Das japanische Datenschutzgesetz – das Recht zum Schutz von persönlichen Daten*

Bernd GÖTZE**

I. EINFÜHRUNG

Seit 2017 hat Japan ein zentrales Gesetz im engeren Sinn eines nationalen Datenschutzgesetzes. Dieses erfasst, konzentriert auf ein einziges Gesetz, den Problemkreis vom Schutz persönlicher Daten. Der Name des Gesetzes lautet übertragen „Gesetz betreffend den Schutz persönlicher Information[en]“[1]. Nachfolgend soll hier die Abkürzung GSpI benutzt werden. Dieses Gesetz stellt eine den Anwendungsbereich des ersten japanischen Da-

---

* Diese Ausführungen stellen in konzentrierter Gestalt formell wie inhaltlich eine auf die Form dieser Zeitschrift gebrachte Abhandlung des neu aufgenommenen Kapitels „Datenschutz“ in dem „Handbuch Japanisches Handels- und Wirtschaftsrecht“ dar; dort § 23 der in Vorbereitung begriffenen 2. Auflage (Herausgeber H. Baum/M. Bälz/M. Dernauer/G. Koziol).

** Dr. jur., Wirtschaftsanwalt in Singapur, Luther LLP (Singapur-Büro der Luther Rechtsanwaltsgesellschaft).

1 Das 個人情報の保護に関する法律 *Kojin jōhō no hogo ni kansuru hōritsu*, Gesetz Nr. 57/2003. Zitierte Artikel ohne Gesetzesangabe sind solche des GSpI. Zur Wahl des japanischen Gesetzgebers des Terminus „Informationen“ (und nicht „Daten“) nachfolgend unter II.1.c).

tenschutzgesetzes aus dem Jahr 2003 extrem erweiternde Neufassung dar.[2] Abgesehen von der Tatsache, dass international das Thema Datenschutz zunehmend an Bedeutung gewonnen hatte und während jener Periode viele Staaten gesetzliche Grundlagen für einen besseren Schutz vor Verletzungen (insbesondere der ungefragten Weitergabe oder des Verkaufs solcher) persönlicher Daten eingeführt hatten, lag der Grund für eine weitgehende Gesetzesänderung insbesondere in der hohen Schwelle, die nach dem Gesetz von 2003 erreicht sein musste, auf dass gegenüber potenziellen Verletzern staatliche Maßnahmen überhaupt angeordnet oder Sanktionen angedroht oder ausgesprochen werden konnten. Der vorliegende Beitrag stellt die Situation *de lege lata* nach der ersten großen Anpassung[3] des GSpI 2020 dar. Diese ist weitenteils seit Juni 2022 in Kraft.

Es war jedoch nicht allein die globale Tendenz zu einem vermehrten rechtlichen Schutz bei Verletzungen persönlicher Daten, welche zu der Revision führte. Auch der Ruf nach einem effektiveren Datenschutz aus der japanischen Bevölkerung und seitens der Verbraucherverbände hat dazu beigetragen. Offenbar gewordene negative Auswirkungen der Nutzung der im Netz – und später auf allen Kanälen sozialer Medien – leicht zugänglichen Daten zu Vermarktungszwecken waren Gegenstand fast täglicher kritischer Medienberichterstattung. Sodann zwangen die verstärkte Nutzung durch die Wirtschaft als Marktteilnehmer von aus dem Internet ‚gemolkenen' Daten[4] und das Aufkommen von *Big Data* den Gesetzgeber zu gesetzgeberischer Aktivität. Mindestens ebenso wichtig war indes, dass bedeutende Handelspartner wie Deutschland, bzw. natürlich die gesamte Eurozone, ein striktes Datenschutzregime eingeführt hatten. Japan erkannte die Vorteile, rasch eine „Angemessenheit" im Sinne der europäischen DSGVO[5] zu erreichen. Im Ergebnis wurde der Angemessenheitsbeschluss[6] im Januar 2019 durch die EU-Kommission gefällt und trat umgehend[7] in Kraft. Wichtig ist hervorzuheben, dass wegen der aus Sicht der EU noch vorhandenen Schwächen des GSpI von 2017 (welches zu jener Zeit die Grundlage für die

2 In Kraft getreten im Jahr 2005.

3 Hervorgebracht durch ein Änderungsgesetz, das 個人情報の保護に関する法律等の一部を改正する法律 *Kojin jōhō no hogo ni kansuru hōritsu-tō no ichibu o kaisei suru hōritsu*: Gesetz zur teilweisen Änderung des Gesetzes und anderer gesetzlicher Regelungen betreffend den Schutz persönlicher Information, Gesetz Nr. 44/2021.

4 Durch extensives sog. *data fishing*.

5 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

6 Die *Adequacy Decision*, 相互十分性の認定 *sōgo jūbun-sei no nintei*, vom 23. Januar 2019.

7 Nämlich schon am nächsten Tag, den 24. Januar 2019.

Verhandlungen mit der EU bildete) ein Zusatzkatalog von separat ausgehandelten Sonderanforderungen notwendig war. Das deshalb, weil der Schutzumfang des Gesetzes aus EU-Sicht als noch nicht ausreichend angesehen worden war.[8] Mit dem nunmehr seit Mitte 2022 geltenden GSpI hat sich dieser Problemkreis zum größeren Teil, indes noch nicht vollständig, erledigt. Was dazu geführt hat, dass das Thema Datenschutz im Wirtschaftsverkehr mit Japan aus deutscher Sicht allenfalls einen Bruchteil der Aufmerksamkeit verdient, wie sie etwa gegenüber Staaten besteht, denen die DSGVO-Angemessenheit nicht bescheinigt ist.[9]

Im Zusammenhang mit der für Japan vergleichbar kurzen Zeitspanne von nur etwa fünf Jahren vom ersten Entwurf bis zu der im Jahr 2017 erfolgten Revision des GSpI hin zu dessen geltender Fassung 2020 erscheint folgendes Detail erwähnenswert: Es war zwar nicht der Gesetzgeber, aber die gemäß jenem Gesetz gegründete nationale Datenschutzkommission[10] (nachfolgend: DSK), welche klar einer Vorgabe aus einem Kommissionsbericht aus dem Jahr 2019[11] folgte. Dieser Bericht sprach von dem Ziel, dass die revidierte Fassung des GSpI regelmäßig in Hinblick auf notwendig werdende Anpassungen zu untersuchen sei und die DSK dem Gesetzgeber dazu ausgearbeitete und begründete Vorschläge zu Änderungen unterbreiten werde – wobei in dem Bericht die Zeitspanne von fünf Jahren ausdrücklich angesprochen war. Durch ein Änderungsgesetz im Jahr 2015 war die Zeitspanne sogar auf drei Jahre verkürzt worden. Diese Überprüfungen wurden auch vorgenommen. Schon jetzt ist vorstellbar, dass im Zuge der sich auch in Japan spürbar ausbreitenden Entwicklung hin zu einer Sharing Economy – und dem damit notwendig einhergehenden noch weiter verflochtenen Austausch von persönlichen Daten – sich die Notwendigkeit zu einer baldigen erneuten Gesetzesanpassung ergeben wird.

---

8 So z. B. die fehlende Kategorie „pseudonymisierte Daten“ und damit die rechtliche Erfassung solcher; aber auch bestehende Lücken im Bereich des rechtlichen Schutzes bei der grenzüberschreitenden Datenversendung und fehlende Regelungen zur exterritorialen Anwendung.

9 Den juristischen Beratungsbedarf sollte man indes trotzdem nicht unterschätzen. Eine Data-Protection-Due-Diligence-Prüfung (etwa im Verhältnis des deutschen Stammhauses zu der japanischen Tochtergesellschaft) durchzuführen ist nicht allein aus japanischer Gesetzessicht, sondern auch vor dem Hintergrund der exorbitanten finanziellen Sanktionen der DSGVO angezeigt.

