

THOMAS HOEREN / TOSHIHIRO WADA

Datenschutz in Japan

Aktuelle Entwicklungen bei der globalen Datennutzung und -übermittlung

Angemessenheit
Datentransfer
Privatsphäre
DS-GVO

■ Japan ist auf dem Weg zu globalem Datenschutz. In Deutschland ist wenig bekannt, wie das Datenschutzrecht in Japan funktioniert, obwohl die japanische Industrie vielfältige Kontakte zu Deutschland hat. Die Autoren beschreiben daher in ihrem Beitrag, wie man in Japan mit der Philosophie des Datenschutzes umgeht, welche Konstellationen eine besondere Sensibilität im Datenschutzrecht aufweisen und wie man sich an die neuen europäischen Standards im Datenschutzrecht anpasst.

■ Japan is on its way to global data protection. Not much is known in Germany about how data protection law works in Japan even though the Japanese industry has many contacts to Germany. Therefore, in their article the authors will describe Japan's way of dealing with the philosophy of data protection, which constellations demonstrate a particular sensitivity to data protection law and how they are adjusting to the new European standards in data protection law.

Lesedauer: 12 Minuten

I. Einleitung

Das japanische Datenschutzrecht beruht auf dem Act on the Protection of Personal Information (im Folgenden: APPI), welcher am 23.5.2003 verabschiedet wurde und am 1.4.2005 vollständig in Kraft getreten ist.¹ Im September 2015 wurde der APPI inhaltlich grundlegend überarbeitet und ist nun seit dem 30.5.2017 in seiner neuen Form in Kraft.² Hauptgründe für die Anpassung waren zuvor bestehende Unklarheiten in Bezug auf die vielen verschiedenen modernen Datenformate sowie vor allem die Notwendigkeit, die gesetzlichen Regelungen konkreter auf den Trend der Globalisierung abzustimmen.³

Die zunehmende Unternehmenstätigkeit auf internationaler Ebene führt folglich auch zu einer globalen Datenübermittlung und -nutzung. Dementsprechend ist es nötig, dass das japanische mit dem ausländischen Datenschutzrecht in Einklang gebracht wird. Dieser Aufsatz möchte die Situation des Datenschutzes in Japan allgemein skizzieren und anschließend einen Überblick über den APPI und seine Regelungen geben.

II. Der Umgang mit Datenschutz in Japan und die Mentalität der Japaner

1. Datenschutzbewusstsein

Die japanische Regierung nahm im Oktober 2015 eine Umfrage in Bezug auf die o.g. Veränderung des APPI vor. Dabei ergab sich, dass 26,0% der 1.736 Befragten den Inhalt der Veränderung des APPI verstehen, während 39,8% der Befragten nur

über die Vornahme einer Veränderung informiert sind.⁴ Grundlegend ließ sich feststellen, dass mehr als die Hälfte der Befragten einen sorgfältigen Umgang mit Informationen über Einkommen oder Kredit, Krankheit oder Vorstrafe für wichtig erachten.⁵

2. Sensibilität

a) Übermäßig sensible Reaktion

In Japan gibt es seit langem schon die Tendenz, den Umgang mit Daten sehr sensibel zu betrachten und die Weitergabe personenbezogener Daten zu vermeiden. Dies führt konsequenterweise zu sehr eingeschränkten Nutzungsmöglichkeiten eben solcher Daten. Welche Auswirkungen dies auf den Alltag haben kann, zeigen folgende Beispiele:

■ Kurz nach dem Inkrafttreten des APPI im Jahre 2005 verunglückte ein Zug. Ein Teil der Krankenhäuser verweigerte die Weitergabe von Informationen über die Opfer, und zwar nicht nur gegenüber den Rettungskräften, sondern auch gegenüber den Opferfamilien.

■ Als Lehrer eine Liste aller Klassenmitglieder in einer Schule erstellen wollten, lehnten manche Eltern dies ab.

■ Bei einer Naturkatastrophe ist es aus Rücksichtnahme auf die trauernden Opferfamilien wichtig, dass die Kommunalregierungen die Namen von Opfern oder Vermissten nicht bekannt machen und auch im Nachhinein auf Diskretion achten.

