処理者は閲覧要求の方法や手続を設けるにおいて、個人情報を収集する方法や手続に比べて難しくしてはならない。

2) 個人情報の訂正・削除、処理停止及び破棄を求める権利

個人情報保護法第３６条（個人情報の訂正・削除）

① 第３５条に基づき、自己の個人情報を閲覧した情報主体は個人情報処理者に対してその個人情報の訂正又は削除を求めることができる。ただし、他の法令にその個人情報が収集対象に掲げられている場合には、その削除を求めることができない。

② 個人情報処理者は、第１項による情報主体の要求を受けたときは、個人情報の訂正又は削除に関して他の法令に特段の手続が規定されている場合を除き、遅滞なくその個人情報を調べて情報主体の要求に応じて訂正・削除など必要な措置を講じた上で、その結果を情報主体に知らせなければならない。

③ 個人情報処理者が第２項に基づいて個人情報を削除するときは、復旧又は再生されないよう措置を取らなければならない。

④ 個人情報処理者は、情報主体の要求が第１項但書きにあたるときは、遅滞なくその内容を情報主体に知らせなければならない。

⑤ 個人情報処理者は、第２項による調査を行うにあたり、必要に応じて当該情報主体に訂正・削除を求める事項の確認に必要な証拠資料を提出させることができる。

⑥ 第１項・第２項及び第４項による訂正又は削除の要求、通知方法及び手続など必要な事項は大統領令に定める。

情報主体は、個人情報保護法第３５条に基づいて自己の個人情報を閲覧した後、個人情報処理者にその個人情報の訂正・削除を求めることができる。この場合、個人情報処理者はその個人情報が他の

法令に収集対象に掲げられていない限り、その訂正・削除を求められた日から１０日以内に当該個人情報の訂正・削除などの措置をとった事実（削除の要求に応じない法的根拠があれば、その事実及び理由と異議申立方法）を情報主体に知らせなければならない。一方、情報主体は、前述の閲覧要求と同様、個人情報処理者が設けた方法や手続に従って訂正・削除を求めなければならない。

個人情報保護法第３７条（個人情報の処理停止など）

① 情報主体は、個人情報処理者に対して自己の個人情報処理の停止を求めることができる。この場合、公共機関に対しては、第３２条に基づいて登録対象になる個人情報ファイルのうち自己の個人情報に対する処理の停止を求めることができる。

② 個人情報処理者は、第１項による要求を受けたときは、遅滞なく情報主体の要求に応じて個人情報処理の全部を停止し、又は一部を停止しなければならない。ただし、次の各号の一にあたる場合には、情報主体の処理停止要求を拒絶することができる。

1. 法律に特段の規定があり、又は法令上の義務を守るために避けられない場合
2. 他人の生命・身体を害する恐れがあり、又は他人の財産その他の利益を不当に侵害する恐れがある場合
3. 公共機関が個人情報を処理しなければ他の法律に定める所管業務を行うことができない場合
4. 個人情報を処理しなければ情報主体との間で取り決めたサービスを提供することができないなど、契約の履行が困難な場合であって、情報主体がその契約の解約意思をはっきり明らかにしていない場合

③ 個人情報処理者は、第２項但書きによって処理停止の要求を拒絶したときは、情報主体に遅滞なくその事由を知らせなければならない。

④ 個人情報処理者は、情報主体の要求に応じて処理が停止された個人情報に対し、遅滞なく当該個人情報の破棄など必要な措置を講じなければならない。

⑤ 第１項から第３項までによる処理停止の要求、処理停止の拒絶、通知などの方法及び手続に必要な事項は、大統領令に定める。

次に、情報主体は個人情報処理者に対し、自己の個人情報処理を停止することを求めることができる。このときは、個人情報処理者は、法令上の規定などの制限的な事由に限らず、当該個人情報を処理しなければ契約履行が困難な場合であって情報主体がその契約の解約意思をはっきり明らかにしていない場合にも、個人情報処理の停止要求を拒絶することができる。かかる拒絶事由がなければ、個人情報処理者は処理停止を求められた日から１０日以内に当該個人情報の処理停止措置をとった事実（処理停止の要求に応じない法的根拠がある場合、その事実及び理由と異議申立方法）を情報主体に知らせなければならない。一方、情報主体は個人情報処理者が設けた方法や手続に従って処理停止を求めなければならない。

個人情報保護法第３９条の７（利用者の権利等に対する特例）

① 利用者は、情報通信サービスプロバイダーなどに対し、いつでも個人情報の収集・利用・提供などの同意を撤回することができる。

② 情報通信サービスプロバイダーなどは、第１項による同意の撤回、第３５条による個人情報

の閲覧、第３６条による訂正を求める方法を個人情報の収集方法より容易にしなければならない。

③ 情報通信サービスプロバイダーなどは、第１項に基づき同意を撤回すれば、遅滞なく収集された個人情報を復旧・再生できないよう破棄するなど、必要な措置を講じなければならない。

なお、現行の個人情報保護法は、情報通信サービス（オンラインサービス）に関して利用者がいつでも個人情報の収集・利用・提供などの同意を撤回できるという規定を設けている（個人情報保護法第３９条の７）。かかる同意撤回権は、情報主体自らが同意したものに限って同意を撤回できるので、情報主体自らが処理に同意していなくても個人情報処理者が処理している情報主体に関するすべての個人情報の処理停止を求められる処理停止要求権とは相違する。しかしながら、２０２３年9月１５日施行される改正個人情報保護法のもとでは、情報通信サービスプロバイダーに対する特例規定である第３９条の７が削除され、当該内容は前述の従来の第３７条（個人情報の処理停止など）の規定でカバーされている[21]。

最後に、個人情報保護法は情報主体の破棄要求権に関する明示的な規定を設けていないが、情報主体は個人情報の漏洩などの被害を防止し、自分の個人情報が誤用・濫用にならないよう、個人情報の処理目的が達成されるなど個人情報を保管し続ける必要性がなくなったときは、個人情報処理者に自己の個人情報の破棄を求めることができる[22]。

ウ．最近の改正により一層能動的な自己情報統制権を実現

２０２３年3月１４日公布された改正個人情報保護法に基づき、情報主体の権利に関して次の規定が新設された。

1) 個人情報の転送要求

個人情報保護法第３５条の２（個人情報の転送要求）

① 情報主体は、個人情報処理能力などを考慮して大統領令の定める基準にあたる個人情報処理者に対し、次の各号の要件をいずれも満たすときは、個人情報処理者が処理する自己の個人情報を自己に転送することを求めることができる。

1. 情報主体が転送を求める個人情報が情報主体の本人に関する個人情報であって、次の各目の一にあたる情報であること

ア．第１５条第１項第１号、第２３条第１項第１号又は第２４条第１項第１号による同

[21] 情報主体が同意を撤回した場合、前述の処理停止拒絶事由に該当しなければ、個人情報処理者は遅滞なく収集された個人情報を復旧・再生できないように破棄するなど必要な措置を講じなければならない（２０２３年９月１５日施行される改正個人情報保護法第３７条第３項）。

[22] 個人情報保護委員会、「個人情報保護法令及び指針・告示解説」、２０２０年１２月、３４頁。

意を得て処理される個人情報

イ．第１５条第１項第４号に基づいて締結した契約を履行し、又は契約を締結する過程で情報主体の要請による措置を履行するために処理される個人情報

ウ．第１５条第１項第２号、同項第３号、第２３条第１項第２号又は第２４条第１項第２号に基づいて処理される個人情報のうち、情報主体の利益又は共益的目的のために関係中央行政機関の長からの要請に応じて保護委員会が審議・議決して転送要求の対象に指定した個人情報

2. 転送を求める個人情報が、個人情報処理者が収集した個人情報に基づいて分析・加工して別途生成した情報でないこと

3. 転送を求める個人情報がコンピューターなど情報処理装置で処理される個人情報であること

② 情報主体は、売上高、個人情報の規模、個人情報処理能力、産業別の特性などを考慮し、大統領令の定める基準にあたる個人情報処理者に対し、第１項による転送要求対象である個人情報を技術的に許容される合理的な範囲内で、次の各号の者に転送することを求めることができる。

1. 第３５条の３第１項による個人情報管理専門機関

2. 第２９条による安全措置義務を履行し、大統領令の定める施設及び技術基準を満たす者

③ 個人情報処理者は、第１項及び第２項による転送を求められた場合には、時間、費用、技術的に許容される合理的な範囲内で当該情報をコンピューターなど情報処理装置で処理可能な形態で転送しなければならない。

④ 第１項及び第２項による転送要求を受けた個人情報処理者は、次の各号の一にあたる法律の関連規定にも拘わらず、情報主体に関する個人情報を転送しなければならない。

1. 「国税基本法」第８１条の１３

2. 「地方税基本法」第８６条

3. その他第１号から第２号までの規定に類似する規定であって、大統領令に定める法律の規定

⑤ 個人情報処理者は、情報主体が本人であるかどうかが確認されない場合など大統領令に定める場合には、第１項及び第２項による転送要求を拒絶・中断することができる。

⑥ 情報主体は、第１項及び第２項による転送要求により、他人の権利又は正当な利益を侵害してはならない。

⑦ 第１項から第６項までの事項以外に、転送要求の対象になる情報の範囲、転送を求める方法、情報を転送・拒否する方法、転送要求の拒絶及び転送中断の方法など必要な事項は大統領令に定める。

従来の個人情報保護法は、ＧＤＰＲの個人情報移動権規定（第２０条 Right to data portability）に相応する権利に関する規定を導入していなかった。しかしながら、個人信用情報（個人情報の中でも個人の信用度や信用取引能力を把握するために必要な情報）に適用される特別法である「信用情報の利用及び保護に関する法律」は、個人信用情報に対する転送要求権の規定（第３３条の２）[23]を設

[23] 「信用情報の利用及び保護に関する法律」上の転送要求権規定は２０２１年８月４日施行された。これは、

けていた。この点、一般法である個人情報保護法にも一般的権利として個人情報の転送要求権規定を導入するために、２０２３年3月１４日公布された改正個人情報保護法のもとで個人情報の転送要求権規定が新設された[24]。

情報主体は、一定規模以上の個人情報処理者に対して自己の個人情報を本人、その他の個人情報処理者又は個人情報管理専門機関に転送することを求めることができ、個人情報処理者は時間、費用、技術的に許容される合理的な範囲内で当該情報を情報処理装置（コンピューターなど）で処理可能な形態で転送しなければならない。

この新設規定の詳細は、今後立法される個人情報保護法の施行令に盛り込まれるが、公布された法律規定の内容は概ねＧＤＰＲの転送要求権規定の内容に類似するものと思われる。しかしながら、情報主体が自己ではない第三者に個人情報の転送を求めるにおいて、技術的に可能な場合（where technically feasible）、他の個人情報処理者に個人情報を直接移転する権利がある旨が示されたＧＤＰＲ第２０条とは異なり、改正個人情報保護法第３５条の２によれば、情報主体は一定の基準（売上高、個人情報の規模、個人情報の処理能力、産業別特性など）にあたる個人情報処理者のみに対して転送を求めることができ、個人情報の転送を受ける者も個人情報管理専門機関又は一定の基準（法律による安全措置義務を履行し、一定の施設及び技術基準を満たさなければならない）にあたる者に限られる。これらの点で、改正個人情報保護法の転送要求権の規定は、ＧＤＰＲの転送要求権に比べて一部限られた範囲の権利を規定するものとみられる。

2) 自動化した決定に対する情報主体の権利

個人情報保護法第３７条の２（自動化した決定に対する情報主体の権利など）

① 情報主体は、完全に自動化したシステム（人工知能技術を適用したシステムを含む）で個人情報を処理して行われる決定が、自己の権利又は義務に重大な影響を及ぼすときは、その個人情報処理者に対して当該決定を拒否し、又はその決定に対する説明などを求めることができる。ただし、自動化した決定に対する拒否は、個人情報が第１５条第１項第３号又は第５号から第７号までの規定によって処理される場合に限って行うことができる。

② 個人情報処理者は、第１項に基づいて情報主体が自動化した決定を拒否し、又はこれに対する説明などを求めたときは、正当な事由がない限り、自動化した決定の適用を排除し、又は人的介入による再処理・説明など必要な措置を講じなければならない。

③ 個人情報処理者は、自動化した決定の基準と手続を情報主体が容易に確認できるよう開示するなど必要な措置を講じなければならない。

信用情報主体である個人が、金融会社、公共機関などに提供した本人の個人信用情報を本人や本人の信用情報管理会社（マイデータ事業者）、個人信用格付け会社などに転送することを求める権利に関して規定している。

[24] ただし、本規定の施行日は、公布（２０２３年3月１４日）から１年が経過した日から公布後２年が過ぎない範囲で大統領令に定める日とし｛個人情報保護法付則第１条第２号（２０２３年3月１４日法律第１９２３４号に改正されたもの）｝、２０２３年7月11日を基準に未だ指定されていない（２０２３年5月１８日付けで立法予告された個人情報保護法施行令改正案には当該内容なし）。

④　第１項から第３項までの事項以外に自動化した決定の基準・手続の開示などに必要な事項は大統領令に定める。

２０２４年3月１５日施行される改正個人情報保護法のもとでは、ＧＤＰＲの自動化した意思決定規定（第２２条 Automated individual decision-making, including profiling）に相応する権利として、自動化した決定に対する情報主体の権利規定が新設された。

情報主体は、完全に自動化したたシステム（人工知能技術を適用したシステムを含む）で個人情報を処理して行われる決定に対し、これを拒否したり当該決定に対する説明などを求めることができる。個人情報処理者は、かかる情報主体の要求に対し、正当な事由がない限り、自動化した決定の適用を排除したり、人的介入による再処理・説明など必要な措置を講じなければならない。さらに、個人情報処理者は、自動化した決定の基準や手続を情報主体にわかりやすく開示するなど、必要な措置を講じなければならない。

この新設規定の詳細も今後立法が行われる個人情報保護法施行令に盛り込まれることが見込まれ、公布された法律規定の内容は概ねＧＤＰＲの自動化した意思決定の規定に類似すると思われる。

2.　司法的救済システムによる情報主体の被害救済

個人情報保護法は、前述の第４条第５号における情報主体の権利、すなわち個人情報の処理による被害を迅速且つ公正な手続によって救済を受ける権利を保障するために、民法や民事訴訟法などの一般法の法理とは別に損害賠償を請求したり権利侵害の禁止・中止を請求できる権利に関する規定を整備している。

ア．個人情報保護法による損害賠償請求

1)　立証責任が転換された損害賠償請求

個人情報保護法第３９条（損害賠償責任）

①　情報主体は、個人情報処理者が同法に違反した行為によって損害を被った場合、個人情報処理者に損害賠償を請求することができる。この場合、その個人情報処理者は故意又は過失がないことを立証しなければ、責任を免れることができない。

個人情報処理者の責に帰すべき事由による個人情報の漏洩などの事故が発生し、それによって情報主体が損害を被った場合、情報主体は個人情報処理者に民法上の不法行為（民法第７５０条）に基づく損害賠償を請求することができる[25]。ただし、このとき、情報主体（原告）は個人情報処理者（被

[25] 情報主体は個人情報処理者に対して債務不履行（契約不履行）に基づく損害賠償を請求することも可能であり（不法行為とは請求権競合関係にあり、債務者である情報主体は2つの損害賠償請求権のいずれでも選択して

告）の故意又は過失があったことを立証する責任があるが、その立証に必要な情報の所在の不均衡などにより、個人である情報主体が、主に企業や団体又は公共機関であることが多い個人情報処理者の故意又は過失を具体的に立証することは現実的に極めて難しい。よって、情報主体をして個人情報処理者の故意又は過失を証明させることは、事実上、情報主体の被害が救済されることを著しく困難にする結果を招く。

これらの点を踏まえ、個人情報保護法第３９条は、同法の規定に違反した行為によって情報主体が損害を被った場合、個人情報処理者に自ら故意又は過失がないことを証明する責任を負わせることで、情報主体の権利の一つとされる迅速且つ公正な被害救済を受ける権利を実質的に保障するとともに、個人情報処理者の遵法率を高めることを目指している[26]。

すなわち、個人情報保護法第３９条による損害賠償請求権は、（ⅰ）個人情報処理者の個人情報保護法の違反行為に（ⅱ）よって（違法行為と損害との因果関係）（ⅲ）損害を被ったという3つの要件を立証すれば行使することができる。このとき、損害は、財産的損害（例えば、クレジットカード番号、住民登録番号などの漏洩によるクレジットカードの不正使用、不法ローンなどにより財産的損失）と、精神的損害（例えば、メールアドレス、電話番号などの漏洩により情報主体の意思に反して迷惑メール、マーケティング広告などが受信されることによる非財産的被害）をいずれもいう[27]。

情報主体は、上記の損害賠償請求権の行使要件のうち、（ⅲ）損害が発生したこと並びにその損害額を立証しなければならないが、大法院はこれについて（特に精神的損害について）、諸事情を総合考慮してその裁量により損害額（慰謝料の額）を定めることができるという立場である。具体的に、「個人情報を処理する者が収集した個人情報が、情報主体の意思に反して漏洩された場合、それによって情報主体に慰謝料で賠償するに足りる精神的損害が発生したかどうかは、漏洩された個人情報の種類と性格は何か、個人情報の漏洩により情報主体を識別する可能性が発生したかどうか、第三者が漏洩された個人情報を閲覧したかどうか又は第三者の閲覧有無が明らかになっていなければ第三者による閲覧可能性があるかどうか、今後閲覧される可能性があるかどうか、漏洩された個人情報がどの範囲まで拡散したかどうか、個人情報の漏洩により更なる法益侵害の可能性が発生したかどうか、個人情報を処理する者が個人情報を管理してきた実態と個人情報が漏洩された具体的な経緯、個人情報の漏洩による被害の発生・拡散を防ぐために如何なる措置が講じられたのかなど、諸事情を総合考慮

行使することができる）、この場合には債務者（個人情報処理者）が自己の故意又は過失がないことを立証しなければならない（民法第３９０条）。しかし、この場合にも、債権者（情報主体）は、債務者（個人情報処理者）に個人情報の漏洩などの事故において責に帰すべき事由があるという事実及び債務者が債務の内容による履行をしないことによって債権者が損害を被ったという点を立証しなければならない。一方、個人情報保護法上、損害賠償請求権は個人情報処理者が「個人情報保護法に違反した行為」により情報主体が損害を被ったという点さえ立証すれば良いため、原告である情報主体にとっては民法上の債務不履行に基づく損害賠償請求権の行使に比べて個人情報保護法上の損害賠償請求権を行使したほうが有利であるといえる。

[26] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、３９４～３９５頁。

[27] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、３９２～３９３頁。

して具体的な事件に応じて個別に判断しなければならない」と判示し（大法院２０１２年１２月２６日宣告２０１１ダ５９８３４、５９８５８、５９８４１判決など参照）、不法行為による精神的苦痛に対する慰謝料の額に関しては「事実審の法院が諸事情を斟酌してその職権に属する裁量によって定めることができる」と判断した（大法院２０１８年１０月２５日宣告、２０１８ダ２１９３５２、判決[28]）。

2) 懲罰的損害賠償

個人情報保護法第３９条（損害賠償責任）

③ 個人情報処理者の故意又は重大な過失により、個人情報が紛失・盗難・漏洩・偽造・変造又は毀損された場合であって、情報主体に損害が発生したときは、法院はその損害額の３倍[29]を超えない範囲内で損害賠償額を定めることができる。ただし、個人情報処理者が故意又は重大な過失がないことを証明したときは、その限りではない。