10 In wortgetreuer Übertragung die „Kommission für den Schutz persönlicher Informationen“, 個人情報保護委員会 *Kojin Jōhō Hogo I'in-kai*; vgl. die offizielle Website *https://www.ppc.go.jp/*.

11 So in einem Dokument mit Rahmenausführungen der Kommission (*https://www.ppc.go.jp/files/pdf/seidokaiseitaiko.pdf*) 個人情報保護法いわゆる三年ごと見直し制度改正大綱 *Kojin jōhō hogo-hō iwayuru sannen-goto minaoshi seido kaisei daimō*.

Den nachfolgenden Darstellungen seien zum besseren Verständnis folgende Punkte vorangestellt: Das Recht auf Schutz von persönlichen oder personenbezogenen Daten wird in Japan nicht als ein grundlegendes, womöglich anderen Rechten übergeordnetes oder überordenbares Recht angesehen. Manche in anderen Rechtsordnungen inzwischen etablierten datenschutzrechtlichen Prinzipien sind aber durch die Literatur und Rechtsprechung im Wege der Auslegung einer bestimmten Verfassungsnorm[12] als ein Ausfluss des Persönlichkeitsrechts anerkannt worden. Entsprechend kann man (aus deutschrechtlicher Sicht) einen grundrechtsähnlichen Status ausschließen. Erst recht ist es nicht als Menschenrecht oder ein menschenrechtsähnliches Recht einordenbar.

Weil oft als Eingangsfrage zum Thema Datenschutz in Japan aufgebracht, sei weiterhin schon hier erwähnt, dass die Ernennung eines (sei es unternehmensinternen oder externen) Datenschutzbeauftragten vom Gesetz nicht explizit gefordert wird, aber in untergesetzlichen Normenkatalogen angesprochen – und nur in ganz begrenzten Wirtschaftsbranchen zur Pflicht erhoben ist.[13]

II. Rechtliche Grundlagen

1. Das Gesetz betreffend den Schutz persönlicher Informationen

Das GSpI war von Beginn an darauf ausgelegt, die einzige nationale Gesetzesgrundlage zum Datenschutz zu sein.[14] So richten sich die Vorschriften dieses Gesetzes an staatliche Stellen ebenso wie an andere Nutzer bzw. potenziell „in den Besitz von Daten gelangende Stellen“. Das hat Auswirkungen auf die Struktur des Gesetzes (dazu unmittelbar nachfolgend). Betrachtet man die rechtlichen Grundlagen zum Datenschutz in Japan indes genauer, so muss schon hier darauf hingewiesen werden, dass der Regelungskatalog tatsächlich viel breiter angelegt und umfangreicher ausgestaltet ist, als es der Umfang des GSpI auf den ersten Blick vermuten lässt. Basierend auf dem und in Ergänzung zu dem GSpI hat die DSK nämlich einige Verwaltungsrichtlinien[15], 規則 *kisoku*, und eine ganze Anzahl von erläuternden

12 Art. 13 der japanischen Verfassung, wonach jeder Bürger als eine Einzelpersönlichkeit geachtet werden soll: 個人として尊重される (*kojin toshite sonchō sareru*).

13 Wobei in der wirtschaftlichen Praxis aber schon seit geraumer Zeit selbst nur mittelgroße Unternehmen, die dieser Verpflichtung an sich nicht unterfallen, allein aus Beweisgründen und als Nachweis einer guten Unternehmensführung (*compliance criteria*) solche Beauftragte für Datenschutzfragen ernannt haben.

14 So schon 2014 in einem Papier eines auf Kabinettsebene angesiedelten „Büros zur Festlegung einer IT-Gesamtstrategie“, welches eine Blaupause für geplante gesetzgeberische Maßnahmen zum Schutz von persönlichen Daten zu erstellen hatte.

(sog.) Leitlinien, ガイドライン *gaidorain* (*guidelines*), für die Praxis erlassen. Insbesondere Letztere richten sich an Verwender und dienen der Erläuterung der gesetzlichen Vorschrift. Denn sehr viele der Normen des GSpI verweisen im Zusammenhang mit Verwenderpflichten wegen Einzelheiten durch einen eingeschobenen Nebensatz auf die in Leitlinien der DSK enthaltenen Einzelregelungen. Was dann in etwa formuliert ist als 個人情報保護委員会規則で定めるところにより… *kojin jōhō hogo i'in-kai kisoku de sadameru tokoro ni yori* ..., d.h. „wie in den von der Datenschutzkommission herausgegebenen Leitlinien [weiter] festgelegt [ist]". Auf diese Verwaltungsrichtlinien – insbesondere aber die von der DSK erlassenen Leitlinien – wird nachfolgend unter II.2. und II.3. einzugehen sein.

Auch hier sei als Bemerkung vorangestellt: Der Kreis der zum Schutz von Daten verpflichteten Personen wird im privatrechtlichen Bereich durch eine wichtige Definition eingeschränkt: Geschützt sind nur der Umgang und die Nutzung (i.w.S.) von Daten im geschäftlichen Bereich, vgl. nachstehend II.1.c). Im privaten Bereich werden Datensubjekte nicht zum Schutzsubjekt der rechtlichen Normen des GSpI. Und Datenanwender, -nutzer oder -verwender werden auch nicht potenziell zum Adressaten anordnender oder maßregelnder Verwaltungsakte einerseits – oder, was Strafbestimmungen angeht, nicht zum Schädiger bzw. Rechtsverletzer andererseits.

a) Die Struktur des Gesetzes

Im Katalog der Eingangsbestimmungen in Kapitel I enthalten ist als Art. 1 eine generelle Zielbestimmungsklausel. In Art. 2 finden sich zehn recht umfassend definierte Begriffsbestimmungen und Art. 3 schließt mit einer grundsätzlichen „Visionsklausel" zum Schutz persönlicher Daten.[16]

Insgesamt teilt sich das Gesetz in sieben Kapitel, wovon für die Praxis der Verwender neben den Definitionen in Art. 2 Abs. 2 insbesondere Art. 7[17] sowie das gesamte Kapitel IV, Abschnitt 1 (Artt. 15 bis 35) von Bedeutung sind. Abschnitt 2 desselben Kapitels regelt ähnlich Einzelheiten betreffend die Datenkategorien „anonymisierte Daten" und „pseudonymisierte Daten"[18] (Artt. 36 bis 39 und Artt. 35-2 und 35-3). Die Vorschriften des

15 Die aber nur innerhalb der Verwaltung Geltung entfalten.

16 Art. 3 ist überschrieben mit 基本理念 *kihon rinen*, was man mit „grundsätzliche Vision" oder „Ideale" übertragen kann. Diese lautet in Übersetzung etwa, dass es „in Ansehung des Prinzips der hohen Wertschätzung der Persönlichkeit von Individuen anzustreben ist, mit privaten Informationen mit großer Umsicht zu verfahren". Die Formulierung spricht mit Nennung eines verfassungsrechtlichen Terminus aus, dass der rechtliche Schutz von Daten dem grundsätzlichen Persönlichkeitsrecht der japanischen Verfassung entspringt.