Der Grund für diesen übermäßig sensiblen Umgang ist, dass der Zweck des APPI nicht richtig verstanden worden ist. Es ist das Ziel der Regierung, der Ministerien, der Kommunalregierungen und des *National Consumer Affairs Center of Japan*, dass die Regelungen des APPI besser verstanden werden.

b) Datenabfluss

Datenabfluss existiert sowohl bei öffentlichen als auch bei nicht-öffentlichen Stellen in Japan. Bisherige Datenabflussfälle wurden z.B. wegen Angriffen durch Virus-E-Mails, der Mitnahme von Daten durch interne Personen auf Seiten des Datenverarbeitenden oder auch der falschen technischen Einstellung aus Versehen herbeigeführt. Nun haben viele Japaner Bedenken, ob die verlorenen Daten sichergestellt wurden und wie diese jetzt behandelt bzw. verwertet werden.

¹ Gesetz Nr. 57/2003; alle Gesetzesangaben entsprechen dem japanischen Originaltext.

² Die englische Übersetzung des APPI ist abrufbar unter: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

³ Zu Gründen der Veränderung *IT Strategic Headquarters*, Pāsonaru dēta no rikatsuyō ni kansuru seido kaisei taikō [Grundsatz der Systemveränderung in Bezug auf die Verwendung von persönlichen Daten], S. 5 ff., abrufbar unter: http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryō2.pdf.

⁴ *Cabinet Office, Government of Japan*, „Kojin jōhō hogo hō no kaisei ni kansuru seron chōsa“ no gaiyō [Übersicht der „Meinungsforschung über die Veränderung des APPI“], S. 3 ff., abrufbar unter: <http://survey.gov-online.go.jp/tokubetu/h27/h27-kojing.pdf>.

⁵ *Cabinet Office, Government of Japan* (o. Fußn. 4), S. 15 ff.

3. Zusammenfassung

Japaner haben großes Interesse am Datenschutz. Datenabfluss ist ein ernstes Problem in Japan und die Japaner sind vorsichtig im Umgang mit Daten. Allerdings gibt es auch grundlegende Missverständnisse über den Sinn und Zweck der existierenden rechtlichen Regelungen des APPI.

III. Japanisches Datenschutzrecht APPI

1. Anwendungsbereich des APPI

Die Vorschriften des ersten bis dritten Kapitels des APPI sind sowohl auf den öffentlichen als auch auf den privaten Sektor anwendbar. Die Vorschriften des vierten bis siebten Kapitels des APPI finden nur auf den privaten Sektor Anwendung. Art. 76 Abs. 1 Nr. 1-5 APPI regelt die Ausnahme der Anwendung des vierten Kapitels.

Ein Teil der Vorschriften des APPI verweist auf die Vorschriften des Cabinet Order to Enforce the Act on the Protection of Personal Information (im Folgenden: COE-APPI) und die der Enforcement Rules for the Act on the Protection of Personal Information (im Folgenden: ER-APPI).⁶ Beide Regelwerke beinhalten ausführliche oder konkrete Fälle und weitere Rechtsverweisungen in vielfältigen Bereichen.

2. Grundlage des APPI

a) Zweck des APPI

Gem. Art. 1 APPI liegt der Hauptzweck des APPI darin, auf der einen Seite die Rechte und Interessen Einzelner zu schützen und auf der anderen Seite die Nützlichkeit persönlicher Informationen zu berücksichtigen. Die Nützlichkeit von Daten, vor allem Big Data, spielt eine wichtige Rolle in der Digital- und Wirtschaftspolitik in Japan.⁷ Die Analyse und Nutzung von Big Data anhand neuer Technologien oder Services wie IoT, Roboter oder Sharing Economy durch Internetplattformen können die vorhandene Industrie und das Wirtschaftswachstum erheblich unterstützen.

Der APPI enthält Vorschriften über die Pflichten aller Datenverarbeitenden, sodass die Rechte und Interessen Einzelner geschützt werden. Wie gezeigt, bezweckt der APPI also nicht nur den Schutz der Privatsphäre an sich. Dennoch wurde seit dem Inkrafttreten des APPI der Schutz der Privatsphäre stärker denn je hervorgehoben. Ferner kommt noch hinzu, dass, wenn gegen die Regeln des APPI und damit gegen den Schutz der Privatsphäre verstoßen wurde, ex post auch noch das Deliktsrecht als regulierendes Instrument in Betracht kommt.

b) Legaldefinitionen

Es gibt ähnlich gelagerte fundamentale Begriffe in Bezug auf Daten im APPI, nämlich „persönliche Information“ (Art. 2 Abs. 1 APPI), „persönliche Daten“ (Art. 2 Abs. 6 APPI) und „gespeicherte persönliche Daten“ (Art. 2 Abs. 7 APPI).