④ 法院は、第３項の賠償額を定めるときは、次の各号の事項を考慮しなければならない。

1. 故意又は損害発生の恐れを認識した程度
2. 違反行為によって被った被害の規模
3. 違反行為によって個人情報処理者が取得した経済的利益
4. 違反行為による罰金及び課徴金
5. 違反行為の期間・回数など
6. 個人情報処理者の財産状態
7. 個人情報処理者が情報主体の個人情報紛失・盗難・漏洩後、その個人情報を回収するために努力した程度
8. 個人情報処理者が情報主体の被害救済のために努力した程度

個人情報処理者が単に個人情報保護法に違反したことにとどまらず、個人情報処理者の故意又は重大な過失により個人情報が紛失・盗難・漏洩・偽造・変造又は毀損された場合のように、侵害行為の可罰性が高い場合、個人情報保護法は情報主体の被害救済強化のために法院をして実損害の３倍（２０２３年９月１５日施行される改正個人情報保護法においては５倍）を超えない範囲で懲罰的損害賠償を許容している。一方では、不合理に過度な賠償にならないよう、かかる懲罰的損害賠償額を算定するにあたり、法院は多様な要素を総合考慮して判断することを義務付けている。

---

[28] 当該ケースにおいて、被告（クレジットカード会社）は個人情報保護法など関連法令などに違反してセキュリティソフトのインストール及び管理・監督義務などセキュリティ措置を取る義務を果たしておらず、個人情報が漏洩された原告らに対して不法行為による損害賠償責任が認められた。法院は、そのクレジットカードの顧客情報漏洩事故によって漏洩された個人情報は原告ら個人を識別できるだけでなく、個人の私生活及び信用と密接な関わりのある情報であり、漏洩事故の全般的な経緯などを総合してみれば、その伝播及び拡散過程で既に第三者によって閲覧されたか、今後個人情報が閲覧される可能性が高いので、社会通念上、原告らに個人情報の漏洩による精神的損害が現実的に発生したとされるのが妥当であるとし、諸事情を考慮して被告が原告らに賠償すべき慰謝料をそれぞれ１０万ウォンとした。

[29] ２０２３年９月１５日施行される改正個人情報保護法によれば、この限度は５倍に引き上げられる。

3) 法定損害賠償

個人情報保護法第３９条の２（法定損害賠償の請求）

① 第３９条第１項にも拘わらず、情報主体は個人情報処理者の故意又は過失により、個人情報が紛失・盗難・漏洩・偽造・変造又は毀損された場合には、３００万ウォン以下の範囲で相当の金額を損害額にして賠償を請求することができる。この場合、当該個人情報処理者は故意又は過失がないことを立証しなければ、責任を免れることができない。

② 法院は、第１項による請求がある場合、弁論全体の趣旨と証拠調査の結果を考慮して第１項の範囲で相当の損害額を認めることができる。

③ 第３９条に基づき、損害賠償を請求した情報主体は、事実審の弁論が終結する前までその請求を第１項による請求に変えることができる。

情報主体は、前述の個人情報保護法第３９条に基づき、一般的な損害賠償の法理に比べてより容易に個人情報処理者に対して損害賠償を請求することができる。それにも拘らず、大量の個人情報の漏洩などの事故があった場合、被害者である情報主体としては自ら被った被害の規模さえも具体的に算定することが難しいことが多い。

すなわち、個人情報保護法第３９条の請求権の要件である「違反行為によって損害が発生したこと」に関し、損害が発生したという事実及びその損害額を立証することそのものが現実的に困難なことがある。例えば、財産的被害については、個人情報を違法に利用して不法ローンを受けたり不法な取引により情報主体の財産の損失が発生しない限り、個人情報の漏洩だけで財産上の損害を認めることは容易ではない。さらに、精神的損害についても、法院は、前述のとおり、漏洩された個人情報の種類と性格、個人情報の漏洩による情報主体の識別可能性の発生有無など諸事情を総合考慮して事件に応じて精神的損害の認定有無を個別に判断するため、被害者である情報主体が個人情報の漏洩などによって精神的損害が発生したという事実や具体的に被った損害規模を証明することは困難である[30]。

こうした背景のもと、大量の個人情報漏洩事故において個人に過ぎない被害者（情報主体）を損害から容易に救済されるようにする一方、個人情報処理者に個人情報保護責任を実質的に負わせるために、個人情報保護法は法定損害賠償制度を設けている。

これによれば、情報主体は、損害賠償請求権を行使するために具体的な損害額を証する必要がなく、個人情報処理者の故意又は過失により個人情報の紛失・盗難・漏洩・偽造・変造又は毀損によって損害が発生したことさえ主張すれば、法院が弁論全体の趣旨と証拠調査の結果を考慮して３００万ウォンの範囲で相当の損害額を認めることができる。

このときも、個人情報処理者の故意又は過失の不存在に対する立証責任は被告である個人情報処理

[30] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、３９８頁。

者が負担することから、民法上の不法行為の法理による損害賠償請求（原告が被告の故意又は過失の存在を立証しなければならない）に比べて故意又は過失に対する証明責任が転換されている。

情報主体は、個人情報保護法第３９条による損害賠償を請求したにも拘らず、事実審の弁論が終結する前にはいつでもその請求を法定損害賠償請求に変えることができる（個人情報保護法第３９条の２第３項）[31]。従って、原告（情報主体）が第３９条による損害賠償請求訴訟で実損害の証明が困難になっても、事実審の弁論が終結する前であれば、第３９条の２による損害賠償請求に変えることにより最小限の権利救済が行われるようにすることができる。

イ．損害賠償の保障

個人情報保護法第３９条の９（損害賠償の保障）

① 情報通信サービスプロバイダーなどは、第３９条及び第３９条の２による損害賠償責任の履行のために保険又は共済に加入し、又は準備金を積み立てるなど必要な措置を講じなければならない。

② 第１項による加入対象になる個人情報処理者の範囲、基準などに必要な事項は大統領令に定める。

個人情報保護法は、情報通信サービスの利用者が個人情報保護法第３９条及び第３９条の２に基づいて個人情報処理者である情報通信サービスプロバイダーに損害賠償を請求する場合、その賠償責任の履行を保障するために、一定基準以上の売上高及び利用者数以上の情報通信サービスプロバイダーに保険や共済に加入するなど必要な措置を取らせている。

本規定は当初、情報通信技術の発達によって個人情報の漏洩による利用者の被害事例が増える中で、情報通信サービスプロバイダーに賠償能力がなく利用者に損害が賠償されない状況を防ぐために導入された特例規定である[32]。しかし、２０２３年３月１４日公布された改正個人情報保護法のもとで情報通信サービスプロバイダーに対する特例規定が一概に削除されたことにより、当該内容は２０２４年３月１５日施行される改正個人情報保護法の新設規定第３９条の７に移管され、その適用対象も情報通信サービスプロバイダーではない個人情報処理者一般に拡大した。

---

[31] 明文の規定はないが、権利救済の実効性の強化を図る趣旨を踏まえ、法定損害賠償を請求した情報主体が事実審の弁論終結前までに実損害を証明することにより、個人情報保護法第３９条による損害賠償請求に変えることも可能とされる（個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、４０１頁）。

[32] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、４５６～４５７頁。

ウ．団体訴訟

個人情報保護法第５１条（団体訴訟の対象等）

次の各号の一にあたる団体は、個人情報処理者が第４９条による集団紛争調停を拒否し、又は集団紛争調停の結果を受諾しないときは、法院に権利侵害行為の禁止・中止を求める訴訟（以下「団体訴訟」という）を申し立てることができる。

1. 「消費者基本法」第２９条に基づき、公正取引委員会に登録した消費者団体であって、次の各目の要件をいずれも備えた団体
   ア．定款によって常時的に情報主体の権益増進を主な目的とする団体であること
   イ．団体の正会員数が１千人以上であること
   ウ．「消費者基本法」第２９条による登録から３年が経過していること
2. 「非営利民間団体支援法」第２条による非営利民間団体であって、次の各目の要件をいずれも備えた団体
   ア．法律上又は事実上、同じ侵害を被った１００人以上の情報主体から団体訴訟の申立てを求められていること
   イ．定款に個人情報の保護を団体の目的に掲げた後、直近３年以上、そのための活動実績があること
   ウ．団体の常時構成員数が５千人以上であること
   エ．中央行政機関に登録されていること

市場経済の持続的な発展、情報通信技術の急激な発達などにより、個人情報侵害被害の拡散速度は速くなっており、その被害規模もますます大型化している一方、個人情報侵害被害を被る不特定多数の個人は依然として非組織化・破片化の状況にとどまっている。このように、個人情報侵害誘発者と侵害被害者との非対称性により、個人情報の侵害に対する被害救済を情報主体である個人だけに任せる場合、実質的な被害救済が行われない問題が発生し得る[33]。

とりわけ、個人情報に係る侵害行為の中でも、個人情報の目的外利用・提供又は収集目的を達成した個人情報の未破棄など、情報主体の権利を侵害する行為については、個別の情報主体は被害事実がわかりにくく、かかる権利侵害行為が持続するだけでなく、今後情報主体が到底予期せぬ方向に２次、３次被害が起きる可能性が高い。例えば、個人情報の目的外利用・提供においては、情報主体が予期できないほどに当初の収集・利用目的を逸脱した目的で個人情報が利用されたり、情報主体に知られていない第三者に個人情報が提供される場合、情報主体は自己の個人情報の開示や利用に関して自ら決める権利、すなわち個人情報自己決定権が著しく侵害される。

さらに、このような権利侵害行為による被害は、個別の情報主体ではなく、当該侵害行為によって被害を被る全体被害者の利益のために一概に禁止・中止されることが求められ、これによってはじめて個人情報保護法第４条第５号における情報主体の権利、すなわち個人情報の処理によって発生した

[33] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、５０９～５１０頁。

被害から迅速且つ公正な手続によって救済される権利が実質的に保障されることができる。

これらの点を総合考慮し、個人情報保護法は２０１１年制定当時、欧州型団体訴訟（Verbands-klage）[34]を導入した。これにより、一定の基準を備えた消費者団体や非営利民間団体は、個人情報の目的外利用・提供や個人情報の閲覧禁止など個人情報の処理に係る情報主体の権利侵害行為に対して禁止・中止を請求することができる。このとき、訴訟の対象は訴の申立て当時から続いている個人情報に係る権利侵害行為なので、訴の申立て当時、その行為が終了したり訴訟進行中に禁止・中止された場合、その訴訟は特段の事情がない限り、訴訟の利益を失って却下される。さらに、権利侵害行為の禁止・中止請求ではない金銭的被害救済請求は、団体訴訟によって申し立てることができないため、損害賠償などの請求は被害者である情報主体個人が前述の個人情報保護法第３９条などに基づいて行わなければならない。

個人情報保護法第５３条（訴訟代理人の選任）
団体訴訟の原告は、弁護士を訴訟代理人に選任しなければならない。

個人情報保護法第５４条（訴訟許可申請）
① 団体訴訟を申し立てる団体は、訴状とともに次の各号の事項を記載した訴訟許可申請書を法院に提出しなければならない。
1. 原告及びその訴訟代理人
2. 被告
3. 情報主体の侵害された権利の内容

② 第１項による訴訟許可申請書には、次の各号の資料を添付しなければならない。
1. 提訴団体が第５１条各号の一にあたる要件を備えていることを疎明する資料
2. 個人情報処理者が調停を拒否し、又は調停結果を受諾しなかったことを証明する書類

個人情報保護法第５５条（訴訟許可要件など）
① 法院は、次の各号の要件をいずれも備えた場合に限って、決定により団体訴訟を許可する。
1. 個人情報処理者が紛争調停委員会の調停を拒否し、又は調停結果を受諾しなかったこと
2. 第５４条による訴訟許可申請書の記載事項に欠缺がないこと

② 団体訴訟を許可し、又は許可しない決定に対しては、即時抗告することができる。

個人情報保護法第５６条（確定判決の効力）
原告の請求を棄却する判決が確定した場合、これと同じ事案に関しては第５１条による他の団体は団体訴訟を申し立てることができない。ただし、次の各号の一にあたる場合には、その限りで

[34] 一定の資格を備えた団体が多数の被害者らの利益のための訴訟を申し立てる権限が与えられる制度であり、ドイツ式団体訴訟制度を受け入れたものと理解されている（チョ・マンヒョン、「個人情報保護法上の団体訴訟に関する小考」、土地工法研究第６０巻、２０１３、３７３頁）。これは、多数の被害者のうち個人（代表当事者）が被害者集団全体のために訴訟を申し立てる集団訴訟（Class Action）と相違する。

はない。
1. 判決が確定した後、その事案に関して国・地方自治体又は国・地方自治体が設立した機関によって新しい証拠が現われた場合
2. 棄却判決が原告の故意によるものであることが判明した場合

一方、不必要な訴訟の濫用を防ぐために、個人情報団体訴訟は必ず個人情報集団紛争調停手続を経る必要があり、管轄法院に訴訟許可申請書を提出して訴訟許可決定を得て申し立てることができる。

団体訴訟の確定判決の効力は他の団体へ及び、当該事案と同じ事案に関しては他の団体が改めて団体訴訟を申し立てることができない。しかしながら、当該効力は個別の情報主体へ及ぶものではないので、情報主体の個人は団体訴訟の結果に関係なく、自ら権利侵害行為の禁止・中止を請求する訴訟（例えば、民法上の不法行為の中止又は差止請求訴訟など）を申し立てることができる。

3. 制裁システムによる個人情報処理者の義務履行の強制

前述の１.と２.での内容は、情報主体が自ら行使することができる個人情報自己決定権の内容と範囲を定めることで、情報主体の個人情報自己決定権が実現されるようにするものだった。本項目では、個人情報保護に係る政府の主務機関である個人情報保護委員会[35]が行政的・刑事的な制裁手段を通じて個人情報処理者の義務履行を強制し、情報主体の個人情報自己決定権の行使が実際に個人情報自己決定権の実現につながるよう担保する内容について取り上げる。

ア．行政制裁手段

1) 資料提出の要求及び検査

個人情報保護法第６３条（資料提出の要求及び検査）
① 保護委員会は、次の各号の一にあたる場合には、個人情報処理者に関係物品・書類など資料を提出させることができる。
1. この法に違反する事項を見つけ、又は嫌疑があることを知った場合
2. この法の違反に対する通報を受け、又は苦情が受理された場合
3. その他情報主体の個人情報保護のために必要な場合であって大統領令に定める場合
② 保護委員会は、個人情報処理者が第１項による資料を提出せず、又はこの法に違反した事実があると認められれば、所属の公務員をして個人情報処理者及び当該法の違反事実に係る関

[35] 個人情報保護に関する事務を独立して行うための国務総理所属の中央行政機関（個人情報保護法第７条第１項及び第２項）。

係人の事務所又は事業場に出入りして業務状況、帳簿又は書類などを検査させることができる。この場合、検査を行う公務員は、その権限を表す証票を持参し、それを関係人に提示しなければならない。

③ 関係中央行政機関の長は、所管の法律に基づいて個人情報処理者に第１項による資料の提出を要求し、又は個人情報処理者及び当該法の違反事実に係る関係人に対して第２項による検査を行うことができる。

個人情報保護委員会は、個人情報保護法の違反行為などを調べて確認するために、個人情報処理者に資料の提出を求めたり、個人情報処理者の事務所や事業場に出入りして関連資料の検査を行うことができる。対象になる個人情報処理者には、公共機関に限らず民間企業や団体も含まれ、法執行の統一性や一貫性を維持するために、金融機関、医療機関、教育機関、通信キャリアなど他の部処所管の民間企業や団体に対しても、資料提出の要求や事務所などへの出入り・検査が可能とされる。

ただし、個人情報の保護に係る所管の法律である個別法（例えば「信用情報の利用及び保護に関する法律」など）において、関係中央行政機関の長に資料提出の要求又は事務所などの出入り・検査権限を与えている場合には、その分野ならではの特殊性や自律性を尊重するために、関係中央行政機関の長にも当該所管法律による資料提出の要求又は事務所などへの出入り・検査が可能であるという規定も併せて設けている（個人情報保護法第６３条第３項）[36]。

2) 是正措置、過料又は課徴金

個人情報保護法第６４条（是正措置など）

① 保護委員会は、個人情報が侵害されたと判断するに足りる相当の根拠があり、それを放置した場合には回復し難い被害を被る恐れがあると認められれば、この法に違反した者（中央行政機関、地方自治体、国会、法院、憲法裁判所、中央選挙管理委員会は除く）に対して次の各号にあたる措置を命ずることができる。

1. 個人情報侵害行為の中止
2. 個人情報処理の一時的な停止
3. その他個人情報の保護及び侵害防止に必要な措置[37]

② 関係中央行政機関の長は、個人情報が侵害されたと判断する相当の根拠があり、これを放置する場合、回復し難い被害を被る恐れがあると認められれば、所管の法律に基づいて個人情

[36] ２０２３年９月１５日施行される改正個人情報保護法のもとでは、関係中央行政機関の長の権限に関する内容が削除され、個人情報保護に係る法規の違反行為によって重大な個人情報侵害事故が発生した場合、関係機関の長に協力を求めることができるという旨が新設される。一方、新設規定である第６３条の２を通じ、法違反の疑いや通報がなくても、個人情報の侵害事故が発生する危険性が高く、個人情報保護の脆弱点を事前に点検する必要性が認められる個人情報処理者に対する個人情報保護実態の事前点検に関する根拠規定を設ける。

[37] 個人情報漏洩サイトの遮断、技術的・管理的保護措置、個人情報処理方針又は約款の改正などが盛り込まれることができる（個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、５５４頁）。

報処理者に対して第１項各号にあたる措置を命ずることができる。
③ 地方自治体、国会、法院、憲法裁判所、中央選挙管理委員会は、その所属機関及び所管の公共機関が同法に違反したときは、第１項各号にあたる措置を命ずることができる。
④ 保護委員会は、中央行政機関、地方自治体、国会、法院、憲法裁判所、中央選挙管理委員会がこの法に違反したときは、当該機関の長に第１項各号にあたる措置を取るよう勧告することができる。この場合、勧告を受けた機関は、特段の事由がない限り、これを尊重しなければならない。

個人情報保護委員会又は関係中央行政機関の長は、通報、調査などによって個人情報処理者の法違反事実を確認し、その法の違反によって個人情報が侵害されたと判断するに足りる相当の根拠があり、これを放置すれば回復し難い被害を被る恐れがあると認める場合、個人情報侵害行為の中止など個人情報の保護及び侵害防止のために必要な是正措置を命ずることができる[38]。

さらに、個人情報保護委員会又は関係中央行政機関の長は、個人情報保護法第７５条に定める事由にあたる個人情報処理者に（事由に応じて）５千万ウォン以下、３千万ウォン以下、２千万ウォン以下又は１千万ウォン以下の過料を賦課することができる。行政秩序罰である過料は、概ね個人情報保護責任者の未指定、個人情報処理方針の未公開など、個人情報保護法における手続や基準に違反した場合に賦課される。