17 In Kapitel III, Abschnitt 1.

Kapitels II betreffen die Zuständigkeiten der Zentral- und Lokalregierungen, auf die in diesem Beitrag nicht eingegangen wird. Kapitel V beschreibt die Einrichtung, die Organisation an sich und die Aufgaben der DSK, Artt. 59 bis 74. Fragen der behördlichen Aufsicht durch die DSK einerseits und durch einige gesondert akkreditierte privatrechtlich organisierte Agenturen andererseits (dazu nachfolgend unter IV.2.) sind in den Artt. 40 bis 46 erfasst. Am Ende stehen die Strafbestimmungen[19] in Kapitel VII (Artt. 82 bis 88).

b) Persönlich-sachlicher Anwendungsbereich

Auf die herkömmlich im Deutschen mit „Datensubjekt" bezeichneten Personen verweist das GSpI nur kurz mit 本人 *honnin*. Auf diese wird hier, weil das ohnehin die treffendste Übersetzung darstellt, durchgehend als „Betroffene/r" verwiesen. Als Betroffene gelten nur lebende natürliche Personen; juristische Personen sind nicht erfasst. Während die DSGVO auf die Adressaten (sprich: Verpflichteten) des Gesetzes differenzierend mit dem Begriffspaar „Verantwortlicher" und „Verarbeiter" verweist, hat sich der japanische Gesetzgeber für eine singuläre Bezeichnung mit dem Begriff „Verwender" entschieden. Das GSpI definiert diese als „mit persönlichen Informationen umgehende Geschäftsleute", 個人情報取扱う事業者 *kojin jōhō toriatsukau jigyō-sha*.[20] Das bedeutet gegenüber dem alten (2017) Gesetz einen stark erweiterten Anwendungsbereich. So werden jetzt, sozusagen „am unteren Ende der Skala", auch alle natürlichen Personen erfasst, die z. B. kleingewerblich oder überhaupt irgendwie geringfügig geschäftsmäßig handeln. Wegen des Wegfalls einer früher bestehenden Beschränkung in der Mindestbeschäftigtenzahl bzw. der Anzahl von Datensubjekten oder Zahl von vorgehaltenen Datensätzen unterfallen nunmehr auch kleine Unternehmen und Kleinstbetriebe den Bestimmungen des Gesetzes. Gefordert ist allein, dass Daten zu einem geschäftlichen Zweck gesammelt, gespeichert, behandelt usw. werden: 業務の用に供して取扱う *gyōmu no yō ni kyōshite toriatsukau*.

Weitgehend ausgenommen von der Anwendung dieses Gesetzes sind Staatsorgane und andere enumerativ aufgezählte öffentliche Stellen,[21] für welche entweder Sondergesetze erlassen oder gesonderte Regelungen ge-

18 Die Kategorie „pseudonymisierte Daten" ist erst im Jahr 2020 durch das Änderungsgesetz (vgl. Fn. 3) als definierte Datenkategorie eingeführt worden und mithin erst seit April 2022 in Kraft.

19 罰則規定 *bassoku kitei*.

20 Das Verb *toriatsukau* (取扱う) aus dieser Definition war maßgeblich für die hier gewählte Benennung als „Verwender".

21 Staatsorgane, 国の機関 *kuni no kikan*, Gebietskörperschaften sowie staatliche und regionale Selbstverwaltungskörperschaften.

schaffen sind.[22] Das GSpI schließt weiterhin den gesamten Pflichtenkatalog aus Kapitel IV – mithin also den wichtigsten Teil betreffend die Verwendern bzw. Verarbeitern von Daten auferlegten Pflichten – im Rahmen jeder in beruflicher Eigenschaft ausgeübten journalistischen, wissenschaftlichen, künstlerischen bzw. literarischen Tätigkeit aus.[23]

c) Begriffsbestimmungen, Kategorien von Daten

Der japanische Gesetzgeber hat sich für den zentralen Terminus technicus des Gesetzes, nämlich den Begriff „Daten" – indes erstaunlicherweise nur teilweise –, für eine andere Wortwahl als die inzwischen weitgehend eingebürgerte Benennung entschieden. Anstelle des in der Umgangssprache (und selbst in der juristischen Fachsprache) vorwiegend benutzten Lehnbegriffes データ *dēta* findet sich, zumindest in der kardinalen Definitionsklausel, nur der rein japanische Begriff 情報 *jōhō*.[24] Die Bezeichnung als データ *dēta* taucht aber im Text dennoch an prominenten Stellen auf. So nennen drei der in Art. 2 Abs. 2 enthaltenen Begriffsbestimmungen Wortkomposita mit diesem Bestandteil.[25] Was den möglichen semantischen Ansatz des Gesetzgebers bestätigt, nur bei Pluralität von *Information* von dem Terminus „Daten", also ausgedrückt in *katakana* als データ *dēta*, Gebrauch machen zu wollen.

Trotz der Komplexität der Definitionsklauseln für die wichtigsten Begriffe des GSpI sollen hier drei Beispiele in möglichst bedeutungsnaher (nicht wörtlicher) deutscher Übersetzung angeführt werden. Einmal die kardinale Definition für „persönliche Informationen" und (weil separat definiert, aber von der Eigenschaft her auch der Definition von „Daten" unterworfen) der Begriff „individuelle Identifikationscodes". Sodann die Begriffsbestimmung für „sensitive Daten".

---

22 So z.B. das Gesetz betreffend den Schutz der von Verwaltungsorganen vorgehaltenen persönlichen Informationen, Gesetz Nr. 58/2003, 行政機関の保有する個人情報の保護に関する法律 *Gyōsei kikan no hoyū suru kojin jōhō no hogo ni kansuru hōritsu*, und das inhaltlich fast gleichlautende Gesetz betreffend den Schutz der von selbstständigen Körperschaften der Verwaltung vorgehaltenen persönlichen Informationen, Gesetz Nr. 59/2003, 独立行政法人等の保有する個人情報の保護に関する法律 *Dokuritsu gyōsei hōjin-tō no hoyū suru kojin jōhō no hogo ni kansuru hōritsu* .

23 Diese in Art. 76 Abs. 1 enthaltenen Regelungen kann man insoweit vergleichen mit der in der DSGVO für die einzelnen EU-Mitgliedstaaten enthaltenen Möglichkeit (dort in Art. 85 Abs. 2), durch eine Öffnungsklausel national abweichende Einzelregelungen zuzulassen.

24 Was umgangssprachlich eher für „Information" – zuweilen für „Auskunft" – steht. Im IT-Bereich findet sich *jōhō* neuerdings häufiger auch im Sinne von „Daten". Im originären Internetrecht hingegen überwiegend im Sinne von „Inhalte" bzw. „Netzinhalte".

25 Diese Begriffe sind 個人データ *kojin dēta* für: persönliche Daten, データベース *dēta bēsu* (von engl. *data base*) und 保有個人データ *hoyū kojin dēta* für: „vorgehaltene persönliche Daten".

1. „*Persönliche Informationen*“[26] sind nach diesem Gesetz solche die folgenden Voraussetzungen erfüllenden Informationen über lebende natürliche Personen, nämlich:
(i) mit Ausnahme von individuellen Identifikationscodes alle jene [*Informationen*], die z. B. den Namen, das Geburtsdatum oder eine andere personenbezogene Beschreibung oder Darstellung usw. enthalten oder diese aufzeichnen und durch welche eine bestimmte Person identifiziert werden kann – was auch solche Informationen umfasst, welche durch einfachen Vergleich mit weiteren Informationen eine Identifikation ermöglichen. Dabei gelten als „Beschreibung oder Darstellung usw.“ auch alle auf elektromagnetischem Weg erstellten Aufzeichnungen, seien es elektronisch oder magnetisch erstellte oder solche, die durch andere Formen wie durch Gesten oder Bewegungen hervorgerufen werden und durch menschlich-kognitive Methoden nicht erkannt werden können; Gleiches gilt für nachstehend 2. sowie für Art. 18 Abs. 2.;
(ii) solche [*Informationen*], die einen individuellen Identifikationscode enthalten.