Der Begriff „persönliche Information“ umfasst Informationen in Bezug auf lebende Individuen (Art. 2 Abs. 1 APPI). Im Kern geht es dabei um Name und Geburtsdatum (Art. 2 Abs. 1 Nr. 1 APPI), die die Grundelemente sind, um einen ganz bestimmten Betroffenen zu identifizieren. Durch die Veränderung im Jahre 2015 wurde ferner der Begriff des Identifikationsmerkmals hinzugefügt und definiert (Art. 2 Abs. 1 Nr. 2, Art. 2 Abs. 2 Nr. 1 und 2 APPI). Zu ihm gehören z.B. die körperliche, genetische oder biometrische Charakteristik sowie Reisepass- und Rentennummer (Art. 2 Abs. 2 Nr. 1 und 2 APPI i.V.m. Art. 1 COE-APPI). Mit dem neu definierten Identifikationsmerkmal kann man Betroffene genauer identifizieren.

Außerdem wurde der Begriff der sensiblen Daten (Art. 2 Abs. 3 APPI) novelliert. Die Erhebung von sensiblen Daten ist gem.

Art. 17 Abs. 2 APPI durch die Einholung der Einwilligung der Betroffenen zulässig. Die Ausnahmefälle sind in Art. 17 Abs. 2 Nr. 1-6 APPI geregelt. Sensible Daten können nicht durch Opt-out an Dritte in Japan übermittelt werden (Art. 23 Abs. 2 APPI).

Auch der Begriff „anonymisierte Daten“ (Art. 2 Abs. 9 APPI) wurde durch die Veränderung eingefügt. Durch die Verarbeitung von persönlichen Informationen werden anonymisierte Daten geschaffen und bestimmte Personen können nicht mehr identifiziert werden. Diese Neuerung fördert die Nutzung von Big Data.

Betroffener ist die bestimmte Person, die durch die persönliche Information identifiziert wird (Art. 2 Abs. 8 APPI). Der APPI enthält zwei Arten des Datenverarbeitenden. Der eine ist der Datenverarbeitende, der die persönliche Information behandelt (Art. 2 Abs. 5 Satz 1 APPI), der andere ist der, der mit anonymisierten Daten arbeitet (Art. 2 Abs. 10 Satz 1 APPI). Die staatlichen Organe, die Kommunalregierungen und die *Incorporated Administrative Agency* gehören nicht zu den Datenverarbeitenden (Art. 2 Abs. 5 Satz 2, Abs. 10 Satz 2 i.V.m. Art. 2 Abs. 5 Satz 2 Nr. 1-4 APPI).

c) Pflichten des Datenverarbeitenden

Das vierte Kapitel des APPI statuiert die Pflichten des Datenverarbeitenden. Im ersten Abschnitt geht es um den Umgang mit der persönlichen Information (Art. 15-35 APPI). Der zweite Abschnitt enthält Vorschriften in Bezug auf die Schaffung und Behandlung anonymisierter Daten (Art. 36-39 APPI).

d) Ausschuss Personal Information Protection Commission

Der Ausschuss *Personal Information Protection Commission* (PPC) entspricht einer unabhängigen Datenschutzbehörde. Der PPC dient gem. Art. 60 APPI der Wahrung eines angemessenen Umgangs mit der persönlichen Information.

Die konkreten Aufgaben des PPC sind in Art. 61 APPI geregelt. Der PPC entwirft die Grundleitlinien (Art. 61 Nr. 1 APPI) und spielt als Aufsichtsorgan des Datenverarbeitenden eine wichtige Rolle (Art. 61 Nr. 2 APPI). Zur Verbesserung des Umgangs mit persönlichen Informationen oder anonymisierten Daten durch den Datenverarbeitenden ergreift der PPC stufenweise Maßnahmen zum Schutz des Umgangs mit persönlichen Daten.⁸

IV. Datenschutzproblematik zwischen Japan und Deutschland

1. Zusammenarbeit des PPC mit der EU-Kommission

Der PPC und die *EU-Kommission* streben eine Erleichterung der beiderseitigen Datenübermittlung an. Im Januar 2017 fasste die *EU-Kommission* die Vorstellung in einem Papier („adequacy decisions“) zusammen und erklärte die aktive Kooperation mit Japan als einem der Handelsverkehrspartner.⁹ Japan ist noch nicht als Drittland i.S.d. Art. 25 Abs. 1 RL 95/46/EG (DS-RL) qualifiziert, in dem ein angemessenes Datenschutzniveau gewährleistet ist. Seit dieser Erklärung finden Treffen zwischen Japan und

⁶ Cabinet Order Nr. 507/2003; die englische Übersetzung des COE-APPI ist abrufbar unter: https://www.ppc.go.jp/files/pdf/Cabinet_Order.pdf. Die englische Übersetzung der ER-APPI ist abrufbar unter: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf.