一方、個人情報保護委員会は、情報通信サービスプロバイダーが個人情報保護法に違反した一定の場合、その違反行為に係る売上高の１００分の３以下にあたる金額（売上高がないか売上高の算定が困難な場合は、４億ウォン以下の金額）を課徴金[39]として賦課することができる（個人情報保護法第３９条の１５）。本規定は、情報通信サービスプロバイダーに限って適用される特例規定であるが、２０２３年９月１５日施行される改正個人情報保護法のもとでは、情報通信サービスプロバイダーに対する特例規定が一括削除されることによって第３９条の１５が削除され、新設規定である第６４条の２に関連内容が移される。

さらに、改正法のもとでは、情報通信サービスプロバイダーに適用される課徴金は個人情報処理者全体に拡大し、３％課徴金の上限額の基準は「違反行為に係る売上高」から「全体売上高」に変わっ

[38] ２０２３年９月１５日施行される改正個人情報保護法のもとでは、「個人情報が侵害されたと判断する相当の根拠があり、それを放置すれば回復し難い被害が生じる恐れがあると認められれば」という要件を削除し、是正措置要件を緩和する。

[39] 課徴金は、行政法上の義務に違反した者に経済的利益が発生した場合、その利益を奪って間接的に義務の履行を確保するために賦課する制裁的金銭負担の性格を有する。これは、売上高などを考慮して算定され、課徴金の賦課は行政審判や行政訴訟により取消しを請求しなければならない。一方、過料は、過去の義務違反に対して一定の制裁を加えることにより、行政法規の違反に対する処罰を目的とする行政秩序罰の一種であり、可罰性の程度によって過料の限度額が決まり、不服の際に「非訟事件手続法」に基づいて異議申立をしなければならない。
ちなみに、課徴金を賦課した行為に対しては、過料を賦課することができない（個人情報保護法第７６条）。

たが[40]、課徴金を算定するときは違反行為と関わりのない売上高は除外される。

3) 是正措置命令などの内容及び結果の公表

個人情報保護法第６６条（結果の公表）

① 保護委員会は、第６１条による改善勧告、第６４条による是正措置命令、第６５条による告発又は懲戒勧告及び第７５条による過料賦課の内容及び結果に対して公表することができる。

② 関係中央行政機関の長は、所管法律に基づいて第１項による公表を行うことができる。

③ 第１項及び第２項による公表の方法、基準及び手続などは、大統領令に定める。

個人情報保護委員会又は関係中央行政機関の長は、前述の行政処分及び後述する告発などの内容と結果をインターネットのホームページや一般の日刊新聞などに公表することができる[41]。この制度は、個人情報保護法の違反に対する行政処分結果を公開することにより、個人情報処理者の警戒心を高めるために施行されている。

イ．刑事告発権

個人情報保護法第６５条（告発及び懲戒勧告）

① 保護委員会は、個人情報処理者に同法など個人情報保護に係る法規の違反による犯罪の疑いがあると認められるに足りる相当の理由があるときは、管轄の捜査機関にその内容を告発することができる。

② 保護委員会は、同法など個人情報保護に係る法規の違反行為があると認められるに足りる相当の理由があるときは、責任がある者（代表者及び責任のある役員を含む）を懲戒することを当該個人情報処理者に勧告することができる。この場合、勧告を受けた者は、これを尊重しなければならず、その結果を保護委員会に知らせなければならない。

③ 関係中央行政機関の長は、所管法律に基づいて個人情報処理者に対して第１項による告発をし、又は所属機関・団体などの長に第２項による懲戒勧告を行うことができる。この場合、第２項による勧告を受けた者は、これを尊重しなければならず、その結果を関係中央行政機関の長に知らせなければならない。

個人情報保護委員会又は関係中央行政機関の長は、個人情報の保護に係る法規違反による犯罪の疑いがあると認められるに足りる相当の理由があれば、管轄の捜査機関にその内容を告発することがで

---

[40] グローバル立法傾向（ＥＵ及びイギリスは全世界売上高の４％、中国は前年度売上高の５％、シンガポールは前年度売上高の１０％、米国は違反個別件当たり最大１万ドル）に合わせて課徴金の実効性を確保するためである（個人情報保護委員会２０２３年3月7日付けプレスリリース１５頁）。

[41] ２０２３年9月１５日施行される改正個人情報保護法のもとでは、関係中央行政機関の長の公表権限に関する内容が削除され、個人情報保護委員会が関連処分を受けた者に当該処分を受けたという事実を公表することを命ずることができるという旨が新設される。

きる。個人情報保護法は、第７０条ないし第７３条において保護法益の重要性、予想される被害の規模及び社会的費用などに応じて４段階（１０年以下の懲役又は１億ウォン以下の罰金、５年以下の懲役又は５千万ウォン以下の罰金、３年以下の懲役又は３千万ウォン以下の罰金、２年以下の懲役又は２千万ウォン以下の罰金）に分けて刑事罰の規定を置いている。

ただし、経済制裁中心の国際基準[42]とは異なり、個人情報保護責任を企業よりは担当者個人への刑罰中心に規律している問題を改善するために、改正個人情報保護法（２０２３年9月１５日施行）のもとでは、前述のとおり、課徴金の実効性を確保する一方、過度な刑罰規定が一部削除された。

個人情報保護法第７４条（両罰規定）

① 法人の代表者や法人又は個人の代理人、使用人その他の従業員がその法人又は個人の業務に関して第７０条にあたる違反行為をすれば、その行為者を罰する以外にその法人又は個人を７千万ウォン以下の罰金に処する。ただし、法人又は個人がその違反行為を防止するために当該業務に関して相当の注意と監督を怠らなかった場合には、その限りではない。

② 法人の代表者や法人又は個人の代理人、使用人その他の従業員がその法人又は個人の業務に関して第７１条から第７３条までの一にあたる違反行為をすれば、その行為者を罰する以外にその法人又は個人にも当該条文の罰金刑を科する。ただし、法人又は個人がその違反行為を防止するために当該業務に関して相当の注意と監督を怠らなかった場合には、その限りではない。

一方、個人情報処理者の役職員、代理人などの業務処理に対する個人情報処理者の警戒心を高め、管理及び監督を強化するために、個人情報保護法は役職員、代理人などの法違反行為に対して当該行為者だけではなく、個人情報処理者も処罰する両罰規定を設けている。

診療データの二次利用に対する回答

④ 適用法令及び「患者に関する記録」の範囲

患者の健康に関する情報は、一次的に「個人情報保護法」上の敏感情報(個人情報保護法第23条第1項)に該当する。 ただし、個人情報保護法は、個人情報保護に関しては他の法律に特別な規定がある場合を除き、この法律で定めるところに従うと規定し(個人情報保護法第6条)、「**医療法**」は「**患者に関する記録**」に関する規定を設けている。 これと関連して、韓国政府の関連部署である保健福祉部は、医療機関が保有している患者に関する記録を第三者(外部者)に閲覧またはコピー発給などその内容の確認を提供する場合には医療法が優先的に適用されると解釈している(保健福祉部、2022年医療機関開設および医療法人設立運営便覧、217面)。

[42] 注４０を参照。

医療法が適用される患者に関する記録と関連して、医療法は第21条第1項で「(患者)本人に関する記録」の他に具体的な定義規定を設けてないが、保健福祉部は「患者に関する記録」には医療機関が患者の治療·診断過程で保有することとなったすべての記録が含まれ、診断書写本、処方箋写本、診療確認書、入退院確認書などの諸証明書も含まれると解釈している(保健福祉部、2022年医療機関開設及び医療法人設立運営便覧、237面)。

医療法　第21条（記録閲覧等）

⑤ 患者は医療人、医療機関の長及び医療機関従事者に本人に関する記録(追加記載·修正された場合、追加記載·修正された記録及び追加記載·修正前の原本をすべて含む。 以下同じ。）の全部又は一部について閲覧又はその写しの発給等内容の確認を要請することができる。 この場合において、医療関係者、医療機関の長及び医療機関従事者は、正当な理由がなければ、これを拒んではならない。

⑥ 患者に関する記録を二次利用するための要件

i. 医療法上、患者の同意が必要なのか、その他の義務が課せられているのか等

前述したように、医療法が適用される「患者に関する記録」は医療機関が保有する情報に限る。そこで本項目では、研究や医薬品開発などを目的とする第三者に患者に関する記録を医療機関が提供する場合、どのような要件を満たすべきかについて調べる。

まず医療機関は、患者本人でない他の者に患者に関する記録を閲覧させ、又はその写しを出すなど内容を確認できるようにしてはならないことが原則である（医療法第21条第2項）。 ただし、（i）**患者本人が同意した場合**であって、患者の親族又は**患者が指定する代理人が要請する場合、**（ii）患者が死亡し、又は意識がないなど患者の同意を得られないであって、患者の親族が要請する場合、又は（iii）関連法令で特別に定める場合には、例外的に患者に関する記録の内容を患者本人ではなく第三者に提供することができる(医療法第21条第3項)。

医療法　第21条（記録閲覧等）

② 医療人、医療機関の長及び医療機関従事者は、患者でない他の者に患者に関する記録を閲覧させ、又はその写しを出す等の内容を確認することができるようにしてはならない。

③ 第二項の規定にかかわらず、医療人、医療機関の長及び医療機関従事者は、次の各号のいずれかに該当する場合には、その記録を閲覧させ、又はその写しを交付する等その内容を確認することができるようにしなければならない。 ただし、医師·歯科医師又は漢方医が患者の診療のためにやむを得ないと認めた場合は、この限りでない。

4. 患者の配偶者、直系尊属·卑属、兄弟姉妹（患者の配偶者及び直系尊属·卑属、配偶者の直系尊属がすべてない場合に限る。）又は配偶者の直系尊属が患者本人の同意書と親族関係であることを示す証明書等を添付するなど保健福祉部令で定める要件を備えて要請した場合

5. 患者が指定する代理人が患者本人の同意書と代理権を有することを証明する書類を添付するなど保健福祉部令で定める要件を満たして要請した場合
6. 患者が死亡したり意識がないなど患者の同意を得ることができず、患者の配偶者、直系尊属·卑属、兄弟姉妹(患者の配偶者及び直系尊属·卑属、配偶者の直系尊属がすべてない場合に限る。）又は配偶者の直系尊属が親族関係であることを示す証明書等を添付するなど保健福祉部令で定める要件を備えて要請した場合
7. 「国民健康保険法」第14条、第47条、第48条及び第63条により給与費用審査·支給·対象有無確認·事後管理及び療養給付の適正性評価·加減支給等のために国民健康保険公団又は健康保険審査評価院に提供する場合

（以下第5号から第18号までは、第4号と類似して他の法令において特別の規定を設けている場合であって、省略する。）

ただし、このように患者が指定した代理人が患者に関する記録提供を要請するためには、代理人の身分証明書のコピー（すなわち、この時の代理人は自然人を意味するものと解釈される）、患者が自筆署名した同意書及び委任状（施行規則上各書式あり）及び患者の身分証明書のコピーを医療機関に提出しなければならないため（医療法施行規則第13条の3第2項）、患者の同意手続きが個人情報保護法に比べて非常に難しい。 また保健福祉部は、指定代理人は原則として医療機関に直接訪問し、身分証明書の写しの提出及び委任関係を証明しなければならないとみている（保健福祉部、2022年医療機関開設及び医療法人設立運営便覧、227面及び234面）。したがって、通常、研究や医薬品開発等を目的とする第三者が上記の規定により患者に関する記録を提供されることは事実上困難であると考えられる。

ii. 参考: 個人情報保護法の適用による「患者に関する記録」の利用

上記II.A.項で述べたように、患者ではない第三者が医療法上「患者に関する記録」を提供されることは容易ではない。 ただし、医療法ではなく個人情報保護法が適用される領域で患者に関する記録を第三者に提供することも可能であり、以下で項目を分けて調べる。

1. 医療機関 → 患者 → 第三者

医療機関が患者でない第三者に患者に関する記録を提供する上では厳格な要件が適用されるが、上記I.項で見た医療法第21条第1項のように、患者本人は医療機関にいつでも自分の記録閲覧またはコピー発給などその内容の確認を要請することができ、医療機関は正当な理由がない限りこれを拒否できない。 このように患者が提供された本人の記録は、もはや医療法が適用される「医療機関が保有する患者に関する記録」ではないので、患者が当該記録を第三者に提供する場合、これに対しては医療法ではなく個人情報保護法が適用される。

患者が保有する患者に関する記録は、個人情報保護法上の敏感情報(個人情報保護法第23条第1項)に該当し、研究などの目的で患者情報を利用しようとする第3者(個人情報処理者)が患者から敏感情

報を収集して利用するためには、患者から他の個人情報の処理に対する同意と**別途の同意**[43]を得なければならない(個人情報保護法第23条第1項第1号)。 この場合、個人情報処理者に対しては個人情報を処理するにあたって適用される諸般の義務(個人情報の目的外利用制限、個人情報処理方針掲示、安全措置義務[44]など)が課される。

2. 仮名処理された患者に関する記録提供（医療機関 → 第三者）

一方、保健福祉部は個人情報保護法第2条第1号の2により仮名処理した患者に関する記録に対しては医療法第21条が適用されず、個人情報保護法上仮名情報の処理に関する特例関連規定により該当情報を利用及び提供が可能であると解釈している(保健福祉部、2022年医療機関開設及び医療法人設立運営便覧、238面)。 したがって、仮名処理された患者に関する記録については医療法ではなく個人情報保護法が適用され、研究などの目的で患者情報を利用しようとする第三者は個人情報保護法の定めるところにより医療機関から仮名処理された患者に関する記録の提供を受けることができる。

個人情報保護法上仮名処理とは、個人情報の一部を削除したり、一部または全部を代替するなどの方法で、追加情報がなければ特定個人を識別できないように処理することをいう(個人情報保護法第2条第1号の2)。 個人情報処理者は統計作成、科学的研究、公益的記録保存などのためには**情報主体の同意なしに**仮名情報を処理することができ(個人情報保護法第28条の2第1項)、これにより個人情報処理者(医療機関)は科学的研究などの目的で患者に関する記録を仮名処理した後、該当仮名情報を第3者(研究等目的で情報を利用する者)に提供することができる。 このように第三者に仮名情報を提供する場合、当該情報には特定の個人(患者)を調べるために使用できる情報(識別子)が含まれてはならない(個人情報保護法第28条の2第2項)。

さらに、仮名情報を処理する個人情報処理者(医療機関)は、元の状態に復元するための追加情報を別途分離して保管·管理するなど、該当情報が紛失·盗難·流出·偽造·変造または毀損されないよう安全性確保に必要な技術的·管理的および物理的措置をしなければならず(個人情報保護法第28条の4第1項)、仮名情報の処理目的、第3者提供時に提供される者など仮名情報の処理内容を管理するために必要な事項に関する関連記録を作成して保管しなければならない(個人情報保護法第2項)。[45]

また、仮名情報を処理する者は特定個人を調べるための目的で仮名情報を処理してはならず、もし

---

[43] 個人情報処理者は患者に敏感情報の収集·利用目的、収集しようとする敏感情報項目、敏感情報の保有及び利用期間、同意を拒否する権利があるという事実及び同意拒否による不利益がある場合、その不利益の内容を事前に知らせ同意を得なければならない(個人情報保護法第15条第2項)

[44] 敏感情報を処理する個人情報処理システムの場合、個人情報取扱者が個人情報処理システムに接続した記録を2年以上(一般的な場合は1年以上)保管·管理しなければならない(個人情報の安全性確保措置基準第8条第1項)

[45] 2023年9月15日から施行される改正個人情報保護法では、仮名情報を破棄した場合、破棄した日から3年以上保管しなければならない義務も新設される(改正個人情報保護法第28条の4第3項)

仮名情報を処理する過程で特定個人を調べることができる情報が生成された場合、直ちに該当情報の処理を中止し、遅滞なくこれを回収および破棄しなければならない(個人情報保護法第28条の5)。

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

Ⅷ. China

中国の個人情報保護法制に関する調査

Yuna Matsuda

目次

1　エグゼクティブサマリー

第 4 次産業革命時代を迎え、ハイテク技術により人々の生産・生活方法には大きな変化が生じている。個人情報は、新しい時代の原動力であり、デジタル経済のインフラとして幅広く活用されている。商業活動にも利用され、莫大な経済利益や生活の利便性の向上にもつながっている。一方、情報技術を活用した個人情報の大規模の収集と利用は、個人のプライバシー侵害問題も同伴しており、個人情報保護における法制が重要視されている。個人情報の「保護」と「利用」の均衡は、中国を含む各国の課題でもある。

中国は、2003 年から個人情報保護のための立法を推進してきたが、中々制定までたどり着かずにいたところ、個人情報の漏洩やセキュリティの問題が急増し、大規模なデータ漏洩事件や個人情報の不正利用による社会的な問題が浮き彫りになり、2021 年にようやく「個人情報保護法」が公開された。

中国憲法は、情報自己決定権を明文化していない。また、憲法裁判所制度が存在しないため、憲法解釈を通じた保障もできない状況である。従って、個人情報保護法は、初めて個人情報保護について体系的な規定を設けた法律であるだけでなく、国家機関の個人情報処理を法的に制限した初の法律でもある。

個人情報保護法では、データ主体の権利について定めているが、知る権利と情報自己決定権、個人情報について閲覧・複製・移動を求める権利、不正確・不完全な個人情報に対し訂正や補完を求める権利、個人情報の削除を求める権利、個人情報処理ルールについて説明や解釈を求める権利、個人が死亡した場合近親者が相続できる権利、権利行使の請求が拒否された場合の提訴できる権利が含まれる。

告知・同意のプロセスにおいては、オプトイン方式を採用しており、法律や行政法規で定める特定の場合を除き、個人情報の処理には事前に本人の同意を取得することが必要である。

その他、自動化された意思決定やデータ・ポータビリティ権に関わる規定を設け、監督機関としては、国家インターネット情報弁公室を中心に、分散型モデルを採用している。

救済制度としては、個人や組織は、個人情報関連業務担当省庁に個人情報処理の違法行為をまずは通報でき、担当省庁が多くの人々の個人情報権益の侵害につながると判断した場合は、司法救済として、検察庁や国家インターネット情報弁公室等が指定した組織が公益訴訟を提起することができる。

個人情報保護の法制において、中国は法律の制定を通じ大きく一歩前に進んだが、データ主体の権利や事業者の義務についての規定は抽象的な部分が多く、独立した監督機関の不在や不十分な救済制度等、まだ改善を要する部分が多く残る。

2　個人情報に関わる憲法と法律上の規定

2.1　憲法における個人情報関連規定

憲法の個人情報に対する保護は、EU 基本権憲章のように、憲法の条文で明文化する場合があれば、ドイツやアメリカのように憲法解釈を通じ、個人情報保護を基本権として認める場合もある。

中国の憲法は、日本・ドイツ・アメリカと同様、個人情報の保護に対する明文化した規定を設けていない。また、中国には憲法裁判制度が存在しないため、裁判所が具体的な事件を審理する際に、憲法の条文を根拠として引用することはできない。従って、憲法条文の解釈を通じ、情報自己決定権を導出することも、アメリカのように、個人情報を基本権であるプライバシー権の範疇に入れて保護することもできない。中国で憲法に位置付けは、裁判の根拠ではなく、法律を制定する根拠であるため、憲法違反を根拠に提訴することはできない[1]。