In der vorstehenden Definition ist mit Hinweis auf Nr. 2 auf einen weiteren Unterbegriff verwiesen, der „individuelle Identifikationscodes“ wie folgt definiert:

2. Als „*individuelle Identifikationscodes*“[27] im Sinne dieses Gesetzes sind solche in einer Kabinettsanordnung näher festgelegten [Folgen von] Zeichen, Buchstaben, Ziffern, Symbole[n] oder anderen Codes zu verstehen, welche unter eine der nachfolgend beschriebenen Kategorien fallen:
(i) solche [Codes], durch welche mittels einer Folge von Zeichen, Buchstaben, Ziffern, Symbolen oder anderen Codes persönliche charakteristische Kennzeichen einer bestimmten Person in die Form gebracht wurden, eine elektronische Verarbeitung zu ermöglichen, und welche dann einer Identifizierung [eben] jener Person dienen können, und
(ii) solche aus einer Folge von Zeichen, Buchstaben, Ziffern, Symbolen oder anderen Codes bestehenden und auf elektronische Weise aufgezeichneten und registrierten Codes, die bestimmten Personen im Zusammenhang mit dem Anbieten der Nutzung einer Dienstleistung oder von An- und Verkaufsgeschäften oder bei der Ausgabe von Karten zugeordnet werden und die dann dazu dienen können, eine Unterscheidung von jenen eine solche Dienstleistung nutzenden oder Kaufgeschäfte durchführenden Personen vorzunehmen, oder die den jeweiligen Karteninhaber identifizierbar machen.

3. Als „*besonderes Augenmerk erfordernde persönliche Informationen*“[28] gelten nach diesem Gesetz solche persönlichen Informationen betreffend Datensubjekte, welche eine rassische oder religiöse Zugehörigkeit aufzeigen, die Hinweise auf die soziale Stellung, eine Krankengeschichte, Vorstrafen oder Tatsachen auf durch Straftaten erlittene Schäden beinhalten und deren Handhabung [deshalb] ganz besondere Sorgfalt erfordert, um jede Diskriminierung und das Entstehen von Vorurteilen gegen oder anderen Nachteilen für diese Datensubjekte zu vermeiden – was auch solche in Kabinettsbeschlüssen gesondert festgelegten persönlichen Informationen einschließt.

---

26 個人情報 *kojin jōhō*.
27 個人識別符号 *kojin shikibetsu fugō*.
28 要配慮情報 *yō-hairyo kojin jōhō* für „sensitive Daten“.

Weiter finden sich in Art. 2 im weiteren Verlauf die Begriffe „anonymisierte Daten“, 匿名加工情報 *tokumei kakō jōhō*, und, indes erst seit der Revision von 2020, „pseudonymisierte Daten“, 解明加工情報 *kaimei kakō jōhō*, definiert.

Es würde den Umfang dieses Beitrages sprengen, die unter jene vorstehend dargestellten und damit dem Schutzbereich dieses Gesetzes unterfallenden Arten von persönlichen Daten auch nur annähernd aufzuzählen. So viel sei indes verdeutlicht: In der Praxis werden neben althergebrachten Daten wie Namens- und Geburtsangaben sowie Wohnort, Telefonnummern usw. auch Fotos, Fingerabdrücke, Netzhautabbildungen und auch Gesichtserkennungsdaten als schützenswerte Daten erfasst. Umfassende Aufzählungen und Erklärungen finden sich in den von der DSK herausgegebenen Leitlinien, ガイドライン *gaidorain* (*guidelines*) (vgl. vorstehend den Beginn von II.1.) sowie hier nachfolgend unter II.3.). Diese z. T. sehr umfangreichen und mit technischen Ausdrücken gespickten Leitlinien müssen naturgemäß bei der Prüfung des Tatbestandsmerkmals „Daten“ herangezogen werden.

Als Verständnishilfe zu dem, was sich hinter dem in der zweiten Begriffsbestimmungsklausel genannten abstrakten Terminus „individuelle Identifikationscodes“ versteckt, mögen zwei konkrete Beispiele dienen, die im Rahmen der nationalen Anwendung des Gesetzes wichtig sind: Einmal sind darunter privatwirtschaftlich benutzte bzw. vergebene Personenkennzahlen (etwa im Versicherungs- und Bankenverkehr) oder auch amtliche Personenkennziffern zu verstehen – z. B. persönliche Steuer- oder Sozialversicherungsnummern.[29] Oder die per Sondergesetz eingeführten nationalen Personenkennziffern.[30] Das wiederum erleichtert das Verständnis, wenn man an die wirtschaftliche Anwendung von Zahlenkombinationen denkt. Im Wirtschaftsverkehr wird diese Bestimmung für Empfänger (und letztlich Verwender) von feststehenden Zahlen- bzw. Codekombinationen relevant, wenn in technischen Geräten enthaltene elektronische Komponenten algorithmische Daten versenden (und zwar oft versteckt, wie etwa GPS-Daten), die dann zeitgleich einem bestimmten – oder zumindest bestimmbaren – individuellen Datensubjekt zugeordnet werden können.

---

29 Diese in angelsächsischen Staaten meist als SSN (*social security number*) und TIN (*tax identification number*) bezeichneten Personenkennzahlen haben in deren Abkürzungsform sogar in die japanische Fachliteratur Eingang gefunden.

30 Nach dem „Gesetz betreffend die in Verwaltungsverfahren benutzten und Verwendung findenden, der Unterscheidung von Individuen dienenden individualisierten Personenkennziffern“, 行政手続における特定の個人を識別するための番号の利用等に関する法律 *Gyōsei tetsuzuki ni okeru tokutei no kojin o shikibetsu suru tame no bangō no riyō-tō ni kansuru hōritsu* (meist verkürzt in englisch-japanischer Mischweise verwiesen als das マイナンバー法 *Mainanbā-hō*, das *My-number*-Gesetz, Gesetz Nr. 27/2013).

d) Inhaltlicher Anwendungsbereich

Die tatbestandlich erfassten Handlungen bzw. potenziell schädigenden Aktivitäten werden, wenn man die japanischen Bestimmungen sprachlich betrachtet und mit Deutsch oder Englisch vergleicht, mit relativ wenigen Nomen- oder Verbformen bezeichnet. Im GSpI wie in den diversen Leitlinien und *kisoku* wird das, was man als tatbestandlich relevante Handlung bezeichnen könnte, meist durch die Verbform 取り扱う *toriatsukau* = „etwas behandeln" wiedergegeben. Man kann das auch als ein „Umgehen mit" ausdrücken. An manchen Stellen findet sich der Doppelausdruck 利活用する *ri-katsuyō suru* = „anwenden und gebrauchen" (bzw. in substantivierter Form „Anwendung und Gebrauch").[31] Diese unterschiedliche Wortwahl ist indes in solchen Fällen, in denen kein spezifischeres Verb benutzt wird, im Sinn eines Überbegriffs für die Vielzahl der im Umgang mit Daten ansonsten (d. h. auch in anderen Sprachen) benutzten Begriffe zu sehen. Wie etwa Daten *erheben*, *empfangen*, *speichern*, *verändern*, *verarbeiten*, *übermitteln*, *löschen* u. v. m.

e) Geografischer Anwendungsbereich

Mit Ausnahme eines einzigen Tatbestandes war das GSpI 2017, weil als ein nationales Gesetz konzipiert, nur in Japan anwendbar. Der Verstoß gegen datenschutzrechtliche Vorschriften war, wenn aus Japan heraus im Ausland Auswirkungen zeigend oder aber z. B. als japanische Tochtergesellschaft aus dem Ausland nach Japan hinein begangen, durch das GSpI nicht erfassbar. Erst das GSpI 2020 brachte eine Ausweitung, d. h. eine partielle echte Extraterritorialität im Anwendungsbereich.[32] Die bis dato einzige Vorschrift, welche eine Erstreckung auf im Ausland begangene Handlungen vorsah, ist durch tatbestandliche Erweiterung und durch Einfügen neuer Vorschriften ergänzt und damit sehr erweitert worden. Außerhalb Japans ansässige, mit persönlichen Daten i. S. d. GSpI (im weitesten Sinn) umgehende Unternehmen unterliegen damit seit Mitte des Jahres 2022 umfassend den Pflichten des japanischen Datenschutzgesetzes. Was bedeutet, dass die DSK ihnen Berichtspflichten auferlegen kann, sie kann sie mit Auflagen belegen oder ihnen können Anweisungen erteilt und sie können um Auskunft angegangen werden. Die DSK kann Vor-Ort-Untersuchungen verlangen und vornehmen bzw. vornehmen lassen. Der gesamte Katalog der Strafbestimmungen des GSpI findet auf diese Unternehmen Anwendung (vgl. die Darstellung nachfolgend unter IV.1.). Ob und in welchem

31 Manchmal auch allein die Verbform 活用する *katsuyō suru*, was ebenfalls „gebrauchen", „verwenden" oder „umgehen mit etwas" umschreibt.