⁷ Zu der Digitalpolitik in Japan *IT Strategic Headquarters*, Sekai saisentan IT kokka sōzō sengen, kanmin dēta katsuyō suishin kihon keikaku [Erklärung der Erschaffung des IT-Weltspitzenstaats und Grundplan zur Beschleunigung der Datennutzung durch den öffentlichen und den nicht-öffentlichen Sektor], abrufbar unter: <http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20170530/siryu1.pdf>.

⁸ S. hierzu Art. 40-43 APPI.

⁹ *European Commission*, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017) 7 final, Stand: 10.1.2017, S. 6 ff., abrufbar unter: <http://eu-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN>.

der *EU-Kommission* sowie den EU-Mitgliedstaaten statt.¹⁰ Am 20.3.2017 nahm nicht nur eine Delegation des *PPC*, sondern auch der *japanische Minister für Economy, Trade and Industry* am Gespräch mit den Mitgliedern der *EU-Kommission* in Hannover teil.¹¹ In dem Gespräch v. 3.7.2017 in Brüssel wurde festgestellt, dass die Rechtssysteme in Bezug auf Privatsphäre zwischen den EU-Mitgliedstaaten und Japan gut harmonisieren.¹² Am 6.7.2017 fand das Gipfeltreffen zwischen der EU und Japan in Brüssel statt.¹³ Der Präsident der Europäischen Kommission, *Jean-Claude Juncker*, und der japanische Premierminister, *Shinzō Abe*, gaben eine gemeinsame Erklärung zur künftigen Zusammenarbeit ab.¹⁴

2. Datenübermittlung von Japan an Deutschland

Der Datenverarbeitende kann gem. Art. 24 Satz 1 APPI nach Einholung der Einwilligung der Betroffenen die persönlichen Daten von Japan an Dritte im Ausland übermitteln.¹⁵ Ausland i.S.d. Art. 24 Satz 1 APPI ist ein Staat oder ein Gebiet, das nicht zu Ja-

10 Zum Besuch der japanischen Delegation in Deutschland vgl. PM der *BfDI* v. 9.3.2017, abrufbar unter: https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/Japanische_Delegation_2017.html?cms_templateQueryString=japan&cms_sortOrder=score+desc.

11 *PPC*, Press statement v. 20.3.2017, abrufbar unter: https://www.ppc.go.jp/files/pdf/290320_statement.pdf.

12 *PPC*, Press statement v. 3.7.2017, abrufbar unter: https://www.ppc.go.jp/files/pdf/290704_pressstatement.pdf.

13 *Europäische Kommission*, Wirtschaftspartnerschaftsabkommen EU-Japan, v. 6.7.2017, abrufbar unter: https://ec.europa.eu/commission/news/eu-japan-economic-partnership-agreement-2017-jul-06_de.

14 *European Commission*, Joint Declaration by Mr. Shinzo Abe, Prime Minister of Japan, and Mr. Jean-Claude Juncker, President of the European Commission, v. 6.7.2017, abrufbar unter: http://europa.eu/rapid/press-release_STATEMENT-17-1917_en.htm.

15 S.a. *Schiebel/Kirchhoff*, Der internationale Transfer von Kunden- und Mitarbeiterdaten, *JAPANMARKT* 2017, Nr. 2, S. 36.

16 *PPC*, Kojin jūhū no hogo ni kansuru hūritsu ni tsuite no gaidorain (Gaikoku ni aru daisansha e no teikyū hen) [Richtlinien über APPI (Über die Datenübermittlung an Dritte im Ausland)], S. 5, abrufbar unter: <https://www.ppc.go.jp/files/pdf/guidelines02.pdf>.

17 *PPC* (o. Fußn. 16), S. 2 ff.

18 *PPC*, Kojin jūhū hogo hū dai 24 jū ni kakawaru iinkai kisoku no hūkūsei ni tsuite [Über die Richtung der ER-APPI in Bezug auf Art. 24 APPI], abrufbar unter: https://www.ppc.go.jp/files/pdf/290616_siryō1.pdf.