ただ、憲法 33 条と 38 条を個人情報の保護の根拠だと主張している憲法学者は存在する。

中国憲法の基本権条文は、第 2 章の「国民の基本権と義務」に集中されているが、33 条は「国家は人権を尊重・保障する」と、38 条は「国民の人格尊厳は不可侵である」と定めている。33 条を個人情報保護の根拠だと主張する学者は、人権は抽象的な概念であるが、人間として享受すべき全ての権利を網羅しており、個人情報権もその一つだとしている。個人情報は情報漏洩のリスクが高く、個人が企業や国家からの不当な干渉を排除するのも現実的に難しいため、個人情報権への保護を人権保護に含ませるべきとの見解である[2]。また、38 条を根拠とすべきと主張する学者の見解は下記の通りである。人格尊厳は、尊厳と人格に分かれるが、尊厳は人間の尊厳、人格は人格権を意味する。38 条は個人情報保護に関する内容を明示していないが、個人情報権がもつ人格権的特性に鑑みれば、国民の人格尊厳性への保護を通じ、個人情報権も間接的に保護されているといえる[3]。憲法における個人情報保護関連条文は、その他、37 条の身体自由の不可侵、39 条の住居不可侵、40 条の通信の自由と秘密保護権等がある。

2.2　法律における個人情報保関連規定

憲法の条文及び憲法の有効解釈が、情報主体に権利を付与できておらず、国民は自身の権利で政府に対抗することができない。行政分野では、公共機関と個人の権利に不均衡が生じている。

---

[1] 2016 年 6 月 28 日に制定された最高裁判所（最高人民法院）「裁判所の民事裁判文書作成規範（人民法院民事裁判文书制作规范）」第 4 条は、「憲法を裁判の根拠として引用することはできない。」と定めている。

[2] 姚岳绒「情報決定権を基本権利とすることの関する論証（论信息自决权作为一项基本权利在我国的证成）」（政治学法律第 4 期、2012）77～78 頁。

[3] 孫平「政府巨大型データベース時代におけるプライバシー保護（政府巨型数据库时代的公民隐私权保护」（法学第 7 期、2007）24 頁。

中国における個人情報と関わる法律としては、本稿で紹介する民法典と個人情報保護法以外に、2012 年の「インターネット情報保護を強化することに関する決定」、2016 年の「ネットワーク安全法」、2021 年の「データ安全法」がある。ネットワーク安全法はサイバーセキュリティ全般、データ安全法はデータ処理活動のセキュリティ全般について定めている。これらの法律はデータ主体の権利よりは事業者の義務やデータ処理活動ルールに焦点を当てている。

① 民法典

中国の民法典は、2021 年 1 月 1 日より実施されたが、人格権制度を基盤に、情報自己決定権を保護しており、初めて法律の形で個人情報に関する権利を定めた。民法典は、総則編と人格権編で個人情報保護に関する規定を設けている。

総則編 111 条では、なぜ法律で個人情報を保護する必要があるかを論じ、人格権編では、1032～1039 条にかけ、個人情報に対し定めている。

中国民法典ではプライバシーと個人情報を下記の表の通り区分して保護している。

中国は、他国に比べ、個人情報という概念の普及が遅れているため、既存の法律では個人情報よりはプライバシーという表現を使用しており、両者の区別について特段の言及がなかったところ、民法典が初めて両者に区別について明文化した。民法典のプライバシー権は狭義的なプライバシー権であり、個人情報は識別可能性を基準に定義している。事業者の処理活動における指針を提供し、データ主体の閲覧権、複製権、削除権、異議や訂正の申し出ができる権利を含む各種権利についても定めている。

表　民法典における個人情報とプライバシーの区別

	内容	適用する条文
プライバシー（隠私）	私的秘密空間（プライベート空間）	プライバシーに関する規定
	私的秘密活動（プライベート活動）	
	私的秘密情報（プライベート情報）	
個人情報	一般個人情報	個人情報に関する規定
	私的秘密情報	プライバシーに関する規定

② 個人情報保護法

そして、2021 年 11 月 1 日より、個人情報について体系的に定める個人情報保護法が実施されるようになった。当該法律は、「EU 一般データ保護規則」（以下 GDPR：General Data Protection Regulation）をモデルに制定している[4]ため、類似している規定が非常に多い。また、GDPR で

[4] 対外経済政策研究院「中国の個人情報保護法の主要内容と展望」（世界経済フォーカス第 5 期、2022）2 頁。

は認められていない「死者の権利」についても保護規定を設けている。

個人情報保護法 1 条は、「個人情報の権益を保護し、個人情報処理活用を規範化し、個人情報の合理的利用を促すため、憲法に基づき当該法律を定める」としている。立法目的は、ビックデータ時代において、個人情報を保護しつつ十分に活用することである。個人情報保護法は、保護と利用という 2 つの価値を明確にし、両者が均衡を目指している。また、権益という表現を使用しており、データ主体の法的権利と利益の保護を強調している。

3 条は、適用範囲について定めているが、「中国境内の組織または個人が自然人の個人情報を処理する活動を行う際は当該法律を適用する。また、境外の組織または個人であるとしても、①中国境内の自然人に商品やサービスを提供する場合、②中国境内の自然人を分析、評価等をする際は、当該法律を適用する」とした。海外の組織や個人が中国国民の個人情報権益、公共利益や安全を侵害する場合は、国家情報関連省庁により、個人情報提供ブラックリストに登録され、氏名公開とともに、個人情報の提供が禁止または制限される（42 条)。

個人情報保護法は、民法典の個人情報の定義をより広げている。

4 条は、「個人情報とは、電子又はその他の方式によって記録された既に識別されたか或いは識別可能な、自然人と関連する各種情報を指す。匿名処理をした情報は個人情報に含まれない」と定めた。民法典は、識別可能性だけにフォーカスしている反面、個人情報保護法は、識別可能性と関連性両方を意識している。従って、個人情報に該当するか否かを判断する際には、まず、直接または間接的に特定個人を識別する可能性があるかどうか判断し、識別可能性があると判断した場合、当該情報が個人または識別された個人と関連性があるかどうかを再度判断する必要がある。個人情報に特定個人の識別性が求められるため、クッキー情報単体は、原則個人情報にあたらない。中国の個人情報の定義は、GDPR 4 条 1 号「個人データとは、識別された又は識別され得るデータ主体に関するあらゆる情報を意味する」との定義とほぼ同様である。

民法典では、個人に関わる情報を、プライバシーか個人情報に区分して定めたところ、個人情報保護法では、一般個人情報と敏感な個人情報に区分している。ここで言う敏感な個人情報（28 条）とは、「ひとたび漏洩し又は不法に使用されれば、自然人の人格の尊厳の侵害を引き起こしやすい、 又は人身、財産の安全が損なわれやすい個人情報をいい、生物識別、 宗教信仰、特定の身分、医療健康、金融口座、行動履歴等の情報及び 14 歳未満の未成年者の個人情報が含まれる。」 特定の目的と十分な必要性がある場合で、かつ厳格な保護措置を講じている場合に限り、事業者は、敏感な個人情報を処理することができる。

なお、個人情報の処理原則は、GDPR の原則と一致しているため、重複しない。

表　民法典と個人情報保護法における個人情報とプライバシーに関する規定

法律名	使われている用語	内容	適用する条文
个人信息权 民法典	プライバシー（隠私）	私的秘密空間（プライベート空間）	プライバシーに関する規定
		私的秘密活動（プライベート活動）	
		私的秘密情報（プライベート情報）	
	個人情報	一般個人情報	個人情報に関する規定
		私的秘密情報	プライバシーに関する規定
個人情報保護法	一般個人情報	匿名処理をした情報を除く	個人情報に関する規定
	敏感な個人情報	特別情報及び 14 歳未満の未成年者の個人情報	敏感な個人情報に関する規定

3　個人情報保護法制の現状と課題

3.1　データ主体の権利

個人情報保護法では、独立した第 4 章で、データ主体の権利について定めている。ここで、言及されている権利には、知る権利と情報自己決定権、個人情報について閲覧・複製・移動を求める権利、不正確・不完全な個人情報に対し訂正や補完を求める権利、個人情報の削除を求める権利、個人情報処理ルールについて説明や解釈を求める権利、個人が死亡した場合近親者が相続できる権利、権利行使の請求が拒否された場合の提訴できる権利が含まれる。

利用停止請求権として、まずデータ主体は、個人情報処理を拒否する権利を有する。また、データ主体本人が同意を撤回した場合や、目的のために取り扱う必要がなくなった場合等、違反がなくてもデータ主体は個人データの削除を請求できる。同意の撤回については、特段の規定をないため、いつでも撤回ができるようになっている。

言及すべき部分は、33 条は、国家機関が個人情報を処理する際も個人情報保護法を適用すべきと定めている。これは、中国の個人情報保護法制において、初めて国家機関の個人情報処理を法的に制限したこととなる。すなわち、データ主体は国家に相手に、個人の権利を主張できるようになったのである。

一方、中国にも情報銀行（信息银行）の仕組みが存在する。情報銀行とは、情報技術を利用し、パーソナルデータについて保存・管理・処理・分析・読取ができるサービスであり、銀行で現金を預けるように個人の情報を管理できるほか、ユーザーは情報価値がもたらす付加価値サービスも享受できる。中国でこのサービスを最も早く展開したのは、上海電信社であり、2009 年に E 雲というサービスを始めた。E 雲は、ユーザーの設定に従って、パソコンのエンプティタイムを利用し、パーソナルデータを上海電信の E 雲データセンターにバックアップするため、データを紛失した場合でも、本人がインターネットを通じて電信サーバーに接続すれば、いつでもデータの回復ができるようになっている。E 雲は情報銀行として、パーソナルデータに対する本人のコントローラビリティを保障し、本人以外はパーソナルデーにアクセスできないように保護している。

3.2　告知・同意に関する規定

①告知・同意のプロセス

日本において個人情報取扱事業者にあたる企業が個人情報を取得する場合、要配慮個人情報という一定の個人情報については予め本人の同意が必要ですが、通常の個人情報については、予めその利用目的を公表するか、又は個人情報の取得後速やかにその利用目的を本人に通知若しくは公表する必要があるものの、その個人情報の取得自体には本人の同意は必要としないが、中国の個人情報保護法では、法律や行政法規で定める特定の場合を除き、個人情報の処理には事前に本人の同意を取得することが必要とされている。すなわち、オプトイン方式を採用しているが、個人情報保護制度においての「告知・同意」のプロセスは、個人情報処理につい

て、データ主体に十分に告知をしてから同意を得ることが大前提であり、これは、個人情報におけるデータ主体の自己決定権を保障するためである。

データ主体の同意が不要な場合は、以下の 6 つの状況に限る（13 条）。

(一)データ主体を当事者の一方とする契約の締結、履行に必要である場合、或いは法により制定した労働規則制度や法により締結した集団契約に基づいて人的資源の管理を実施するために必要である場合。

(二)法定の職責又は法定の義務の履行に必要である場合

(三)突発的な公衆衛生上の事件に対応するため、又は緊急状況下において自然人の生命、健康及び財産の安全を保護するために必要な場合。

(四)公共の利益のためにメディア報道、世論監督等の行為を実施して、合理的な範囲内で個人情報を処理する場合。

（五）本法の規定に従って、合理的な範囲内で、データ主体が自ら公開した又はその他既に合法的に公開されている個人情報を処理する場合。

(六)法律、行政法規が規定するその他の事由。

また 14 条は、同意の有効条件について定めているが、「個人の同意に基づいて個人情報を処理するとき、当該同意は、データ主体が充分に事情を理解していることを前提に、自発的かつ明確に行わなければならない。法律、行政法規が、個人情報の処理にはデータ主体の個別の同意又は書面による同意を得なければならないと規定している場合は、当該規定に従わなければならない。個人情報の処理目的、処理方法及び処理する個人情報の種類に変更が生じた場合は、改めてデータ主体の同意を得なければならない」と定めている。

データ主体は、個人情報処理活動における同意を撤回でき（第 15 条）、個人情報の処理が商品又はサービスの提供のために必要である場合を除き、事業者は同意の撤回を理由に商品やサービスの提供を拒否してはならない（第 16 条）。

17 条では、事業者が告知すべき事項を定めているが、事業者は目立つ方法により、明瞭かつ理解しやすい表現を用いて、個人に対し、真実のとおり正確かつ完全に以下の事項を告知する必要がある。

（一）事業者の名称又は氏名及び連絡先。

（二）個人情報の処理目的、処理方法、処理する個人情報の種類、保存期限。

（三）データ主体が本法の規定する権利を行使する方法及び手続。

（四）法律、行政法規が告知すべきであると規定するその他の事項。

なお、14 歳未満の未成年者の個人情報を処理する際には、当該未成年者の両親又はその他監護者の同意を取得しなければならない（31 条）。

②プロファイリングの場面に特化したデータ保護の仕組み

告知・同意に関する具体的した規定を設けたには、中国での「ビックデータ殺熟」問題が深刻だったからでもある。「ビックデータ殺熟」とは[5]、ビッグデータをもとに購入履歴や消費傾向を分析し、ユーザーが知り得ないアルゴリズムによって商品やサービスの値段を変えてしまう行為を指すが、これは、サイトの会員やヘビーユーザーであるほど損をする場合が多いとされる。個人情報保護法では、この問題への対策として「自動化された意思決定」に関する規定を設けている。

73 条は、「自動化された意思決定とは、コンピュータプログラムを通じて個人の行動習慣、興味、嗜好又は経済、健康、信用状態等を自動的に分析、評価したうえで意思決定する活動をいう」と定めているが、「事業者が個人情報を利用して自動化された意思決定を行う場合には、意思決定の透明度及び結果の公平性・公正性を保証するものとし、取引価格等の取引条件において、データ主体に対して不合理な差別的待遇を行ってはならない」としている（24 条 1 項）。

また、「自動化された意思決定の方法によりデータ主体に対して情報のプッシュ通知、商業的なマーケティングを行う場合は、その個人的特徴に向けられたものではないオプション項目も同時に提供するか、データ主体に対して簡便な拒否方法を提供しなければならない。自動化された意思決定の方式により、データ主体の権益に対し重大な影響をもたらす決定を行う場合、データ主体は、事業者に対して説明を求める権利を有し、かつ事業者が自動化された意思決定の方式のみによって決定を行うことを拒否する権利を有する」（24 条 2 項）と定めている。当該規定は、データ主体に対し個人情報を処理するアルゴリズムを拒否できる権利やアルゴリズムに対し説明を求める権利を付与している。これは、GDPR22 条のプロファイリングを含む個人に対する自動化された意思決定規定と、13 条の自動化された意思決定の際のデータ主体の説明要求権と内容が一致している。

③データ・ポータビリティ権への保障

データ・ポータビリティ権については、45 条にて、「データ主体は、事業者からその個人情報を閲覧し、複製する権利を有する…データ主体がその個人情報の閲覧、複製を請求した場合、事業者は速やかに提供しなければならない。データ主体が個人情報をその指定する事業者に移転することを要求した場合で、国家インターネット情報弁公室が規定する条件に合致している場合、事業者は移転の手段を提供しなければならない。」と定めている。この規定により、データ主体は事業者に個人情報の副本や他者への転送を求められるようになった。個人情報保護法は、データ・ポータビリティ権について定めた初の法律である。ただし、データ・ポータビリティ権の範囲や転送方法等については定めておらず、まだ要補完の部分が多く残る。

この条文は、中国でこれからデータ・ポータビリティ権を保障するという宣言に該当し、具体的に保護措置は、実施細則や別途の法律で詳しく定める必要がある。

---

[5] CRI 日本語「ビックデータ殺熟」（2021 年 11 月、https://japanese.cri.cn/20211101/ea5ce9fb-92e1-cee5-6b6a-7c1491d4277e.html）を参照。

プラットフォーム経済の急速発展により、大手プラットフォーム事業者の独占問題や不正競争が蔓延している。典型的な例として、上述したプラットフォーム事業者による「ビックデータ殺熟」問題や「二者択一」独占行為（取引先に対して、競合他社とは取引しないよう迫る行為）が挙げられる。「二者択一」行為は、排他的な提携協議の締結、パケット制限等の方式で排他的提携協議が保障され実施されることが一般的である。データ・ポータビリティ権によって、ユーザーのデータにおける自主権が強化され、事業者の間でのデータ流動の自由が保障されるようになったので、公平競争の促進につながると思われる。公平競争の促進のため、個人情報保護法が制定された直後である 2021 年 2 月、国務院独占禁止委員会は「プラットフォーム経済における独占禁止に関する指針」も合わせて公開した。

④第 3 者への個人情報提供

21 条の規定によると、事業者が個人情報の処理を第 3 者に委託する場合、個人情報の処理方法、目的、期間、個人情報の種類、個人情報への保護措置を約定するとともに、受託者による個人情報処理活動に対して監督を行わなければならない。

また、第 3 者へ情報を提供する場合は、データ主体に、受領者の名称又は氏名、連絡先、処理目的、処理方法及び個人情報の種類を告知し、データ主体から個別同意をえる必要があり、受領者は、上記の処理目的、処理方法及び個人情報の種類等の範囲内において個人情報を処理すべく、もしも従来の処理目的、処理方法を変更する場合には、改めてデータ主体の同意を取得する必要がある（23 条）。

⑤敏感な個人情報の処理

2.2 で敏感な個人情報の定義について述べたが、事業者が、敏感な個人情報を処理する場合、データ主体の個別同意が必要であり、法律や法規で書面同意が必要であると定めている場合は、書面同意を得る必要がある（28 条）。

3.3　告知・同意プロセスの限界と対策

なお「告知―同意」にプロセスの限界は、中国でも指摘されている。

事業者は、契約締結において、個人情報の保護より法的責任を避けることにフォーカスを当てているため、免責条文を多く入れる可能性が高く、契約内容が冗長になる恐れがある。また、個々の年齢、専門知識、教育水準によって理解能力の差は大きいため、データ主体が告知・同意の内容を十分に理解したとは断言できない。告知・同意規則は、契約を締結する双方が合理的な能力を有することを前提にするが、全てのデータ主体が情報処理の危険性、例えば、告知の具体的な内容や同意した場合もたらす結果等について十分に認識しているとは言えない。同意に多くのコスト・時間がかかるため、データ主体は同意疲れを感じる場合も多く、プライバシーポリシーも流し読みが多いと思われる。従って、告知・同意の具体的な内容を把

握しているデータ主体は非常に少ない恐れがある。統計によると[6]、データ主体が告知・同意説明書を十分に読む場合年間平均 244 時間が所要され、丁寧に読まない場合も年間 154 時間が必要となる。データ主体は、告知・同意の内容を十分に把握できていないまま、時間の余裕がない等で同意するケースが多い。

その改善策として、既に一部の企業で導入しているが、告知・同意プロセスにプライバシー設計を追加する方法が挙げられている。この方法はより実効的な告知になるとの主張が存在する[7]。製品設計は個人情報保護の要求を満たす必要があるため、告知・同意のプロセスにプライバシー設計の要求を追加すると、告知内容の費用や難易度を下げることができ、データ主体の認識も高められるため、事業者とデータ主体の認識のすれ違いが最小化しつつ、データ主体の個人情報への自己決定権を高められとされる。例としは、中国の BiliBili アプリケーションは、ユーザーがテストに合格した場合のみ、アプリケーションの利用が可能になるよう設計されている。テストの内容には、個人情報の保護や製品の使用ルール等が含まれるため、効果的な告知となっている。類似している例で、電子製品を使用する場合、データ主体に動画で個人情報の収集・利用・結果を伝え、最後テストを行う方法がある。

もう一つの方法としては提言されているのは、GDPR が 2021 年標準契約の約款テンプレート[8]制定したように、中国政府が各種業界における標準計画書を予め設計し、事業者が統一した契約書を作る方法である。政府が契約書に対し解釈を行いつつ、宣伝活動に取り組める紛争が起きたとしても有効に解決できるという主張である[9]。中国政府の強みの一つは政策の柔軟性と普及の速さであり、中央の政策は短時間で地方まで伝わるため、実効性の高い方法になると思われる。

3.4　個人情報保護法を執行する監督機関の組織と権限

60 条 1 項の規定により、個人情報の保護法を執行する中央の監督機関は、国家インターネット情報弁公室(国家互**联**网信息**办**公室)となる。国家インターネット情報弁公室は、個人情報の保護に関わる管理監督業務全般を総括・調整する。

国家インターネット情報弁公室が行うべき業務には以下の事項が含まれる（62 条）

（一）個人情報保護の具体的なルール、基準を制定する。

---

[6] Omriben-Shahar & Carle.Schneider, *The failure of Mandated Disclosure*, 159 University of Pennsylvania Law Review, Vol. 52, 2011, pp.658-659.