32 Art. 75.

Umfang das erfolgreich sein wird, kann sich erst in der Anwendungspraxis nach dem erst recht kürzlich erfolgten Inkrafttreten zeigen.

2. Kisoku, Verwaltungsrichtlinien[33]

Nur der Vollständigkeit halber seien hier die beiden wichtigen *kisoku* aufgeführt, welche Regelungen für die verwaltungsinterne Behandlung von persönlichen Daten von Bürgern aufstellen.[34] Schutzobjekte sind in beiden Fällen diejenigen Daten, bei denen die Unterscheidbarkeit bzw. Individualisierbarkeit der Datensubjekte erhalten geblieben sind.[35] Was vorstellbar eher den größeren Teil der von Verwaltungsorganen gehaltenen persönlichen Daten ausmachen dürfte. Eine tatbestandliche Handlung ist nicht beschrieben. Verpflichtete sind einmal (bei den *Kisoku Nr. 1,* 規則一号 *kisoku ichigō*) „Verwaltungsorgane“, 行政機関 *gyōsei kikan*. Und in den *Kisoku Nr. 2,* 規則二号 *kisoku nigō* sind es „selbstständige Körperschaften der Verwaltung oder jenen ähnliche“, 独立行政法人等 *dokuritsu gyōsei hōjin-tō*.[36]

3. Die Leitlinien der Datenschutzkommission, ガイドライン *gaidorain*

Der Regelungsinhalt der von der Kommission für die Privatwirtschaft herausgegebenen, von eins bis sechs nummerierten, grundlegenden und für die Praxis wegen ihrer Detailliertheit sehr wichtigen Leitlinien ergibt sich weitgehend schon aus den jeweiligen sekundären Überschriften. Dazu kommen weitere von Ressortministerien erlassenen Leitlinien für Anwender aus bestimmten Branchen bzw. Sektoren.

Einige dieser Leitlinien der DSK (aber auch der Ministerien) zeigen einen erheblichen textlichen Umfang. Die – zumindest gesetzestechnisch gesehen – so etwas wie einen „Allgemeinen Teil“ (für alle weiteren Leitlinien) bil-

---

33 Ein vom Verfasser vorzugsweise unübersetzt belassener Begriff. Im hier vorliegenden verwaltungsrechtlichen Kontext kann man diesen mit „Verwaltungsrichtlinien“ bezeichnen. Häufiger findet sich der Begriff „Amtsanweisung“.

34 Die dritte Verwaltungsrichtlinie betrifft nicht materielle, sondern formelle Anweisungen an die Verwaltung, 平成二十八年十月五日個人情報保護委員会規則第三号, die am 5. Oktober Heisei 28 [2016] herausgegebenen *kisoku* der Datenschutzkommission.

35 非識別加工情報 *hi-shikibetsu kakō jōhō*, also nicht anonymisierte Daten.

36 Der formell vollständige Titel heißt übersetzt „*Kisoku* betreffend Vorschriften für das Verhalten von Verwaltungsorganen mit den von ihnen vorgehaltenen und gemäß Kapitel 4 Abschnitt 2 GSpI angebotenen nicht anonymisierten persönlichen Daten“, 行政機関の保有する「個人情報の保護に関する法律」四章の二の規定による行政機関非識別加工情報の提供に関する規則 *Gyōsei kikan no hoyū suru ‘Kojin jōhō no hogo ni kansuru hōritsu‘ yon-shō no ni no kitei ni yoru gyōsei kikan hi-shikibetsu kakō jōhō no teikyō ni kansuru kisoku.* In der fast gleichlautenden *kisoku* Nr. 2 sind nur die „Verwaltungsorgane“ ersetzt durch „selbstständige Körperschaften der Verwaltung oder jenen ähnliche“.

dende Leitlinie Nr. 1 der DSK umfasst z. B. über 160 Seiten[37] und führt den Titel „Leitlinien zum Gesetz betreffend den Schutz persönlicher Daten Nr. 1 – Allgemeine Grundsätze". Weitere Leitlinien betreffen die grenzüberschreitende Versendung von Daten: „Nr. 2 – Betreffend das Anbieten [von Daten] an Personen im Ausland". Andere sind nur an Verwaltungsorgane oder Gebietskörperschaften gerichtet.[38] Drei weitere sind branchenbezogen erlassen, etwa für den gesamten Finanzsektor,[39] für die Branche der Kreditvergabe – aber auch für die Forderungseintreibung bzw. Factoring.

Als untergesetzliche Regelwerke zeigen Leitlinien im Grundsatz keine direkte Bindungswirkung. Dennoch trifft jede der Leitlinien eine konkrete Aussage dazu. Es heißt dort:

„In diesen guidelines bedeuten die Formulierungen ‚müssen' oder ‚haben zu', dass dann, wenn [hierin aufgestellten] Regeln nicht gefolgt oder diesen nicht entsprochen wird, die Möglichkeit besteht, das [Verhalten] als einen Gesetzesverstoß anzusehen."[40]

Und der Folgesatz führt aus, dass andererseits bei der Nichtbefolgung von fakultativ formulierten Regelungen (in Kann-Form) zwar nicht unmittelbar eine Gesetzwidrigkeit angenommen werde, dass aber bei der Beurteilung durch die DSK die in Art. 2 Abs. 3 formulierte Zielbestimmungsklausel und der in Art. 1 niedergelegte Gesetzeszweck herangezogen würden.

Während es nach der Revision von 2017 noch recht lange gedauert hatte, bis Übersetzungen der Leitlinien verfügbar waren, sind im Zuge der Reform 2022 inzwischen die meisten der Leitlinien zumindest in halboffizieller Übersetzungsfassung über das Netz abrufbar.

---

37 Mit Anhängen ist die japanische PDF-Fassung 182 Seiten stark, wobei die jeweilige Wiedergabe zuerst des Gesetzes- oder *kisoku*-Textes einerseits und eine Fülle von Beispielen andererseits relativ viel Raum einnehmen.

38 So die „Leitlinien betreffend den Schutz der von Verwaltungsorganen nach dem Gesetz betreffend den Schutz persönlicher Daten vorgehaltenen persönlichen Daten Nr. 5 – Betreffend die seitens der Verwaltungsorgane nicht identifizierbar gemachten Daten" oder „Leitlinien betreffend den Schutz der u. a. von selbstständigen Körperschaften der Verwaltung nach dem Gesetz betreffend den Schutz persönlicher Daten vorgehaltenen Daten Nr. 6 – Betreffend die u. a. seitens der selbstständigen Körperschaften der Verwaltung nicht identifizierbar gemachten Daten".

39 Leitlinien betreffend den Schutz persönlicher Informationen in der Finanzbranche, 金融分野における個人情報保護に関するガイドライン *Kin'yū bunya ni okeru kojin jōhō hogo ni kansuru gaidorain.*

40 Beispielsweise 「しなければならない」及び「してはならない」と記述している事項については、これらに従わなかった場合、法違反と判断される可能性がある *‚shinakereba naranai' oyobi ‚shite wa naranai' to kijutsu shite iru jikō ni tsuite wa, korera ni shitagawa nakatta ba'ai, hō-ihan to handan sareru kanō-sei ga aru*.