19 *PPC*, Nichi EU kan no sūgo no enkatsuna kojīn deta iten ni tsuite [Über die erleichterte beiderseitige Datenübermittlung zwischen Japan und EU], abrufbar unter: https://www.ppc.go.jp/files/pdf/290704_enkatsuiten.pdf.

pan gehört. Dritter i.S.d. Art. 24 Satz 1 APPI ist derjenige, der weder Datenverarbeitender noch durch die betroffenen persönlichen Daten identifizierter Betroffener ist. Auch ausländische Regierungen werden in den Begriff des Dritten einbezogen.¹⁶ Wenn die Muttergesellschaft in Deutschland als Empfängerin und die Tochtergesellschaft in Japan als Veräußerin nicht derselbe Rechtsträger sind, ist Erstere Dritte i.S.d. Art. 24 Satz 1 APPI.

Ausnahmsweise erfolgt die grenzüberschreitende Übermittlung persönlicher Daten, ohne dass der Betroffene in deren Weitergabe an Dritte im Ausland einwilligt.¹⁷ Der *PPC* kann gem. Art. 24 Satz 1 APPI anerkennen, dass das Datenschutzniveau des Empfängerlands dem japanischen entspricht. Bislang ist noch kein Land durch den *PPC* qualifiziert. Eine weitere Möglichkeit ist, dass die Voraussetzung gem. Art. 24 Satz 1 APPI i.V.m. Art. 11 Nr. 1 oder Nr. 2 ER-APPI erfüllt wird. Dadurch wird der Empfänger nicht als Dritter i.S.d. Art. 24 Satz 1 APPI angesehen. Infolgedessen sind auf diese zwei Fälle Art. 23 Abs. 2 APPI und Art. 23 Abs. 5 APPI anwendbar. Außerdem verweist Art. 24 Satz 1 APPI auf Art. 23 Abs. 1 Nr. 1-4 APPI und die Ausnahmefälle sind damit ebenso wie beim inländischen Datentransfer gültig.

V. Ausblick

Der *PPC* wird im Laufe der ersten Hälfte des Jahres 2018 Kriterien zur Anerkennung gem. Art. 24 Satz 1 APPI in die ER-APPI einfügen, während die *EU-Kommission* an „adequacy decisions“ für Japan arbeitet.¹⁸ Der *PPC* plant die Anerkennung der EU-Mitgliedstaaten zur Erleichterung des Datentransfers zwischen Japan und der EU.¹⁹



Prof. Dr. Thomas Hoeren

ist Direktor der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) an der Westfälischen Wilhelms-Universität Münster und Mitherausgeber der ZD.



Toshihiro Wada

ist Absolvent der Aoyama Gakuin Universität Tokio (M.A.) und wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht (ITM) an der Westfälischen Wilhelms-Universität Münster.

BARBARA SCHMITZ

Der Abschied vom Personenbezug

Warum der Personenbezug nach der DS-GVO nicht mehr zeitgemäß ist

Risikobasierter Ansatz
Personenbezogene Daten
IP-Adresse
Big Data

■ Der Personenbezug ist derzeit das zentrale Element im Datenschutz. Ist ein Personenbezug nicht vorhanden, greifen die Regelungen des Datenschutzrechts nicht. Soll jedoch auch im Zeitalter von Internet of Things (IoT) und Big Data ein Betroffenschutz funktionieren, sollten wir uns von dem lieb gewordenen Personenbezug verabschieden. Der nachfolgende Beitrag zeigt auf, warum der Personenbezug im Datenschutzrecht ausgedient hat, und will zur Diskussion über neue Konzepte und Betrachtungen anregen.

Lesedauer: 16 Minuten

■ Personal reference is currently the central element in data protection. If a personal reference is not present then the provisions of data protection law do not apply. However, if in the age of Internet of Things (IoT) and Big Data a protection for affected persons should work then we will have to say goodbye to the much loved personal reference. The following article will show why personal reference in data protection is no longer needed and wants to stimulate a discussion on new concepts and viewpoints.

I. Der Personenbezug

Das wesentliche Element des deutschen, europäischen und internationalen Datenschutzrechts ist der Personenbezug. Er stellt das Eintrittstor für die Anwendung der Regelungen des Daten-

schutzrechts dar. Liegt ein Personenbezug vor, gelten die Regelungen des Datenschutzrechts umfassend. Die Folgen daraus sind hingegen unterschiedlich. Während im europäischen Raum die Anwendung des Datenschutzrechts zur Folge hat, dass das