7 張翱鵬「中国の個人情報保護制度に関する研究」（忠北大学博士論文、2022 年 2 月）218～219 頁。

[8] European Commission, Standard Contractual Clauses (SCC), https://ec.europa.eu/info/index_en

[9] 張翱鵬「中国の個人情報保護制度に関する研究」（忠北大学博士論文、2022 年 2 月）219～220 頁。

（二）小規模な事業者、敏感な個人情報の処理及び顔認識、人工知能等の新テクノロジー、新アプリケーションを対象に、専門の個人情報保護ルール・基準を制定する。
（三）安全で便利な電子身分認証技術の研究開発と応用の普及を支援し、オンライン身分認証のための公共サービスの構築を促進する。
（四）個人情報保護の社会的サービス体系の構築を推進し、関係機構による個人情報保護の評価、認証サービスの展開を支援する。
（五）個人情報保護に関する苦情申立て、通報業務のメカニズムを完備する。

また、国務院の関連部門は、各自の職責の範囲内において、個人情報保護及び監督管理業務の責任を負うように定められている（60 条 2 項）。従って、個人情報保護への監督業務は、非常に多くの省庁に分散されている。例えば、消費問題になると工商行政省庁が担当し（消費者権益保護法第 32 条）、信用情報や郵便関連問題は、中国銀行と国家郵便局が担当する（通信とネットユーザー個人情報保護規定 17 条、ネットワーク安全法 8 条）。なお、中国は、国家（中央）、省、市、県の 4 級行政体系を取っているため、各階級においても、これから監督機関が存在する（例：○○省インターネット情報弁公室、○○市工商行政局等）。そして、これらの個人情報保護監督業務に携わる省庁を全て「個人情報関連業務担当省庁」と称する。

個人情報関連業務担当省庁の職責は下記の通りである（61 条）。
(一)個人情報保護の宣伝教育を展開し、事業者による個人情報保護業務を指導、監督する。
(二)個人情報保護に関する苦情の申し立て、通報を受理し、処理する。
(三)アプリケーションプログラム等の個人情報保護情況について測定・評価を実施し、測定・評価の結果を公表する。
(四)違法な個人情報処理活動を調査し、処理する。
(五)法律、行政法規が規定するその他の職責。

また、個人情報関連業務担当省庁は、職責を履行するにあたり、以下の措置を取ることができる（63条）。
(一)関係当事者に対し質問し、個人情報処理活動に関する状況を調査する。
(二)個人情報処理活動と関係する当事者の契約、記録、帳簿及びその他の関係資料を閲覧、複製する。
(三)現場検査を実施し、違法が疑われる個人情報処理活動について調査を行う。
(四)個人情報処理活動と関係する設備、物品を調査する。違法な個人情報処理活動に用いられている設備、物品であることを証明する証拠があるものについては、当該部門の主要責任者に対して書面で報告したうえで許可を得て差押え又は押収することができる。

64条の規定により、個人情報関連業務担当省庁が職責を履行する中で、個人情報処理活動に比較的大きなリスクが存在すること、又は個人情報安全事件が発生したことを発見した場合は、当該事業者の法定代表者又は主要責任者に対して事情の聞き取りを行うか、或いは事業者に対して、専門機構に委託してその個人情報処理活動についてのコンプライアンス監査を依頼するよう要求することができる。事業者は、要求に基づき措置を講じ、改善を実施し、隠れた

危険を取り除かなければならない。個人情報関連業務担当省庁が職責を履行する中で、個人情報の違法な処理が犯罪を構成する疑いのあることを発見した場合は、速やかに公安機関に移送して、公安機関の法による処理に委ねる必要がある。

中国の場合、独立した個人情報保護機関を設置する代わりに、既存の国家インターネット情報弁公室を監督業務総括省庁と指定し、多くの省庁に業務を分担させる仕組みを選択した。このような分散モデルは、実際の運用において難点が多く、各監督機関の業務の重複、責任の回避、行政資源の浪費等がおきうる。場合によっては、監督機関をどこにすべきか指定することも難しいかもしれない。また、4つの階級に監督機関が分かれているが、県級は規模が小さく業務遂行能力に有していない場合もある。個人情報保護法は、地方の個人情報関連業務担当省庁が違法事件等を解決できない場合の補完方法について定めておらず、慣例により、上級省庁に報告すると思われるが、段階別報告の末に中央にたどり着いた場合は、既に事件解決のタイミングを逃してしまう恐れがある。また、地方政府は責任回避のため、情報を隠蔽するか虚偽報告を行う可能性もないとはいえない。独立した監督機関の設置は、今後と課題であると思われる。

3.5　司法的救済の仕組み

65条の規定に基づき、いかなる組織、個人も、違法な個人情報処理活動について、個人情報関連業務担当省庁に対して苦情を申し立て、通報する権利を有している。個人情報関連業務担当省庁は、法に基づいて速やかに処理を行うとともに、処理の結果を苦情申立人や通報者に告知し、個人情報保護の職責を履行する部門は、苦情や通報を受け付ける連絡先を公表する義務がある。

また、70条は「事業者が本法の規定に違反して個人情報を処理し、多くの個人の権益を侵害した場合、人民検察院（検察庁）、法律が規定する消費者組織及び国家インターネット情報弁公室が指定した組織は、法に基づき人民法院（裁判所）に訴訟を提起することができる」としている。

70条の規定により、個人情報の侵害について、集団訴訟の可能性もあるようには見えるが、これ以上の詳細な規定は見当たらない。個人や組織は、個人情報関連業務担当省庁に個人情報処理の違法行為をまずは通報でき、担当省庁が多くの人々の個人情報権益の侵害につながると判断した場合は、検察庁や国家インターネット情報弁公室等が指定した組織が公益訴訟を通じ、司法救済を得ることが可能になっている。

3.6 研究・医薬品開発を目的とした診療データの二次利用

結論から述べると、研究目的で患者の診療データを利用したい場合は、①患者本人の明示的な同意を得るか、あるいは、②個人を特定できないかつ復元不可能になるように匿名処理を行う必要がある。従って、匿名処理を行っていれば、本人の同意がなくても利用できる。

中国には、日本の「次世代医療基盤法」のように、個人の医療データの利用・活用について定めている特別法は存在せず、一般法からその根拠を探る必要がある。

「情報安全技術―個人情報安全規範[10]（以下、「規範」とする、2020 年 10 月 1 日より施行）」によると、患者の医療データは、3.2 の敏感な個人情報に該当し、一旦改ざん、破壊、漏出または不正取得、不正利用されると、人身と財産安全、個人名誉、心身の健康に危害を及ぼすか差別待遇に繋がる可能性が高いデータの範疇に属している。従って、患者の診療データや記録への活用に対して、政府の立場は慎重である。国家衛生健康委員会医政司の副局長は、診療データの活用について「個人情報について匿名処理を行ったとしても患者の診療データは公共資源であり、医療機関、医療人員（関係者）は、関連部門の授権なしに取り扱う権限がない[11]」と強調し、医療データ扱いに対する中央政府の基本的な見方を示した。

「ネットワーク安全法[12]（2017 年 6 月 1 日より施行」42 条では、「ネットワークプロバイダは、自らが収集した個人情報を漏えい、改竄、毀損してはならない。提供者の同意を経ずに、他人に対し個人情報を提供してはならない。ただし、処理を経て特定の個人を識別するすべがなく、なお且つ復元不能である場合を除く。」と定めている。上記法律の施行ガイドラインとして「インターネットにおける個人情報安全保護指南[13]（以下「指南」とする、2019 年 4 月 10 日より施行）」が続いて公開されたが、「指南」6.3 二次利用 a）では、「個人情報の二次利用において、利用の範囲は、データ主体と締結した契約や協議内容に準ずる。契約や協議内容を超える範囲での個人情報の利用は認めない。ただし、匿名処理により、個人を特定できないかつ復元が不可能な個人情報については、契約や協議内容の範囲を超えての利用ができる。しかし、この場合でも適切な保護措置を講じる必要がある。」とした。

翌年に公開された、「規範」7.3 個人情報使用の目的制限では、「個人情報を利用する際には、個人情報を収集する時に提示した利用目的または関連範囲を超えてはならない。ここでいう関連範囲とは、個人情報を学術研究や自然、科学、社会、経済等の現象の全体状況の説明等に利用する場合を指す。ただし、対外に学術研究や説明結果を提供する場合は、結果の中に含まれている個人情報に対し、匿名処理を行うべきである。」と補足した。

従って、研究の目的で患者の個人情報を利用するルートは、患者の明示的な同意を得て利用するか、患者の診療データについて匿名処理を行い利用することになる。

では、患者の個人情報が漏洩された場合はどのなるのか。

まず、指南 6.6 の共有と移転では、「個人情報について共有、移転する際は、個人情報安全影響評価を行うべき。」としているが、指南はガイドラインに過ぎず、法的拘束力は有しない。

---

[10] 全文：情報安全技術―個人情報安全規範
http://www.100ec.cn/detail--6571570.html

[11] 2019 年 3 月、国家衛生健康情報化及び知恵病院設立における発表会でのコメントを参照。
https://www.sohu.com/a/315775037_658347

[12] 全文：ネットワーク安全法 https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf

[13] 全文：インターネットにおける個人情報安全保護指南
https://m.thepaper.cn/baijiahao_4000821

「ネットワーク安全法」42 条 2 項では、「個人情報の漏えい、毀損又は紛失が発生するか、発生する恐れのある状況においては、直ちに救済措置を講じ、規定に従い遅滞なく使用者に告知し、なお且つ関係所管機関に対し報告しなければならない。」としている。また、「オンライン診療管理弁法（暫定）[14]」20 条、「オンライン病院管理方法（暫定）[15]」23 条では「患者の個人情報、医療データの漏洩があった場合、医療機関は、主管衛生健康行政部門に報告し、有効な対応措置を取るべきである。」と定めている。医療機関の報告義務や適切な事後措置義務について抽象的に定めているものの、それ以上は記載がない。

診療データを二次利用する際に、どのような義務が課せられるか。

「規範」11.4 二次利用データ安全編では、医療データの二次利用における各プロセスで守るべき規定が定められている。

政府部門、研究者、企業等（以下申請者とする）は、非営利目的での医療データの二次利用ができる。データ量が大きく、全てのデータ主体に連絡できない、あるいは連絡コストが高すぎる場合は、下記プロセスで、データを有している機関（医療機関、地域の衛生情報プラットフォーム、医療連合体、医療学術団体等）を通じ、データを取得し、二次利用することができる。

①データ準備段階：データを有している機関は、二次利用に提供しようとするデータの目録やデータに対する説明を用意すべきである。

②二次利用申請者資格：申請時は、機関ベース（例：○○大学）で申請を行うのが望ましい。個人で申請を行う場合は、レベルの高い研究者に限る。（例：複数件のファンディングプロジェクトに採択されたことのあり、当該研究分野で高い専門知識を有する、かつ社会信用評価が A レベルであること）。データを有する機関は、申請者の申請歴史を漏れなく記録すべきである。

③データ審査段階：データを有している機関は、データ委員会を立ち上げるか独立した第三機関に審査を依頼し、申請者のデータ利用目的の正当性やデータの安全性等について審査を行う。審査員は、専門家データベースよりランダムに選ぶことが望ましい。データ委員会は章程、審査プロセス、審査記録等を制定すべきである。

④匿名処理：データを有する機関は、データを提供する前に、匿名処理を行うべきであり、最小計数原則（匿名処理を行った後、同条件を満たす人が最低でも 5 人になる必要がある）を遵守すべきである。例：今年 A 病院で子宮がんに診断された患者が 4 人であれば、病名を明かしてはならない。

⑤契約締結：データを有する機関と申請者は、データ送付前に、使用契約を締結し、データ保護措置、データが漏洩した場合の対策、データ使用期限等を明確に定める必要がある。

---

[14] オンライン診療管理弁法（暫定）全文：
https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91%E8%AF%8A%E7%96%97%E7%AE%A1%E7%90%86%E5%8A%9E%E6%B3%95%EF%BC%88%E8%AF%95%E8%A1%8C%EF%BC%89/22876322?fr=ge_ala

[15] オンライン病院管理方法（暫定）全文：
https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91%E5%8C%BB%E9%99%A2%E7%AE%A1%E7%90%86%E5%8A%9E%E6%B3%95%EF%BC%88%E8%AF%95%E8%A1%8C%EF%BC%89/22876336?fromModule=lemma_inlink

⑥データ送付時のデバイス：識別可能性が低いデータは、パスワードつきの e-mail や USB 等で送付できるが、患者の個人情報等が含まれており、識別可能性が比較的に高いデータは、遠隔操作等よるダウンロード等、安全性の高い方法を利用しなければならない。

⑦データの削除：申請者はデータ利用が終わり次第書面にて、データを有する機関に通知を行い、使用期限後の 30 日以内にデータを削除し、削除証明を、データを有する機関に送付する必要がある。データを有する機関は通知を受け取り次第検証作業に取り組むべきである。

中国国務院は、2018 年 4 月 28 日に「『オンライン＋医療健康』の発展を推進することに関する意見[16]」で、オンライン診療の普及とともに、オンオフライン医療サービスの一体化推進、2025 年までの「マイ健康 QR コード[17]」の導入を目指していると明かした。

医療オンライン化の推進に伴い、個人情報保護への懸念の声も高まっている。安全性の高い医療データベースやプラットフォームの構築だけでなく、患者の個人情報の保護における法律や政策の基盤も合わせて整えていく必要がある。

以上、中国の個人情報保護法制について述べてきたが、個人情報保護法は、未成年者の年齢を14歳以下指定し、死者の個人情報についても保護する等、GDPRと異なる部分があるとはいえ、類似して内容のほうが圧倒的に多い。中国で個人情報保護法はまだ新生法律であるため、実施細則等も公開されていなく、抽象的な内容や説明不足の箇所が多々あるが、引き続きこれからの動向をフォローしていきたい。

[16]全文： https://www.gov.cn/zhengce/content/2018-04/28/content_5286645.htm

[17] 日本でいえば、マイナンバーカードの医療バージョンのようなものであるが、一人一 QR コードで、スキャンすれば、その人とあらゆる健康情報、診療データが見られるものである。

参考資料

①程啸、“我国《民法典》中個人信息保護制度的創新與発展”、 财政法学、 第 4 期、2020

②程啸、“民法典编纂视野下的個人信息保護”、 中国法学、 第 4 期、2019。

③丁晓東、“個人信息私法保護的困境與出路”、 法学研究、 第 6 期、2018。

④丁晓東、“論数据携带权的属性、影响與中国应用”、 法商研究、 第 1 期、2020。

⑤韩旭至、“個人信息保护告知同意的困境与出路”、 经贸法律評論、 第 1 期、2021。

⑥張翱鹏、「中国の個人情報保護制度に関する研究」、忠北大学博士論文、2022。

⑦張恩典、“大数据时代的算法解释权: 背景、逻辑与构造”、 法学论坛、 第 4 期、2019。

⑧張新宝、“从隐私到個人信息: 利益再衡量的理論與制度安排”、 法学研究、 第 3 期、2015。

⑨張新宝、“個人信息收集: 告知同意原则适用的限制”、 比较法研究、 第 6 期、2019。

⑩張新宝、“互联网生态‘守門人’個人信息保护特別義務設置研究”、 比較法研究、 第 3 期、2021。

⑪趙宏、“信息自决权在我国的保护现状及其立法趋势前瞻"、 中国法律評論、 第 1 期、2017。

⑫張里安·韩旭至、“大数据时代下个人信息的私权属性”、 法学論壇、第 3 期、2016。

⑬趙万一、“从民法與憲法关系的视角谈我国民法典制定的基本理念和制度架构”、中国法学、第 1 期、2006。

⑭朱広新、“民事行为能力制度的完善——以中华人民共和国《民法总则(草案)》为分析对象”、当代法学、 第 6 期、2016。

⑮周汉華、“個人信息保護的法律定位”、 法商研究、 第 3 期、2020。

⑯田姬娟、「中国の個人情報保護法制の改善方案に対する研究」、成均館大学博士論文、2022。

⑰松尾 剛行「中国の個人情報保護法とデータ運用に関する法制度の論点」、総務省 学術雑誌『情報通信政策研究』 第 5 巻第 2 号、2021。

重要条文

民法典　第六章　プライバシー権及び個人情報
第 1032 条【プライバシー権】自然人はプライバシー権を有する。いかなる組織又は個人も密偵、侵入、漏えい、公開等の方式により他人のプライバシー権を侵害してはならない。 2　プライバシーとは、自然人の私生活の平穏及び他人に知られたくない私的秘密空間（プライベート空間）、私的秘密活動（プライベート活動）、私的秘密情報（プライベート情報）をいう。
第 1033 条【プライバシー権侵害の禁止】法律に別段の規定があり又は権利者の同意がある場合を除き、いかなる組織又は個人も次に掲げる行為を実施してはならない。（一）電話、ショートメール、インスタントメッセージ、電子メール、ビラ等の方式 により他人の私生活の平穏を侵すこと（二）他人の住宅、宿泊客室等の私的秘密空間に侵入し、撮影、盗視すること（三）他人の私的秘密活動を撮影、盗視、盗聴、公開すること（四）他人の身体の私的秘密部位を撮影、盗視すること（五）他人の私的秘密情報を処理すること（六）その他の方式により他人のプライバシー権を侵害すること。
第 1034 条【個人情報保護】自然人の個人情報は、法律の保護を受ける。 2　個人情報とは、電子又はその他の方式によって記録された、単独で又はその他の情報と結合して特定の自然人を識別することができる各種情報をいい、自然人の氏名、生年月日、身分証明書番号、生体識別情報、住所、電話番号、メールアドレス、健康情報、 移動履歴情報等を含む。 3　個人情報中の私的秘密情報については、プライバシー権の関係規定を適用する。規定がない場合、個人情報保護の関係規定を適用する。
第 1035 条【個人情報の処理に関する原則】個人情報を処理する場合、合法、正当、必要の原則に従わなければならず、かつ次に 178 掲げる条件に適合しなければならない。（一）当該自然人又はその後見人の同意を得ること。但し、法律、行政法規に別段の規定がある場合を除く。（二）情報の処理に関する規則を公開すること。（三）情報を処理する目的、方式及び範囲を明示すること。（四）法律、行政法規の規定及び双方の約定に違反しないこと 2 個人情報の処理には、個人情報の収集、保存、使用、加工、伝送、提供、公開等を含む。
第 1036 条【個人情報処理の免責事由】個人情報の処理が、次のいずれかに該当する場合、行為者は民事責任を負わない。（一）当該自然人又はその後見人が同意する範囲内で実施する行為（二）当該自然人が自ら公開し、又はその他の既に合法的に公開された情報を合理的に処理するとき、但し、当該自然人が明確に拒絶する場合、又は当該情報の処理により重大な利益侵害となる場合を除く。（三）公共利益又は当該自然人の合法的権益を維持保護するため、合理的に実施するその他の行為
第 1037 条【個人情報主体の権利】自然人は、法に基づき情報処理者からその個人情報を閲覧又は複製することができる。 情報に誤りがあることを発見した場合、異議を提出し、かつ速やかに訂正等の必要な措置を講じるよう請求する権利を有する。 2 自然人は、情報処理者が法律、行政法規の規定又は双方の約定に違反して当該個人情報を処理していることを発見した場合、情報処理者に対して速やかに削除するよう請求 する権利を有する。
第 1038 条【個人情報処理者の安全保護義務】情報処理者は、その収集、保存する個人情報を漏えい、改