III. Rechte und Pflichten

Wie eingangs erwähnt, ergeben sich eine ganze Reihe von Pflichten direkt aus dem Gesetz. Zumindest in Teilbereichen wirtschaftlicher Betätigung werden diese ergänzt durch Leitlinien, *guidelines* der DSK. Eine der grundlegendsten Verwenderpflichten besteht darin, Betroffenen den Zweck jeglicher Datennutzung – genauer gesagt, den Umfang des Nutzungszwecks – in ausreichend detaillierter Weise mitzuteilen. Dazu stellt das Gesetz umfassende Regeln betreffend die Art und Weise der Mitteilung selbst, den Zeitpunkt und den Umfang auf. So etwa zum Zeitpunkt, wann solche Mitteilung zu erfolgen hat.

1. Verwenderpflichten; Pflichten dritter Datenempfänger

Verwender dürfen persönliche Informationen nur erheben und persönliche Daten nur sammeln, wenn sie einen von vornherein festgelegten, detailliert beschriebenen und den Betroffenen mitgeteilten Zweck (Nutzungszweck) erfüllen. Verwendet werden dürfen persönliche Daten also nur, nachdem der Verwender die Betroffenen vorab über den Zweck der Verwendung[41] ausreichend unterrichtet hat, Art. 18 Abs. 1, 2[42] und Art. 27 Abs. 1 (ii). Schriftlichkeit ist nicht gefordert – in der Praxis wird das zumindest im wirtschaftlichen Bereich ohnehin schriftlich geschehen.[43] Der Umgang mit persönlichen Daten ist und bleibt nur im Rahmen genau jenes Zwecks erlaubt, der einmal festgelegt und Betroffenen mitgeteilt wurde. Spätere Zweck- oder Nutzungsänderungen, die sich ergeben können, sind Betroffenen ebenso mitzuteilen. Es ist die Aufgabe der Verwender, den Zweck oder die Zwecke der Nutzung anfangs eindeutig zu formulieren, Art. 23. Bei nachträglich eingetretenen Änderungen, die über einen Minimalumfang hinausgehen, entsteht zwingend eine erneute Vorab-Mitteilungspflicht.

Eine Mitteilung kann individuell gegenüber jedem einzelnen Betroffenen erfolgen, wie das etwa in Arbeits- oder anderen gegenseitigen Vertragsverhältnissen[44] der Fall ist. Das GSpI etabliert aber eine Gleichwertigkeit

41 Das in Parallele zum Zweckbindungsgrundsatz des Art. 5 Abs. 1 lit. b DSGVO.

42 Abs. 1 für Fälle, in denen der Verwender die persönlichen Daten erlangt. Ist der Zweck schon (ggf. online) öffentlich der Allgemeinheit gegenüber bekannt gemacht, ist eine weitere Mitteilung entbehrlich. Abs. 2 regelt die Fälle, in denen Verwender die Daten durch Individualvertrag erhalten. Dann reicht der Verweis auf eine „öffentliche Bekanntmachung" etwa auf der Website nicht aus.

43 In Verträgen, Angeboten (zumindest letztlich in Auftragsbestätigungen), in Allgemeinen Geschäfts- oder Vertragsbedingungen, in einzelnen Anstellungs- oder Arbeitsverträgen oder den Betriebsvereinbarungen 就業規則 *shūgyō kisoku*.

44 Was sogar für gewisse konkret benannte Tatsachen in einer kommerziellen Vertraulichkeitsvereinbarung, einem *Non-Disclosure Agreement*, zulässig sein kann.

insoweit, dass die Unterrichtung über den Zweck in manchen Fällen auch „gegenüber der Allgemeinheit“ stattfinden kann. Das ermöglicht eine Mitteilung der Zweckbeschreibung und -erklärung, wie heute allgemein üblich, auf Websites oder durch physisch überreichte oder ins Netz gestellte Datenschutzerklärungen. Solche Mitteilungen an die Allgemeinheit unterliegen detailliert im GSpI vorgeschriebenen Anforderungen, die sich indes wieder nur teilweise aus dem GSpI selbst, zum weitaus größeren Teil aus den DSK-Leitlinien, *guidelines*, ergeben.

In manchen Fällen ist eine Einwilligung von Betroffenen zeitlich vor der Weitergabe von persönlichen Informationen an Dritte gefordert. Das sind insbesondere Situationen der Rechtsnachfolge bei Unternehmen oder Umstrukturierungen. Oder die häufigeren Fälle des Outsourcings von Aufgaben oder Teilaufgaben an spezielle Dienstleister. Die wichtigste Regel-Ausnahme-Vorschrift stellt dazu Art. 23 Abs. 1 und 2 dar, wobei Abs. 2 insbesondere die Voraussetzungen für eine Zustimmungsfreiheit beschreibt und festlegt. Für sensitive Daten[45] besteht in jedem Fall und unter allen Umständen schon *vor dem konkreten Erhalt* solcher Daten das zwingende Erfordernis, dass Betroffene ihre ausdrückliche Einwilligung erteilen.[46] Eine vom Verwender generell vorgeschlagene Nichtbeteiligungserklärung, also ein *opt out*, lässt das GSpI nicht zu – weder per einseitiger individueller Erklärung durch Betroffene an den Verwender noch durch eine öffentliche, also online erfolgende Fernerklärung, z. B. durch Anklicken einer Box. Zwischen den beiden vorgenannten Gruppen stehen die anonymisierten und pseudonymisierten Daten, für die in den Artt. 35, 35-2 und 36 und 36-2 sehr spezielle und detaillierte Anforderungen aufgezeigt werden. Auch hier müssen die gesetzlichen Vorschriften ganz eng in Gesamtschau mit den *guidelines* der DSK betrachtet werden. Beispiele aus dem Bereich Konsumentenschutz sind etwa, dass bei personenbezogenen oder transaktionsrelevanten Kategorien von weiterzuleitenden Daten es als zulässige Angabe gilt, dass z. B. nur das Lebensalter bzw. Geburtsjahr und das Geschlecht von Betroffenen weitergegeben werden. Und bei geschäfts- oder transaktionsbezogenen Umständen, dass allein die statistische Häufigkeit und ggf. die Zeitangabe von Interessenbekundungen[47], differenzierende Produktmerkmale (wie etwa Farben, Größen, Anwendungsfelder, Kapazitätsangaben) oder Anschaf-

45 Siehe vorstehend die Übersetzung zu Art. 2 Abs. 3.

46 Der Grundsatz ist einmal in Art. 17 Abs. 2 genannt – auch hier versehen mit einem umfangreichen, das öffentliche Interesse betreffenden Ausnahmekatalog. Nochmalige Erwähnung findet der Grundsatz innerhalb des Regel-Ausnahme-Katalogs in Art. 23 Abs. 2.

47 Zugangszahlen oder *clicks* im Netz.

fungs- oder Bestellungswerte bei Kauf- oder Subskriptionsgeschäften usw. weitergegeben würden.

Alle Verwender, die persönliche Daten an Dritte übermitteln, sind nach Art. 25 verpflichtet, jeweils das Datum der Übermittlung, den Namen oder die Bezeichnung des oder der Dritten und weitere von der DSK vorgegebene Einzelheiten aufzuzeichnen und zu registrieren.[48] Und sie haben diese Aufzeichnungen für einen (ebenfalls in Leitlinien) vorgeschriebenen Zeitraum aufzubewahren. Dritte, welche, zu welchem zulässigen Zweck auch immer, von Verwendern persönliche Daten enthalten, unterliegen nach Art. 26 ähnlichen, inhaltlich im Detail sogar noch weiter gehenden, noch mehr Angaben erfordernden Verpflichtungen.