ざん、毀損してはならない。自然人の同意を得ずに、個人情報を他人に対して違法に提供してはならない。但し、加工を経て特定個人を識別することができず、かつ復元できない場合を除く。 2 情報処理者は、技術的措置及びその他の必要な措置を講じて、その収集、保存する個人情報の安全を確保し、情報の漏えい、改ざん、紛失を防止しなければならない。個人情報が漏えい、改ざん、紛失する状況が発生し又は発生するおそれがあるときは、速やかに救済措置を講じ、規定に基づいて自然人に告知し、かつ関係主管部門に報告しなければならない。
第 1039 条【国家機関等の秘密保持義務】国家機関、行政職能を担当する法定機関及びその職員が、職責履行過程において知った自然人のプライバシー及び個人情報については、その秘密を保持しなければならず、 漏えい又は他人に対して違法に提供してはならない。

個人情報保護法　第四章 データ主体の（個人）権利
第 44 条【知る権利・決定権】 個人は、その個人情報の処理について知る権利、決定権を享受し、他人がその個人情報を処理することを制限又は拒否する権利を有する。法律、行政法規に別段の定めがある場合は、この限りではない。
第 45 条【閲覧・複製・情報移動権】 個人は、個人情報処理者からその個人情報を閲覧し、複製する権利を有する。本法第十八条第一項、第三十五条の規定する事由が存在する場合は、この限りではない。 個人がその個人情報の閲覧、複製を請求した場合、個人情報処理者は速やかに提供しなければならない。個人が個人情報をその指定する個人情報処理者に移転することを要求した場合で、国家インターネット情報部門が規定する条件に合致している場合、個人情報処理者は移転の手段を提供しなければならない。
第 46 条【訂正・補充を求める権利】 個人は、その個人情報が不正確又は不完全であることを発見した場合、個人情報処理者に対し、是正、補充を求める権利を有する。個人がその個人情報の是正、補充を請求した場合、個人情報処理者はその個人情報について確認したうえで、速やかに是正、補充しなければならない。
第 47 条【削除権】 以下に掲げる事由のいずれか一に該当する場合、個人情報処理者は自発的に個人情報を削除しなければならない。個人情報処理者が削除しない場合、個人は、削除を要求する権利を有する。(一)処理目的が既に実現した場合、実現不可能な場合、又は処理目的の実現のために必要ではなくなった場合。 (二)個人情報処理者が商品又はサービスの提供を停止した場合、 又は保存期限がすでに満了した場合。 (三)個人が同意を撤回した場合。 (四)個人情報処理者が法律、行政法規に違反し、又は約定に違反して個人情報を処理した場合。 (五)法律、行政法規が規定するその他の事由。 法律、行政法規が規定する保存期限が満了していない場合、又は個人情報の削除が技術的に困難である場合、個人情報処理者は、保存と必要な安全保護措置の実施を除き、それ以外の処理を停止しなければならない。
第 48 条【解釈・説明を求める権利】 個人は、個人情報処理者に対してその個人情報処理ルールについて解釈、説明を行うよう要求する権利を有する。
第 49 条【個人情報相続権】 自然人が死亡した場合、その近親者は、自身の合法、正当な利益のために、

死者の関連する個人情報について本章に規定する閲覧、複製、更生、削除等の権利を行使することができる。死者の生前に別段の取り決めがあった場合を除く。
第 50 条【訴訟提起権】 個人情報処理者は、個人からの権利行使の申請を受理、処理するための簡便なシステムを構築しなければならない。個人による権利行使の請求を拒否する場合は、その理由を説明しなければならない。個人情報処理者が、個人による権利行使の請求を拒否した場合、 個人は、人民法院（裁判所）に訴訟を提起することができる。

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

IX. Canada

Kento Yamamoto
(Associate Professor, Faculty of Law, The University of Kitakyushu)

はじめに

本報告書は、ムーンショット型研究開発事業の一つである「データの分散管理によるこころの自由と価値の共創」（プロジェクトマネージャー：橋田浩一）のディレクターのひとりである山本龍彦より依頼を受け、カナダの個人情報に関する法令調査を行ったものである。調査は依頼時の質問リスト（山本龍彦、飯田匡一、佐藤太樹作成）に基づき行った。本報告書では質問リストに回答する形式をとっている[1]。

本調査の対象であるカナダの個人情報保護法は連邦法と州法に分かれているが、本調査では、主に連邦法を対象とし、州法については補足的に触れるに留める。これは連邦法と州法で相違はあるものの連邦法が標準形であることによる。また、カナダでは個人情報保護の包括立法が公的部門を対象とするものと民間部門を対象とするものに分かれている。よって、本調査が主たる調査対象とするのは、連邦の公的部門を対象とするプライバシー法（*Privacy Act*, R.S.C. 1985）と、民間部門を対象とする個人情報保護及び電子文書法（*Personal Information Protection and Electronic Documents Act*, S.C. 2000 以下 PIPEDA）[2]である。なお、PIPEDA は州が PIPEDA と実質的に類似する法律を制定していない限り、当該州内においても適用される。現在、PIPEDA と実質的に類似する州法を有するのは、ケベック州、アルバータ州、BC 州の 3 州である。この他、個人健康情報（personal health information）についてのみ PIPEDA と実質的に類似する州法を有する州として、オンタリオ州、ニューブラウンズウィック州、ノバスコシア州、ニューファンドランド・ラブラドール州の 4 州がある。さらに、民間部門については、デジタル憲章実施法案（*Digital Charter Implementation Act*, 2022）が提案されており、消費者プライバシー保護法

[1] 同報告書の記述は、山本龍彦ほか編『個人データ保護のグローバル・マップ（仮）』（弘文堂、2024 年刊行予定）〔山本健人執筆部分〕と重なる箇所がある。また、以下の先行研究・先行調査に助けられたところも多い。石井夏生利「カナダのプライバシー・個人情報保護法」情報法制研究 1 号（2017 年）11 頁以下、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」（2011 年 3 月）〔河井理穂子執筆部分〕、消費者庁「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（2009 年 3 月）〔佐藤信行執筆部分〕。

[2] PIPEDA は、民間組織が商業活動の過程で取り扱う個人情報の収集、使用、開示に関するルールを確立することを目的としており（3 条）、民間部門のあらゆる個人情報の取扱いではなく、商業活動の過程での個人情報の取扱いを規律することを想定している。

（*Consumer Privacy Protection Act*）、個人情報及びデータ保護審判所法（*Personal Information and Data Tribunal Act*）、AI データ法（*Artificial Intelligence and Data Act*）の導入が審議されている。同法案が可決されれば（現在連邦下院の第 2 読会を通過している）、PIPEDA の個人情報保護部分が消費者プライバシー保護法に置き換えられる。これらは現行法ではないが、法改正が成立すればカナダの個人情報保護法体系を大きく変更するものであるため、本調査の対象に含めている。

質問リストへの回答

1. 憲法と個人情報保護制との関係性

Q1-①. プライバシー権ないし情報自己決定権が、憲法上（条文または判例上）保障されているかどうか。またその際、プライバシー権と情報自己決定権との異同が意識されているかどうか。

憲法上の権利を規定する 1982 年の「カナダの権利及び自由に関する憲章」は明文でプライバシーの権利を規定していない。現在、カナダにおける憲法上のプライバシーは、不合理な捜索及び押収からの保護を規定する憲章 8 条によって保護されると解されている。表現の自由（憲章 2 条(b)）、民主的権利（憲章 3 条）、生命、自由及び身体の安全の権利（憲所 7 条）も憲法上のプライバシー保護にかかわるが、現時点では憲法上のプライバシー保護の中心は憲章 8 条である。

カナダ最高裁判所は、Spencer 判決[3]で、憲章 8 条が保護するプライバシーの利益を次のように整理している。まず、大きく①身体的プライバシー（自分の体、体液、そこから得られた物質、場合によっては所持品にも及ぶ）、②領域的プライバシー（私的な活動を行う場所に関するもので、最も中心的なものは住居だが、自家用車、職場、ホテルの部屋のような一時的な私的空間にも及びうる）、③情報プライバシーが区別される。そして、情報プライバシーについては、コントロールとしてのプライバシーが注目されてきたが、それだけに留まらないとして、さらに㋐秘密としてのプライバシー（医師と患者の間など、信頼及び信用関係の中で情報が共有されている場合に関わる）、㋑コントロールとしてのプライバシー（自分に関する情報がいつ、どのように、どの程度他者に伝達されるかを自ら決定する個人、集団、又は機関の主張に関連する）、㋒匿名としてのプライバシー（個人が、公共の場やオンライン上で他者から観察される可能性のある情報を共有したり活動を行ったりする際に、その活動を行った主体が誰かを特定されることなく活動できることを保護する）に細分化されている。

Q1-①の「プライバシー権」と「情報自己決定権」に必ずしも対応していないかもしれないが、カナダ最高裁は憲章 8 条のプライバシーを複合的な利益と捉えている、と回答することができる。これはプライバシー権と情報自己決定権あるいは

[3] *R. v. Spencer*, [2014] 2 S.C.R. 212

自己情報コントロール権を別の権利として分けるのではなく、プライバシー権という単一の権利のなかで、様々なプライバシーの利益の共存あるいは相補的な関係を認める方向性を示唆しており、興味深い。

Q1-②. プライバシー権ないし情報自己決定権が憲法上の権利として保障されている場合、かかる権利が、個人情報保護法の目的規定のなかに読み込まれているかどうか。別言すると、個人情報保護法が、プライバシー権などの憲法的価値を実現する法令として位置付けられているかどうか。

カナダの個人情報保護法は「準憲法的法律」と位置づけられている。これはカナダ最高裁が創り出したカテゴリーであり、個人情報保護法のほかに人権法（*Canadian Human Rights Act,* R.S.C. 1985）や情報アクセス法（*Access to Information Act* , R.S.C. 1985）などが準憲法的法律に位置づけられている。カナダ最高裁は、Lavigne 判決でプライバシー法を[4]、UFCW Local 401 判決で PIPEDA と実質的に類似するアルバータ州の個人情報保護法（*Personal Information Protection Act*, S.A. 2003）を準憲法的法律とした[5]。UFCW Local 401 判決によって、実質的に類似する連邦の PIPEDA も間接的に準憲法的法律と位置づけられたことになる。さらに、BC 州のプライバシー法（*Privacy Ac*t, R.S.B.C. 1996）[6]を準憲法的法律とした Douez 判決の法廷意見では、「プライバシー立法」が準憲法的地位にあるとされており[7]、これは「全てのプライバシー保護立法」が準憲法的法律であると述べたものだとする理解も示されている[8]。

カナダ最高裁によれば、準憲法的法律は「我々の社会の特定の基本的な目標」を反映したものであり、「その根底にある広範な政策的考慮を促進するように」解釈されなければならない[9]。準憲法的法律と位置づけることの効果は、「その特別な目的を認識」し[10]、通常は憲法上の権利の解釈に用いられる広く寛大な目的論的解釈を行うことを正当化するというものである[11]。カナダ最高裁はどのような特徴をもつ法律が準憲法的法律になるかについて明確な基準を打ち出してはいないが、「憲

[4] *Lavigne v. Canada (Office of the Commissioner of Official Languages), [2002] 2 S. C. R. 773,* at para.24-25.
[5] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, [2013] 3 S.C.R. 733 at para.19.
[6] この法律はいわゆる個人情報保護法ではなく特定のプライバシー侵害行為を不法行為であるとする法律である。
[7] *Douez v. Facebook, Inc.*, [2017] 1 S.C.R. 751 at para.59.
[8] Andrea Slane, “There Is a There There: Forum Selection Clauses, Consumer Protection and the Quasi-Constitutional Right to Privacy in Douez v. Facebook” (2019) 88 S. C. L. R. (2d) 87 at 99.
[9] *Thibodeau v. Air Canada*, [2014] 3 S.C.R. 340 at para.12.
[10] *Lavigne v. Canada, supra* note 4, at para.24.
[11] Vanessa MacDonnell, "A Theory of Quasi-Constitutional Legislation" (2016) 53 Osgoode Hall Law Journal 508 at 510.

法が定める価値や権利と密接に結びついている」ことを準憲法的法律とすることの根拠として指摘しており[12]、学説では準憲法的法律は「憲法上の要請を実施するための法律」であると理解すべきだとの整理がなされている[13]。

この点に関して、①準憲法的法律は憲章8条が保障する権利の具体化ではなく、その背後にあるプライバシーに関する憲法的価値の具体化であること、②それゆえ、憲法上の権利としての具体化と、準憲法的法律としての具体化が分岐していることに注意が必要である[14]。なお、ここで想定されるプライバシーの憲法上の価値は、便宜的に㋐民主主義に関連するものと、㋑個人の自律に関連するものに整理できる。たとえば、Dagg判決のラフォレスト裁判官の反対意見（この点については多数意見を形成）で、アメリカの憲法学者ウェスティンの著作[15]などを引用しつつ、「プライバシーの保護が現代の民主的国家にとって基本的価値であること」、「プライバシーは、身体的及び道徳的な自律性、すなわち自分自身の考え、行動、決定に関わる自由に基盤を持つこと」が述べられている[16]。Lavigne判決はこの反対意見を引用し、これらの価値を再確認している（para.25）。さらに、UFCW Local 401判決は、「活力ある民主主義のもとでのプライバシー保護の重要性は、いくら強調してもしすぎることはない」という（para.22）。また、同判決は「個人が自分の個人情報をコントロールする能力は、個人の自律性、尊厳、プライバシーと密接に関係している。これらは民主主義の根幹をなす基本的価値である」ともいう（para.19）。

以上の通り、カナダにおいては憲法的価値と個人情報保護法の連関を読み取ることができ、これを憲法実施法であると捉える見解も有力である。

個人情報保護法を準憲法的法律として位置づけている点は、個人情報保護法と憲法の関係性が希薄と思われる日本と比べたとき示唆的である。とくに、カナダ最高裁が、もともと憲法実施法として制定されたわけではない個人情報保護法を、事後的に憲法的価値と関連性をもつ準憲法的法律として認めていった道程は[17]、日本における個人情報保護法と憲法のこれからの関係を考える上で参考になると思われる[18]。また、カナダ最高裁が民間部門を対象とする個人情報保護法も準憲法的法律としている点も重要である。この傾向は、私人間での個人情報保護を憲法的価値のもとで行っていく方向性を示しているといえるだろう。

---

[12] *Lavigne, supra* note 4, at para.25.
[13] MacDonnell, *supra* note 11, at 510-511.
[14] 厳密にいえば、公的機関を対象とする準憲法的法律は部分的には憲章8条の具体化として捉える余地もある。
[15] Alan F Westin, *Privacy and Freedom* (Atheneum, 1970).
[16] *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, paras.65-66.
[17] 国家目標の具体化という観点からカナダの試みを再構成することもできるかもしれない。石塚壮太郎「社会国家・社会国家原理・社会法」法政論究101号（2014年）197頁以下参照。
[18] 異なるアプローチではあるが、實原隆志「個人情報保護法制と憲法」情報法制研究12号（2022年）38頁以下も参照。

2. 個人情報保護法制の現状と課題

Q2-①. 個人情報保護法を制定するにあたってモデルとした国はあるか。

プライバシー法、PIPEDA はともに、1980 年の OECD のガイドライン[19]に強い影響を受けているとされる[20]。とくに、PIPEDA は、OECD8 原則を参照してカナダ規格協会（the Canadian Standards Association）が作成した 10 原則（PIPEDA の別表 1）の遵守を原則とし、本体ではその例外を定めるという建付けになっている。また、PIPEDA 制定の背景としては、EU データ保護指令が採択されたことの影響もある。

Q2-②. クッキー情報は個人情報保護法制における「個人データ（個人情報）」のなかに含まれているか。個人情報保護法上保護の対象となる「個人データ（個人情報）」の定義。

プライバシー法も PIPEDA もその保護する「個人情報」は「個人を識別可能な情報」である。プライバシー法 3 条は、あらゆる形態で記録された個人を識別可能な情報を保護する。同条(a)~(i)号は、ここでいう個人情報に含まれる情報を列挙しており[21]、また、同条(j)~(m)号は同法の「個人情報」に含まれない情報を列挙する[22]。ただし、Dagg 判決でカナダ最高裁は、プライバシーの憲法的価値に言及したうえで、プライバシー法の「個人情報」は広く拡張的に定義されなければならないとしている[23]。よって、少なくともプライバシー法上の「個人情報」はプライバシー法自体が列挙している情報に限らず、広く保護の対象となりうる。

PIPEDA も個人を識別可能な情報を保護対象とする（2 条）。プライバシー法との違いの 1 つが、PIPEDA の場合は情報が記録されているか否かにかからず保護の対象に含まれる点である。OPC[24]のウェブページでは、年齢、氏名、ID 番号、収入、民族的出身、血液型、意見、評価、コメント、社会的地位、懲戒処分歴、ローン記

[19] Organisation for Economic Co-operation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (23 September 1980).
[20] Barbara von Tigerstrom, *Information & Privacy Law in Canada* (Irwin Law, 2020) at 233-234, 294.
[21] 本人の人種、国籍、民族的出身、肌の色、宗教、年齢、婚姻状況に関する情報、個人の学歴、病歴、犯罪歴、職歴に関する情報、個人が関与した金融取引に関する情報、個人に付与された識別番号、記号、個人の住所、指紋、血液型、個人の私的な意見などの情報が挙げられている。
[22] 過去又は現在連邦政府の職員であること、死後 20 年以上経過した個人に関する情報などが挙げられている。
[23] Dagg, *supra* note 16, para. 68.
[24] OPC はプライバシー法及び PIPEDA の監督機関であり、Office of the Privacy Commissioner の略称である。詳しくは Q2-④で説明する。

録、医療記録などが保護の対象に含まれるとされている[25]。

PIPEDA はクッキー情報について直接言及していないが、OPC のガイドラインによれば、個人に対してターゲティング広告を行うための「オンライン上での追跡及びターゲティングに関わる情報は、一般的に個人情報に該当する」としている[26]。このガイドラインに従えば、クッキー情報は PIPEDA の保護する個人情報となり、その収集、利用、開示には少なくとも黙示の同意が必要となる。

Q2-③. データ主体の権利と事業者の義務

Q2-③(a). 利用停止請求権の範囲

プライバシー法は、公的機関の事業又は活動の運営に直接関係する場合にのみ個人情報の収集を許容し（4 条）、目的外利用を禁止し（7 条）、公的機関に対して情報の正確性を維持することを義務付けるが（6 条）、公的機関の記録から個人情報の削除を求める権利は認めていない[27]。プライバシー法が規定するのは、自己情報の開示及び訂正を請求する権利、訂正請求を行ったが訂正がなされなかった場合、訂正の請求があった事実を当該情報に付記する権利である（12 条 2 項(a),(b)）。政府は、請求がなされた場合、通常 30 日以内に請求に対応する[28]。なお、プライバシー法に基づき、政府保有の自己情報の開示を請求できるのは、カナダ国民及び移民難民保護法[29]によって永住権を認められた者である（12 条 1 項）。

PIPEDA は、第 9 原則として個人のアクセスを挙げている。同原則によれば、個人には PIPEDA の適用対象となる組織（以下単に「組織」という場合もこの意味での「組織」を指す）が有する自己の個人情報に対する開示及び修正を請求することができる。請求者が組織の保有する個人情報が不正確ないし不完全であると証明した場合、組織は当該情報を修正しなければならない。この修正は情報の性質に応じて、情報の訂正、削除、又は追加（the correction, deletion, or addition of information）によって行われる（別表 1, s.4.9, 4.9.5）。

Q2-③(b). 同意の位置付け（オプトイン方式かオプトアウト方式か）。本人の同意が要求される場面は。事業者が個人データを取得する場合に当該個人の同意を得ることが義務付けられているかどうか。また、個人データが第三者に提供される場

[25] OPC, “PIPEDA in brief” (May 2019). 本報告書におけるウェブサイトの最終閲覧日はすべて、2023 年 9 月 13 日である。
[26] OPC, “Guidelines on privacy and online behavioural advertising” (December 2011; Revised: August 2021).
[27] Tigerstrom, *supra* note 20, at 242.
[28] OPC, “The Privacy Act in brief” (August 2019). Tigerstrom, *supra* note 21, at 241.
[29] *Immigration and Refugee Protection Act*, S.C. 2001, c. 27, s.2(1).

合、当該個人の同意を得ることが義務付けられているかどうか。

プライバシー法については、個人情報の収集、利用、（第三者への）開示に原則として事前の同意が必要である（8条1項）。同法8条2項は第三者への開示に本人の同意が必要ない場合として、大別して以下の5つを規定している。①収集された当初の目的又はその目的に合致した使用のために開示する場合、②連邦法で開示が許可されている場合、③裁判所または情報を強制する権限を持つその他の機関の令状又は命令に従う場合、④開示が明らかに個人の利益になる場合、⑤開示の公益がプライバシーの侵害を上回る場合[30]。

PIPEDAは、その第3原則が同意であり、個人情報の収集、利用、開示に原則として事前の同意を要求する。また、この同意のためには、個人情報の利用目的、使用・開示のされ方について合理的に理解できるような通知がなされなければならない。この点は、2015年のデジタルプライバシー法による改正でより明確にされた。同改正で追加された6.1条は、個人の同意は、個人情報の収集、利用又は開示の性質、目的、結果を理解することが合理的に期待できる場合にのみ有効である、としている。プライバシー慣行の重大な変更、個人情報の利用目的の追加・変更、新たな第三者への開示を行う場合も同意を得ることが求められる。子どもの個人情報については親あるいは保護者の同意を得る必要がある。同意の方法としては様々な方式が許容されているが、センシティブ情報については明示的な同意が必要だとされる。ただし、同法は医療記録や所得記録はほとんどの場合センシティブ情報に該当しうるとしつつも、個別具体的には文脈に依存するとしており、何がセンシティブ情報になるかについて明確な規定を置いていない。また、個人は、「法律上または契約上の制限および合理的通知に従い、いつでも同意を撤回できる」（別表1, s. 4.3.8）。なお、4条2項及び2015年の改正で追加された4.01条ではPIPEDAの適用除外が規定されており、同条項に該当する事項にはPIPEDAが適用されない。さらに、7条は個人情報の収集、使用、開示に（通知と）同意が必要ない場面を詳細に規定する。

Q2-③(c). ＜通知＝同意＞モデルの限界とその対策。個人の認知限界という観点から＜通知＝同意＞モデルの限界（同意疲れやプライバシーポリシーの流し読み）が予てから指摘されている。こうした課題に対して、各国の個人情報保護法制がどのように対応しているか（事業者に対して実効的な告知方法を義務付けるなど）。

カナダでも「意味のある同意」をどのようなものと考えるかは大きな論点となっている。

たとえば、OPCは2016年に「同意とプライバシー」についてディカッションペ

[30] *See,* OPC, "The Privacy Act in brief" (August 2019)

ーパーを公表し[31]、2018年には「意味のある同意を得るためのガイドライン」を公表している[32]。これらの取り組みは、まさに、冗長で法律的なプライバシーポリシーが使用されていることによって、個人情報のコントロールおよび個人の自律が、往々にして幻想に過ぎないものとなっている、との問題意識の下で行われている。

2018年のガイドラインでは、OPCがプライバシーポリシーのひな型を提案する案を否定し、組織こそが、法的義務だけでなく、顧客との関係の性質を尊重する同意プロセスを開発するための革新的かつ創造的な解決策を見出すのに最も適している、と述べている。このような前提のもと、このガイドラインでは組織がよりよい同意プロセスを設計する際に考慮すべき指針を挙げている。それは、①重要な情報を強調すること、②個人が、いつ、どのレベルの詳細な情報を得るかをコントロールできるようにすること、③「同意する」・「同意しない」の明確な選択肢を個人に提供すること、④革新的・創造的であること、⑤消費者の視点に立つこと、⑥同意を動的かつ継続的なプロセスにすること、⑦アカウンタビリティを果たすこと、の7点である。

一部簡単に補足すると、①は以下の4つの要素についてはプライバシーポリシーや利用規約のなかで埋もれてしまわないように強調する必要があるとする。それは、㋐どのような個人情報が収集されるか、㋑個人情報の共有先、㋒個人情報の収集、使用、開示の目的、㋓危害およびその他の結果に関するリスク、である。ただし、現時点では、どのような形でこれらの要素を強調すべきかの正解はないとされる。さまざまな分野でのベストプラクティスの出現が期待されている。②は、利用者の情報接触のさまざまな傾向――プライバシーポリシーなどの概要をざっと見たいだけの人、事前／事後に深く読み込みたい人など――に対応することが望ましいとされる。情報をレイヤー形式で表示することなどの工夫が求められる。④では、必要な情報を適時に表示することや、使用されるインターフェイスに適した同意プロセスの設計を奨励している。⑦では、「組織が有効な同意を取得していることを証明するためには、プライバシーポリシーに埋もれた項目を指摘するだけでは不十分」とし、「組織は、……個人から同意を得るためのプロセスがあり、そのプロセスが法律に定められた同意義務に準拠していることを証明できなければならない」としている。上記の通り、PIPEDAは、同意のために、個人情報の利用目的、使用・開示のされ方について合理的に理解できるような通知がなされることを要求している。⑦はこの点の確認でもあるが、OPCは単に冗長なプライバシーポリシーでこれらについて記述しているだけでは不十分であるとしているのである。同ガイドラインは、①～⑦のほかに、同意の撤回を尊重すべきこと、同意が銀

[31] OPC, "Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act" (May 2016).
[32] OPC, "Guidelines for obtaining meaningful consent" (May 2018; Revised: August 13, 2021).

の弾丸ではないことにも注意を促している。

法律レベルでは、原則同意を要求しつつも、同意が不要な場合の例外を幅広く認めようとする方向性を模索していると思われる。PIPEDA 自体もそうだが、とくに、消費者プライバシー保護法は、個人情報の収集、利用、開示について原則明示的な同意を求める枠組みを採用しつつも、同意が不要な場合などの例外を認めている。匿名加工情報の取扱いなどをも含め同意の例外を広範に例示することで、自己情報のコントロールと利便性のバランスを図ろうとしているものと思われる。

Q2-③(d). 情報銀行や PDS(Personal Data Store)のように、パーソナル・データに対する本人の controllability を補助するための仕組みや制度はどのように社会実装されているか。

プライバシー法は個人情報バンク（personal information banks）の仕組みをもつが、これは、各公的機関の長に対して、当該公的機関が管理する個人情報のうち、㋐行政目的のために利用された、利用されている、又は利用することができるもの、㋑個人の名前、個人に割り当てられた識別番号、符号、その他の特定の方法で整理され、検索できるようにされているもの、について、すべて個人情報バンクに登録させ、バンクの概要（当該情報を取り扱う趣旨、目的、情報の種類など）を一般公開する仕組みである。プライバシー法上の個人情報バンクは日本の個人情報保護法でいうところの個人情報ファイルの仕組みに近いものである。

一方で、PIPEDA には同様の仕組みはない。そのため、個人情報のコントロールは対公的部門では強く保障されているが、対民間部門ではコントロールを補助するための仕組みに課題があるといえる。

Q2-③(e). AI の利活用やプロファイリングの場面に特化したデータ保護の仕組みが存在するかどうか。

AI の利活用に特化した仕組みは現行法上ないが、AI データ保護法が成立すれば、AI の利活用に特化したデータ保護の仕組みが導入されることになる。

同法提案の狙いは、カナダの価値に沿う信頼できる AI 規正の枠組みを提示すると同時に、政府が責任あるイノベーションを阻害したり、AI の開発者、研究者、投資家、起業家を不必要に排除したりすることのないアジャイルなアプローチを採用しようとするものだとされている[33]。同法の目的は、AI システムの設計、開発、使用について、カナダ全土に適用される共通の要件を定めることにより、AI システムの国際的及び州間の商業活動を規律すること、及び AI システムに関連して、

[33] Innovation, Science and Economic Development Canada, “The Artificial Intelligence and Data Act (AIDA) – Companion document” (March 2023).

個人又は個人の利益に重大な損害を与えるおそれのある特定の行為を禁止することである。なお、同法は連邦の公的機関には適用されない。同法は EU の AI 規則案と同じくリスクベースアプローチを採用している。同法の仕組みは、AI システムを利用する企業に対して、当該 AI システムが「高影響システム（high-impact system）」かどうかを評価させ、高影響システムである場合には、設計、開発、使用可能にすること、または当該システムの管理について追加的な義務を課すというものである。何が高影響システムであるかは、別途規則で定める要素との適合性から判断され、その要素は、健康及び安全に対するリスクと人権に対するリスクの観点から設定される。さらに、①AI 開発のために不法に取得したデータを用いること、②深刻な身体的又は心理的危害を与える可能性のある AI システムを利用可能にし、当該 AI システムによって損害が引き起こされた場合、③公衆を騙すあるいは個人に実質的な経済的損失を与える意図をもって AI システムを使用することなど、に対して刑事罰を科しており、法人の場合は最高で 1,000 万ドルもしくは前会計年度の世界収益の 3%のいずれか大きい額の罰金となる。また、同法の監督などのために AI データコミッショナーが設置される。

プロファイリングに関する明文の規定は現行法上ない。しかし、PIPEDA の 5 条 3 項は「合理的な人が状況に応じて適切であると考える目的のためにのみ、個人情報を収集、使用、開示することができる」と規定しており、この規定は個人情報を扱う目的によっては同意を得たとしても組織が扱ってはならない「立入禁止区域（No-go zones）」を設定していると解されている[34]。OPC のガイドラインによれば、人権法が規定する事由に関する差別をもたらすような方法でおこなわれるプロファイリングは、5 条 3 項の適切な目的に該当しないと解されている[35]。

Q2-③(f). データ・ポータビリティ権は保障されているか。またこの権利は具体的にどのような場面で社会実装されているか。

現行法上はないと思われる。消費者プライバシー保護法はデータ・ポータビリティ権を規定している。

Q2-④. 個人情報保護法を執行する監督機関の組織と権限（制裁や告訴の仕組み）。

プライバシー法及び PIPEDA の監督機関は、プライバシー法によって設置されたプライバシー・コミッショナー及びコミッショナーを長とする OPC（Office of the Privacy Commissioner）である。

[34] OPC, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)" (May 2018).
[35] OPC, *ibid.*

コミッショナーは形式的には総督によって任命されるが、この任命にあたって連邦上院および下院の決議で任命の承認が行われる必要がある。コミッショナーの任期は 7 年であり、再任も可能である。現在のコミッショナー（2022 年 6 月 27 日～）は、人権問題、行政法、憲法を専門とする Philippe Dufresne 氏である。彼の前職は、法務サービスの提供や立法支援などを職務とする連邦下院の the Law Clerk and Parliamentary Counsel である。OPC の組織[36]は、大きく、①コンプライアンス部門、②政策推進部門、③組織管理部門に分かれており、各部門を担当する副コミッショナーによって監督されている。現在、3 名の副コミッショナーが置かれている。また、コミッショナー直属の④法務サービス部門が設置されている。それぞれ簡単に補足すると、①コンプライアンス部門は、プライバシー法及び PIPEDA に基づく調査を行う部門であり、市民からの苦情に基づく調査だけでなく、自己付託により調査を開始する場合もある。この部門には、プライバシー法部局、PIPEDA 部局、コンプライアンス・苦情受付・解決部局が置かれている。②政策推進部門は、プライバシーに関する一般的な情報やガイダンスの作成と普及、各業界・組織へのアドバイスなどを行う部門である。この部門には、政府助言部局、企業助言部局、政策・調査・議会部局、技術分析部局、コミュニケーション部局の 5 つの部局が置かれている。③組織管理部門は、OPC の組織内部の事務および管理を担う部門であり、人材部局、財務・経理部局、情報管理・情報技術部局、事業計画・業績・監査・査定部局が置かれている。④法務サービス部門は、法的助言を行うことで OPC の業務活動を支援する部門である。また、これらの他に内部監査委員会も置かれている。

コミッショナーは、個人情報の不適切な利用、個人情報へのアクセス拒否などの苦情を受付け、調査を行う権限などを有する。調査は職権によって行うこともできる。公的機関への立入調査を行う権限なども付与されており、調査結果や勧告を公的機関の長に報告するが、その判断に拘束力はない（29~35 条）。プライバシー法は同法違反に対する損害賠償を求めることができる規定も持たない。個人情報の開示拒否の場合は、調査結果の報告を受けた後、当該個人及びコミッショナー自身も個人の同意に基づき、連邦裁判所に審理を求めることが可能である（41, 42 条）。この申請は、調査結果の受領後 45 日以内もしくは裁判所が認める期間内におこなわなければならない。

PIPEDA に関しても、コミッショナーはプライバシー法の場合と同様の権限を有しており、調査結果に法的拘束力はなく、PIPEDA 違反に対して制裁金や損害賠償を命じる権限はない。コミッショナーによる調査報告書もしくは調査の中止の通知の受領後、個人は連邦裁判所に審理を求めることが可能であり、コミッショナーも個人を代理してこれを行うことができる（14, 15 条）。連邦裁判所への申請の期限は、報告書もしくは調査中止の通知の受領後、1 年以内もしくは裁判所が認めた

[36] *See*, OPC, “Organizational Structure” (August 2023).

それ以上の期間内である（14 条(2)）。連邦裁判所は、PIPEDA に適合するように組織の慣行を是正するよう命じることや、組織に損害賠償を命じることなどを含む救済を与えることができる（16 条）。また、2015 年のデジタルプライバシー法による改正によって、コンプライアンス協定という仕組みが導入されている。これは、コミッショナーが、ある組織が PIPEDA 違反ないし別表 1 の遵守事項の不履行となる作為・不作為を行った・行おうとしている・行う可能性が高いと合理的根拠に基づき判断した場合、PIPEDA を遵守することを目的とするコンプライアンス協定を締結することができる、というものである。コンプライアンス協定は組織に PIPEDA の遵守に同意することを求めるが、その代わりに、協定を締結した場合、コミッショナーは 14 条・15 条に基づく連邦裁判所への申請を行うことができなくなる。ただし、組織がコンプライアンス協定に違反した場合は、組織に協定の内容を遵守するよう求める命令を裁判所に申請することができる。

プライバシー・コミッショナー及び OPC は、「『プライバシーと他の法益の衝突に直面した場合には、プライバシーの保護を優先させる』という一般的傾向性」を持つと指摘されており[37]、カナダのプライバシー保護にとって重要な役割を担っているが、その権限自体は強力なものではない。消費者プライバシー保護法はプライバシー・コミッショナーの権限強化にも取り組もうとしている。

Q2-⑤．司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

プライバシー法および PIPEDA に基づく司法的救済の仕組みは上記（A7）の通りであるが、若干の補足をしておく。

プライバシー法については、個人の情報アクセス制限に対してのみ裁判所への提訴を認めているが、近時の下級審のなかには、プライバシー法に反する個人情報の収集についても司法審査の対象としたものがある[38]。また、クラスアクションについては、連邦裁判所規則の Part 5.1 に従い認められるかが判断される[39]。PIPEDA については、同法 14 条に基づく手続においてクラスアクションが認められるかが争点となっているようである[40]。

なお、個人情報及びデータ保護審判所法は、個人情報及びデータ保護を専門的に扱う審判所を設置することを構想している。同審判所は、消費者プライバシー保護

[37] 佐藤・前掲注（1）181 頁。
[38] Union of Canadian Correctional Officers - Syndicat des Agents Correctionnels du Canada - CSN (UCCO-SACC-CSN) v. Canada (Attorney General), [2017] 3 F.C.R. 540
[39] *e.g.*, *Canada v. John Doe*, 2016 FCA 191. 直近では、カナダ政府のオンラインアカウント（カナダ歳入庁の「マイアカウント」・「マイサービスカナダ」）の使用に伴い発生した権利侵害の可能性についてクラスアクションが提起されている。*See,* Government of Canada, "Notice of Certification: Government of Canada Privacy Breach Class Action" (August 2023).
[40] *See*, *Haikola v. The Personal Insurance Company*, 2019 ONSC 5982.