Korrespondierend zu den Rechten von Betroffenen (vgl. unmittelbar hier nachfolgend) beschreibt das GSpI in einem recht detaillierten Katalog von Anforderungen, wie Verwender den Verlangen von Betroffenen nach Offenlegung (Art. 28 Abs. 1), Berichtigung (Art. 29 Abs. 1), Löschung und Nutzungsunterlassung (Art. 30) nachzukommen haben.

2. Die Rechte von Datensubjekten

Korrespondierend zu den jegliche Datenüberlassung einleitenden Verwenderpflichten, nämlich den Zweck der Datennutzung und den Umstand der Weitergabe der erhaltenen Daten an Dritte anzugeben, steht Betroffenen das Recht zu, vorab ausreichend genau über den Zweck der Datennutzung sowie davon unterrichtet zu werden, ob und wieweit Daten an Dritte weitergegeben werden. Daneben stehen – im späteren Verlauf nach der Datenüberlassung – die ihnen, den Datensubjekten, durch das GSpI zugestandenen Rechte, jederzeit die Offenlegung überlassener persönlicher Daten[49], deren Berichtigung[50] oder deren Löschung[51] sowie das Unterlassen[52] eines weiteren Gebrauchs zu verlangen.

Alle drei Vorschriften der Artt. 28 bis 30, die es Betroffenen ermöglichen, jene hier vorgenannten Rechte gegen Verwender geltend zu machen,

---

48 Art. 25 Abs. 1. Wobei auch formell die Registrierung jener Tatsachen durch eine seitens der DSK in Leitlinien besonders vorgegebenen Form zu erfolgen hat.

49 Art. 28 Abs. 1, der „Offenlegungsanspruch" von Betroffenen, 開示権 *kaiji-ken.*

50 Art. 29, der Anspruch auf „Korrektur usw.", 訂正等 *teisei-tō*, was Berichtigungen, Hinzufügungen und die Streichung, Entfernung oder Weglassung umfasst.

51 Dieses Recht auf Löschung, 解消 *kaishō,* ist nur auf einzelne mitgeteilte Daten bezogen (und selbst da nur in einem tatbestandlich eng begrenzten Rahmen), was folglich nicht ansatzweise mit dem „Recht auf Vergessenwerden" in Zusammenhang gebracht werden sollte.

52 Auch hier besteht eine tatbestandliche Einschränkung: Art. 30 findet nur Anwendung, wenn jene Daten unter Missachtung von Art. 16 oder 17 erlangt worden sind.

sind, was den Gegenstand und die Rechtsqualität des Verlangens angeht, im Wesentlichen gleich formuliert. So spezifiziert das Gesetz einmal den Gegenstand des Verlangens etwas näher als die Basisdefinition des Art. 2. Hier wird der Begriff „Daten" etwas weiter spezifiziert als „solche vorgehaltenen persönlichen Daten, die eine Identifizierung ermöglichen", 識別される保有個人データ *shikibetsu sareru hoyū kojin dēta*. Gemeint ist eine Identifizierung des Betroffenen. Hinsichtlich der Rechtsqualität des Verlangens formuliert das Gesetz in allen drei Fällen gleichermaßen i.S.v. „verlangen" oder „fordern" können.[53]

Die Untersagungsgründe für eine Nutzung bzw. Weiternutzung und auch Gründe für ein Löschungsverlangen seitens Betroffener waren vor 2022 auf eine *zweckfremde*, d.h. eine den anfangs mitgeteilten Zwecken überschreitende Nutzung einerseits und auf die Weiternutzung von mit unrechtmäßigen Mitteln erlangten Daten andererseits beschränkt. Mit dem GSpI 2020 ist der Katalog der bestehenden Untersagungs- und Löschungsgründe wie folgt erweitert worden: bei Vorliegen aller das neu eingeführte Verbot des Art. 22-2 rechtfertigenden Gründe, dem objektiven Wegfall der Nutzungsgründe für eine Datenüberlassung, dem Eintritt eines Datenlecks und schließlich „für alle anderen Fälle, wenn für Betroffene die Sorge besteht, dass ihre Rechte oder andere berechtigte Interessen verletzt werden können, indem die [einem Dritten] überlassenen Daten oder der Gebrauch dieser seitens der Verwender zur Identifizierung [des Datensubjekts] führen können."

Anträge auf die vorgenannten Verlangen auf Offenlegung etc. müssen nicht notwendig durch Betroffene selbst vorgebracht oder gestellt werden. Art. 32 Abs. 3. erlaubt dazu die Bestellung eines Vertreters. Betroffene sind nach Art. 34 Abs. 1 aber gezwungen, vor dem Erheben einer Klage bei Gericht gegen einen Verwender eine 14-tägige Wartefrist einzuhalten, nachdem ihr Verlangen aus den ihnen nach Artt. 28, 29 und 30 eingeräumten Rechten dem Verwender zugegangen ist – es sei denn, der Verwender hat ein dahin gehendes Verlangen nachweislich bereits abgelehnt.

3. Grenzüberschreitende Datenversendung

Eine grenzüberschreitende Übermittlung von Daten – also aus Japan hinaus ins Ausland – erlaubt das GSpI in Art. 24 nur, nachdem die Verwender von den Betroffenen die vorherige ausdrücklich erteilte Zustimmung erlangt haben. Das erfordert zwingend eine individuelle Erklärung seitens der Betroffenen. Eine Kundgabe an die Allgemeinheit, wie sie an anderen Stellen

53 Das wird nicht im Sinne eines „rechtlichen Anspruchs auf etwas" ausgedrückt, sondern etwas schwächer als 請求することができる *seikyū suru koto ga dekiru*. Sehr ähnlich, aber eher eine Nuance schwächer, findet das in anderen Vorschriften mit dem Verb 求める *motomeru* („etwas verlangen") Ausdruck.

im Gesetz als zulässig angesehen wird – und wie sie im globalen Wirtschaftsleben inzwischen zur Norm geworden ist (also durch Aufnahme einer online erfolgenden Zustimmungserklärung via Website oder in Datenschutzerklärungen) –, lässt das Gesetz ausdrücklich nicht zu.[54] Eine von zwei Ausnahmen im Gesetz stellt allerdings die zwischenstaatliche Lösung dar, die, wie schon eingangs dargestellt, zwischen der EU und Japan durch die Reziprozitätsfeststellung und den Angemessenheitsbeschluss von 2019 erreicht wurde. Im Verhältnis zu EU-Staaten können japanische Verwender also (mit wenigen Ausnahmen) Daten auch ohne eine ausdrückliche Zustimmung durch Betroffene versenden. Insoweit reichen eine ausreichend klare Unterrichtung oder andere Hinweise in der *privacy policy* auf die Möglichkeit der Datenversendung in Länder der EU aus.

Betrachtet man das Thema weiter unter dem Aspekt einer grenzüberschreitenden Datenversendung in andere Staaten (z.B. südostasiatische oder sogar darüber hinausgehend im asiatischen Pazifik-Bereich), so bleibt es bei der Regelung des Art. 24. Was dann für japanische Tochtergesellschaften von EU-basierten Unternehmen oder in Joint-Venture-Strukturen mit japanischen Unternehmen weiterhin erst einmal problembeladen bleibt.[55]

Formell trifft die an sich recht wortreiche Vorschrift des Art. 24 nur eine kurze Grundaussage[56]: Sie verlangte vor 2022 als Einziges, dass Betroffene vor Erlangen ihrer Zustimmung vorab über im Ausland befindliche, also die *Daten empfangende* Dritte zu informieren waren. Mit der Revision im GSpI 2020 sind in Art. 28 Abs. 2 beträchtlich weiter gehende Anforderungen hinzugekommen. Verwender haben die Betroffenen über das Datenschutzregime[57] und den Stand des rechtlichen Schutzes von persönlichen

54 Die gesetzliche Regelung des alten Datenschutzgesetzes von 2003 sah nicht einmal eine Unterscheidung nach dem Wohn- oder Aufenthaltsort bei der Versendung von Daten vor.