法に基づく申立て、同法に基づくペナルティの賦課について管轄権を有する。審判所は 3～6 名の構成員からなり、最大任期は 5 年である（ただし再任は可能）。構成員は同法の担当を指名された大臣の推薦に基づき、総督によって任命される。構成員のうち少なくとも 3 名は情報・プライバシー法の分野での経験を有する者でなければならないとされている。

プライバシー法や PIPEDA に基づく司法救済とは別に、コモンローあるいは、特定の行為をプライバシー侵害とする州法[41]に基づいてプライバシー侵害を理由とした救済を求める仕組みもある[42]。

Q2-⑥. 診療記録等を医薬品開発などの研究目的で利用する場合に、データ主体である患者の同意は要請されるのか？診療データを二次利用するにあたって、匿名加工などの一定の義務が課せられるか？

本質問項目は追加質問として示されたされたものであり、短期間で調査することは困難であったため回答不能である。以下では参考までに、カナダにおける個人健康情報に関する法制度の概要と、オンタリオ州の個人情報保護法の規定について若干の紹介をするが、不十分な調査であることをお断りしておく。

カナダにおける個人健康情報の取扱いはかなり複雑である。多くの州で個人健康情報を特別に扱う法律が存在しており（→はじめにを参照）、また、公的部門に適用されるものと民間部門に適用さるものが分かれている場合もある。さらに、個人健康情報の商業的利用については PIPEDA の適用もある。このように入り組んだ体系となっているため、実態把握のためには実質的には各州法を調査する必要があるので、本調査期間内で調査することは困難であった。

オンタリオ州の個人情報保護法（*Personal Health Information Protection Act*, S.O. 2004）に関する規律を紹介しておく。

同法によれば、個人健康情報[43]の研究目的での開示については一定の条件の下、本人の同意を得る必要はない（44 条）。その条件として、まず、①個人健康情報の保管・管理者（health information custodian、以下単に「管理者」とする）に、書面で、研究計画書及び当該研究計画を承認した研究倫理委員会の審査結果の写しを提出することが求められる。研究計画には、㋐研究に関与する人物の所属、㋑研究の性質・目的、および研究者が予測する研究の公益または科学的利益などの記載が

41 e.g., *supra* note 6.
42 *See*, Tigerstrom, *supra* note 20, ch2.
43 同法の定義する「個人健康情報」は個人を識別する情報であり、個人の身体的または精神的健康に関する情報、個人に対するヘルスケア提供に関する情報、個人に関する医療費の支払いに関する情報、個人の健康番号などが含まれる。また、「識別する情報」には、単独で識別可能なものだけでなく、他の情報と合わせて使用することで識別が可能となり、その状況が合理的に予測できる情報も含まれる（4 条）。

求められる。倫理審査では、以下の観点を含む関連事項が考慮されなければならない。ⓐ個人健康情報の開示対象となる個人のプライバシーを保護し、情報の機密性を保持するための適切な保護措置が講じられるかどうか、ⓑ研究を実施することの公益性、および個人健康情報が開示される個人のプライバシーを保護することの公益性があるかどうか、ⓒ個人健康情報が開示される個人の同意を得ることが非現実的であるかどうか。次に、②個人健康情報を開示する前に情報の取扱いについて管理者の課す条件に研究者が従うことに同意する契約を結ばなければならない。この他、③研究者には、倫理委員会から承認された目的のためにのみ情報を利用すること、個人の識別が合理的に可能になる形で情報公開しないことなどの遵守事項が課せられている。

以上。

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

Ⅹ. United States

Survey of US Federal Privacy Law and the California Privacy Rights Act

Jesse Woo

Both doctrinally and practically, the United States has one of the most complicated bodies of privacy law of any jurisdiction. This complexity stems not from a single statutory regime that seeks to regulate most aspects of data collection and processing (as with is the case with the General Data Protection Regulation in Europe), but rather the opposite. U.S. consumer privacy law is fragmented and lacks a comprehensive governing statute. This report will provide an overview of U.S. federal privacy law as well as the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), which at the time of writing is the most comprehensive and protective consumer privacy law in the country.

Section 1 of this report will provide a broad overview of privacy law in the United States at the Federal and State level, the practical import of self-regulatory models, and emerging issues related to consent. Section 2 will address enforcement issues.

1.1 U.S. Constitutional Law

With some notable exceptions not directly relevant to information privacy, the U.S. Constitution regulates government power, rather than private action. When U.S. persons (citizens and lawful permanent residents) are said to have a "constitutional right," this typically means a right against some government action, or at least against government support of certain private actions.[1] The term "privacy" is also not explicitly found in the text of the Constitution.

Still, concepts that relate to privacy are said to arise from the First, Fourth, and Fifth amendments (among others), as well as from the judicially derived doctrine of substantive due process. The First Amendment protects the right to freedom of expression, and the Supreme Court has held that free expression can require a right to anonymity for certain groups engaging in that expression.[2] In a very real sense this is a form of informational privacy, but again only applies in limited circumstances such as when the government seeks to compel disclosure of anonymous members of a group. The Fifth Amendment protections criminal defendants from having to incriminate themselves and also protections private property, which scholars often characterize as a type of privacy right. In addition, the doctrine of substantive due process is seen as a type of privacy right that protects an individual's autonomy. The rights to access birth

[1] For instance, private contracts in the form of racially restrictive covenants were held to be unconstitutional under the Equal Protection clause of the 14th Amendment because they required government action to be enforced. Shelley v. Kraemer 334 U.S. 1 (1948).
[2] NAACP v. Alabama ex. Rel. Patterson 357 U.S. 449 (1958).

control, to interracial marriage, and until recently to an abortion were protected by substantive due process.

The Fourth Amendment is probably the Constitutional provision most directly related to the informational privacy. It protects against unreasonable searches and seizures by government agents and is most often invoked in the context of criminal prosecution, though it applies broadly to other government actors. Although its text speaks to unreasonable searches and seizures of "persons, houses, papers, and effects," the Fourth Amendment has come to regulate government access to electronic data as well. For example the Supreme Court has held that the government must obtain a warrant before digitally searching the contents of a cell phone,[3] and before accessing a record of a person's location based on cell phone records.[4] Supreme Court search and seizure doctrine is extremely complex, but as it is not especially relevant to the notion of informational self-determination I will not elaborate further. Existing sources cover the topic well. It suffices to say that the U.S. Constitution's application to privacy outside of government action is limited. Several state constitutions also explicitly enumerate a right to privacy, and in some cases it has been suggested that the state rights are stronger than the federal constitutional right, but in practical effect there is nothing in federal or state constitutional law that looks anything like a right to information self-determination.

1.2 U.S. Privacy Law: Federal

There is no generally applicable federal consumer privacy statute or comprehensive data protection law. Instead, the U.S. takes a "sectoral" approach, where specific industries or verticals are governed by their own laws, which are limited in scope. For example, healthcare privacy is governed by the Health Insurance and Portability and Accountability Act (HIPAA), financial privacy by the Gramm-Leach-Bliley Act (GLBA) or Fair Credit Reporting Act, and government records by the federal Privacy Act. The reach of these laws is typically limited to certain organizations, e.g. HIPAA applies to certain data processed by "covered entities" that are defined in statute like doctor's office, and their "business associates." An organization that holds health data but does not fall under one of these definitions will not be bound by the restrictions of HIPAA. Similarly, specific regulatory agencies may issue rules that govern the organizations under their purview. The Department of Health and Human Services issues a privacy rule to further define the HIPAA statutory language. On the other hand, the Children's Online Privacy Protection Act (COPPA) protects the data of all children under 13 years of age regardless of setting or industry, but only when a business possesses "actual knowledge" that it holds a child's data or directs their services at children.

The primary federal privacy regulator is the Federal Trade Commission (FTC), which enforces a "notice and choice" regime.[5] The FTC regulates using the authority granted by its authorizing statute, called "section 5", that gives it the power to regulate "unfair and deceptive practices" in

[3] Riley v. California 573 U.S. 373 (2014)
[4] Carpenter v. United States, 138 S.Ct. 2206 (2018)
[5] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change", https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

commerce. When it comes to privacy, the commission typically acts by performing investigations into companies for deceptive practices and, where appropriate, issuing a "consent decree," which is a kind of negotiated agreement where a company pays a fine and agrees to change its behavior to avoid a lawsuit (kind of like pleading guilty). Consent decrees are public and form a limited sort of common-law for federal privacy. There are numerous literature reviews of FTC privacy consent decrees that I will not duplicate here. For somewhat arcane reasons relating to political history, the FTC does not normally issue rules under section 5 authority, but does if Congress has granted authority in another law, such as under COPPA. Because of this limited authority, the FTC mainly acts when a company has acted deceptively, such as when it makes public statements in its privacy policy that are not true.

All this is to say that, unless a company is in a heavily regulated industry like healthcare or finance, there is relatively little they must do to conform with federal privacy law. They should have a public facing policy, and they must abide by terms of whatever they put in that policy. Policies are typically driven by "best practices," and are written in a way to give companies leeway to act. This is why they are often ambiguous or difficult to understand. Companies must give consumers "notice" in the form of a privacy policy, and "choice" in whether to accept the terms of that policy. Just as there is no constitutional guarantee of informational self-determination, there is no federal data protection law, so the default regulatory posture is quite permissive regarding a company's ability to collect, process, and transfer personal data.

1.3 State Privacy Law: CPRA

Several states have passed generally applicable consumer privacy laws, but the most influential and most protective is California's Privacy Rights Act (CPRA). The CPRA amended an earlier privacy law called the California Consumer Privacy Act (CCPA), and together they are often seen as a major milestone in consumer privacy law in the U.S. It applies to entities who do business in California and either have gross annual revenue over $25 million dollars; buy, sell, or share the information of at least 100,000 consumers, or derive at least 50% of their revenue from selling or sharing consumer information.[6] Because California has both the largest population and economy of any U.S. state, CPRA's effect is quite large even though it is not federal.

The law establishes certain consumer rights, namely: 1) the right of access, 2) right of rectification, 3) right of erasure, 4) a right to know how information is sold or shared, as well as 5) the right to prevent the sale of data. Under CPRA consumers also have the right to limit how companies use or disclose "sensitive personal information" to purposes which are necessary to deliver the goods or services that the company provides to the consumer. Companies must obtain consent to use this information in any other way.[7] There is no specific right to object to processing or profiling, or to data portability as found in the GDPR.

Companies must also limit their collection, use, retention, and sharing of personal data to what is necessary and proportionate for the purpose which it was collected.[8] Third parties who obtain

[6] California Civil Code 1798.140 (d).
[7] California Civil Code 1798.121.
[8] California Civil Code 1798.100 (c).

personal data under agreement with the collecting entity must also respect these rights and limitations.

CPRA defines personal information as:

> *information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:*
>
> *(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.*
>
> *(B) Any personal information described in subdivision (e) of Section 1798.80.*
>
> *(C) Characteristics of protected classifications under California or federal law.*
>
> *(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.*
>
> *(E) Biometric information.*
>
> *(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.*
>
> *(G) Geolocation data.*
>
> *(H) Audio, electronic, visual, thermal, olfactory, or similar information.*
>
> *(I) Professional or employment-related information.*
>
> *(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).*
>
> *(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.*
>
> *(L) Sensitive personal information.*

It excludes public information, matters of public concern, or information that is aggregated or de-identified from this definition.[9] This is one of the most detailed and comprehensive definition of personal information in U.S. privacy law, and likely includes cookies and other online identifiers. It appears to be anticipating the import of machine learning by including inferences drawn from other information. Sensitive personal information is a separate category of data that is similar to the GDPR's definition of special category data but also includes "precise geolocation data".[10]

The statute also establishes a California Privacy Protection Agency to enforce the law and to issue rules that clarify ambiguities or address novel problems. However, it is important to note that much of the law still relies on notice and consent. Companies must notify consumers of how they will use data, and obtain consent for changes. As a state law it applies to companies who serve consumers in California, although differentiating by location is difficult so many companies may choose to apply it broadly.

CCPA/CPRA seem to take some inspiration from the GPDR, particularly in emphasizing consumer rights and data minimization principles as represented in the "necessary and proportionate" language, a term borrowed from EU jurisprudence. Obligations to protect consumer data must also follow the data contractually when the data changes hands, although it does not use the same language of data "controllers" and "processors."[11] In general it does not seek to be as comprehensive as the GDPR, shying away from explicitly regulating developing fields like AI (i.e. it lacks a provision on automated processing).

1.4 Privacy Standards and Self-Regulation

In all jurisdictions, but especially those that lack explicit privacy statutes like the U.S., industry standards and self-regulation are an important source of privacy protection. The most common set of standards are the Fair Information Practices (FIPs, sometimes also called Fair Information Privacy Practices or FIPPs). The Organization for Economic Cooperation and Development (OECD) articulated a commonly cited version of the FIPs in the 1980s.[12] The FTC has its own formulation that is similar.[13] The FIPs are broad principles or guidelines about what constitutes good privacy. They are:

1. **Collection Limitation Principle**. 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.
2. **Data Quality Principle**. 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.

[9] California Civil Code 1798.140 (v)
[10] California Civil Code 1798.140 (ae).
[11] California Civil Code 1798.100 (d)(2).
[12] OECD, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188
[13] FTC "Privacy Online: Fair Information Practices in the Electronic Marketplace", https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

3. **Purpose Specification Principle**. 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 fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle**. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
    a. with the consent of the data subject;
    b. by the authority of law.
5. **Security Safeguards Principle**. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness Principle**. 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.
7. **Individual Participation Principle**. An individual should have the right:
    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b. to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
    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. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. **Accountability Principle**. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Scholars have debated the usefulness of the FIPs,[14] but they remain a frequently cited standard for "good" privacy. Many corporate privacy policies are written in such a way as to address the principles. When companies talk about having "good" privacy practices, they are often referring to some version of the FIPs.

1.5 Consent and Dark Patterns

As mentioned previously, U.S. privacy law primarily operates on a "notice and choice," or consent based model. However, recent scholarship has focused on the limits of the consumer's ability to effectively exercise consent given the prevalence of choice architecture and behavioral psychology techniques in digital interfaces that can subtly nudge them into choices that favor the company's interests at the expense of their privacy.[15] Broadly speaking these techniques are

[14] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 Md. L. Rev. 952 (2017). https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3759&context=mlr

[15] Jen King, Adriana Stephan, *Regulating Privacy Dark Patterns in Practice – Drawing Inspiration from California Privacy Rights Act*, 5 Geo. L. Tech. Rev. 250 (2021). https://georgetownlawtechreview.org/wp-content/uploads/2021/09/King-Stephan-Dark-Patterns-5-GEO.-TECH.-REV.-251-2021.pdf.

known as dark patterns. Although this work is still nascent, it may be the closest analog in U.S. law to a right of informational self-determination.

Even in the 2010s and before, the FTC noted that a lack of understanding often undermined informed consent on the part of users.[16] The commission has often sought enforcement using its section 5 authority against companies that use deceptive practices to charge hidden fees or obscure their data collection practices, such as in the Effen Ads and Vizio consent decrees.[17] However it is only recently in 2021 that the FTC announced increased enforcement against dark patterns as a formal policy.[18] While this stronger regulatory stance is welcome news, the erosion of the consent model has been occurring for over two decades and the commission has not been able to stop it, in large part because it lacks statutory authority to do so.

The CPRA seeks to impose a more robust consent requirement and to directly address dark patterns. The new enforcement agency under the state attorney general, called the California Privacy Protection Agency (CPPA) has proposed rules that clarify and elaborate on the consent requirements, among other issues in the CPRA. It states that consent must be "freely given, specific, informed, and unambiguous indication of the consumer's wishes," and cannot make use of dark patterns.[19] It also authorizes additional regulations to address the use of dark patterns when obtaining consent.[20] A draft proposal for the regulations would require that consent be 1) easy to understand, 2) reflect symmetry of choice (it isn't harder to say 'no' than 'yes'), 3) avoid confusing language or interactive elements, 4) avoid manipulative language or architecture, and 5) be easy to execute.[21] All other consent mechanisms would be considered a dark pattern.

A separate but somewhat related effort are proposals to introduce a duty of loyalty into American privacy law. A duty of loyalty is an academic concept that would require companies to act in the best interest of users when they collect and process user data.[22] For example, a website that collects user information would be obliged to use that data in the user's best interest because the user has entrusted their data to the website. In addition, some activities like selling the data to a third party would constitute per se disloyal conduct. The duty of loyalty is still a novel theory, but it has made its way into some legislative proposals.[23] This works represents the cutting edge of privacy theory and is an attempt to rectify the

---

[16] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change", https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

[17] Effen Ads, LLC (iCloudWork) https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3202-effen-ads-llc-icloudworx. Vizio Inc. and Vizio Inscape Services, LLC https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3024-vizio-inc-vizio-inscape-services-llc.

[18] FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions, https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions

[19] California Civil Code 1798.140 (h)

[20] California Civil Code 1798.185 (a)(20)(C)

[21] California Privacy Protection Agency, Text of Proposed Regulations, Section 2004. https://cppa.ca.gov/meetings/materials/20220608_item3.pdf

[22] Neil M. Richards, Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 Wash. U. L. Rev. 961 (2021). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217

[23] See the Data Care Act of 2021 https://www.congress.gov/bill/117th-congress/senate-bill/919. Massachusetts also had a proposal for a privacy law built around a duty of loyalty. https://malegislature.gov/Bills/192/HD2664.

failures of a consent-based regulatory model with little to no further consideration for how consumers actually interact with consent notices in practice.

2.1 Enforcement

As mentioned above, the FTC is the primary enforcer of general consumer privacy, with specific agencies responsible for the sectoral privacy laws under their purview. The FTC's main enforcement tool is called a consent decree, which is akin to an administrative law version of a guilty plea in U.S. criminal. In a consent decree, the FTC will impose various conditions on the company's business practices for a set duration of time, for instance that they refrain from collecting or processing data in a certain way. The company typically does not admit guilt or liability in these agreements, but if the FTC finds that they violated the consent decree it can levee additional fines and even extend the length of the agreement. Prior to the consent decree the commission may engage in informal investigations and consultation with the company, filing a formal complaint if there is sufficient evidence of wrongdoing. The overwhelming majority of complaints are settled, resulting in a consent decree.[24]

At the state level, enforcement of the regulations promulgated by the CPPA was set to begin on July 1st, 2023, but a recent court decision has delayed that date until March 29, 2024. However, the office of the attorney general (OAG) has been enforcing the older provisions of the CCPA and CPRA that are already in effect.[25] Enforcement by the OAG operate in a similar way to the FTC, with most complaints resolved in a settlement called a stipulated agreement. There have been some cases of cities or localities engaging in their own privacy lawmaking and enforcement,[26] but those efforts are beyond the scope of this report.

2.2 Judicial Proceedings

As stated above, judicial rulings resulting from government privacy enforcement are rare. Private litigation related to privacy is also uncommon but does occur. Although there are several federal privacy laws, they do not all allow for a private right of action.[27] Even where the laws allow for private suit there will be more nuance than can fit in the allotted space here,[28] so this report will address general issues. One of the major obstacles in these kinds of lawsuits is that the terms of service for many web services and platforms will often prohibit litigation in favor of private arbitration. This not only inhibits individual lawsuits but class action suits as well. In addition, damages in privacy cases can be quite difficult to prove outside of situations like data breaches where individuals suffer identity theft or other pecuniary losses.

Lawsuits at the state level are even more complex, given that every state and territory has its own rules of civil procedure and body of common law. In addition, at the time of writing, nine states have pass their own comprehensive consumer privacy laws, with different approaches to private lawsuits. The common law privacy torts first enumerated by Samuel Warrant and Louis Brandeis in 1890[29] are widely recognized in state laws, but these claims can be difficult to win and not generally regarded as effective measures for protecting privacy in the digital age. The CCPA/CPRA creates a private right of action along with

---

[24] Daniel J. Solove, Woodrow Hartog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 610 (2014). https://cyberlaw.stanford.edu/sites/default/files/SSRN-id2312913.pdf.
[25] The OAG maintains separate lists of CCPA enforcement actions (https://oag.ca.gov/privacy/ccpa/enforcement) and privacy enforcement actions more broadly (https://oag.ca.gov/privacy/privacy-enforcement-actions).
[26] Ira Rubinstein, *Privacy Localism*, 93 Wash. L. Rev. 1961 (2018).
[27] One of the "strongest" federal privacy laws HIPAA, does not offer a private right of action for violations.
[28] To give just one example, some federal lawsuits raise a cause of action under the wiretap act and stored communications act, which normally address government spying and access to data.
[29] Samuel D. Warren, Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

statutory damages for data security breaches,[30] but not for any other provision in the law. Enforcement is left to the OAG. Other California privacy laws do allow for private lawsuits, such as the state's health records privacy law.

※This work was supported by JST [Moonshot R&D][Grant Number JPMJMS2293]

[30] California Civil Code 1798.150