55 Und damit auch im Rahmen einer datenschutzrechtlichen Due-Diligence- oder gruppeninternen Compliance-Prüfung. Es bleibt dort der weiterhin schwierige Problemkreis in Fällen grenzüberschreitender Datenversendungen aus Japan hinein in asiatisch-pazifische Länder, bei denen es keine zwischenstaatliche Regelung gibt – dann bestehen in jedem Fall eine Vorab-Informationspflicht und Genehmigungspflicht von Betroffenen. Ein weiteres Beispiel ist das nicht ausgestandene Problem innerasiatischer Wirtschaftsabkommen (APEC-Gemeinschaft) samt dem weiterhin ungelösten Datenschutz über das APEC Privacy Framework.

56 外国にある［…］第三者［…］予め［…］本人の同意を得なければならない *gaikoku ni aru* [...] *daisan-sha* [...] *arakajime* [...] *honnin no dōi o enakereba naranai.*

57 Im Gesetz weit gefasst formuliert als … *kojin jōhō no hogo ni kansuru seido* 個人情報の保護に関する制度, d.h. „das System von …“. Zur Beurteilung dessen, was eine angemessene Schilderung darstellt, kann man nur die Praxis der datenversendenden Unternehmen abwarten.

Daten in jenem Land (also dem Zielland der Datenversendung) sowie über die konkret getroffenen Datenschutzvorkehrungen des datenbearbeitenden Unternehmens im Ausland zu unterrichten. Das muss vor dem Erlangen des Einverständnisses zur grenzüberschreitenden Datenversendung geschehen und muss ausreichend detailliert geschildert werden. Abs. 3 legt dem (nationalen) Verwender zudem die Verpflichtung auf, die Einhaltung der datenschutzrechtlichen Landesbestimmungen und die anhaltende Beachtung der eigenen Datenschutzmaßnahmen und Vorrichtungen des ausländischen Bearbeiters sicherzustellen. Umfangreiche weitere Einzelheiten finden sich in den von der DSK speziell zu diesem Thema erlassenen und mit einem Umfang von (nunmehr, nach der Revision von 2020) 47 Seiten sehr ausführlichen „Leitlinien Nr. 2 – Betreffend das Anbieten [von Daten] an Personen im Ausland".

4. Folgen bei Rechtsverletzungen

In Kapitel VII des GSpI finden sich Strafbestimmungen, die neben der Bestrafung von Handelnden (Freiheitsstrafen und Geldstrafen) auch eine Parallelbestrafung[58] von juristischen Personen (nur mit Geldstrafen) einschließen. In diesem Zusammenhang ist anzumerken, dass in Japan Verstöße gegen Strafnormen außerhalb des Kernstrafrechts nicht als Ordnungswidrigkeit verfolgt und geahndet werden. Der Sanktionsmechanismus ist mithin ein genuin strafrechtlicher mit einem formellen staatsanwaltlichen Ermittlungs- und Anklageverfahren.

Unter Strafe gestellt finden sich insbesondere solche Tatbestände, die auf eine widerrechtliche Gewinnerzielung ausgerichtet sind, oder solche, die eine Erzielung von Gewinn durch Dritte ermöglichen. Strafbedroht ist weiterhin ein Untätigbleiben bei oder die Nichtabwendung von Datenschutzverletzungen, nachdem die DSK gegenüber einem Verwender dahin gehend formell, also per Verwaltungsakt, ein positives Tun oder das Unterlassen von bestimmten Handlungen angeordnet hat.

Strafrechtlich belangt werden können nach der Vorschrift des Art. 83 die Mitglieder der Geschäftsführung[59], andere zur Vertretung berechtigte Personen und weitere, speziell mit Datenschutzaufgaben beauftragte Personen. Art. 86 erstreckt dabei die Strafandrohungen der Artt. 82 und 83 auf Perso-

58 Erfasst durch eine sog. Parallelbestrafungsnorm, 両罰規定 *ryōbatsu kitei.* So ordnet Art. 87 Abs. 1 an, dass neben einem vorwerfbar handelnden Individuum, welches der angedrohten Freiheitsstrafe unterworfen werden kann, zusätzlich die juristische Person (oder der Einzelkaufmann oder eine Einzelperson) zur Leistung der Geldstrafe verurteilt werden kann.

59 役員 *yaku'in* und 管理人 *kanri-nin*.

nen, die eine Straftat nach dem GSpI im Ausland begangen haben.[60] Dadurch kann theoretisch insbesondere eine profitorientierte Geschäftstätigkeit im Ausland, durchgeführt unter Missachtung japanischer Datenschutzvorschriften, zu Anklagen und einer Bestrafung in Japan führen.

Art. 83 stellt einerseits die Übermittlung von aggregierten Datensammlungen (ganzen Datenbanken) und andererseits die Nutzung von erschlichenen Datensammlungen unter Strafe, wenn dieses Handeln mit dem Vorsatz der eigenen Gewinnerzielung oder einer Gewinnerzielung durch Dritte vorgenommen wurde.[61]

Verschiedene positive Handlungen wie auch das Unterlassen im Zusammenhang mit einer formellen Anordnung der DSK (vgl. dazu nachfolgend IV.1.) an Verwender werden durch Art. 85 nunmehr[62] mit einer Geldstrafe von bis zu 300.000 JPY geahndet. So etwa das Nichtaushändigen von angeforderten Dokumenten und Unterlagen bzw. die Nichtvorlage eines angeforderten Berichts. Oder Falschangaben in Dokumenten oder Berichten oder vorsätzliche Falschangaben auf Anfragen der Kommission und falsche Antworten in Befragungen. Sowie letztlich die Verhinderung oder Verweigerung von Ortsbesichtigungen der DSK.

IV. Das Aufsichts- und Kontrollregime

In der hierarchischen Gliederung steht von der Kompetenzbreite her die japanische Datenschutzkommission an oberster Stelle. Im Kapitel IV des GSpI ist in dem mit „Aufsicht“, 監督 *kantoku*, überschriebenen Abschnitt 3, in den Artt. 40 bis 46, der Kompetenzbereich der DSK prominent geregelt.[63] Abschnitt 4, Artt. 47 bis 58, beschreibt die Einrichtung, Akkreditierung, Funktion und Befugnisse von privatrechtlich organisierten branchenorientierten Agenturen, 民間団体 *minkan dantai*. Dazu nachfolgend IV.2.

60 Die Strafandrohung des Art. 82 betrifft aber nur den Personenkreis der bei der Datenschutzkommission angestellten Personen oder dort in eine Position berufene Amtsträger, vgl. Artt. 67 bis 70.

61 Die Strafandrohung ist Freiheitsstrafe bis zu einem Jahr und Geldstrafe bis zu 500.000 JPY.

62 Durch das GSpI 2020 sind alle Beträge erhöht worden. Insbesondere die noch im GSpI 2017 vorgesehenen im internationalen Vergleich sehr niedrigen Geldstrafen für die Parallelbestrafung von juristischen Personen sind auf 1 Million JPY angehoben worden.

63 Art. 40 Abs. 1.

1. Aufsicht durch die Datenschutzkommission und ministerielle Fachressorts

Die DSK ist aufgrund eines Gesetzes errichtet.[64] Hierarchisch ist sie der Zuständigkeit des Premierministers zugeordnet, Art. 59 Abs. 2, und sie ist als eine unabhängige staatliche Institution eingerichtet, Art. 62. Ihre generelle Zielrichtung ist in Art. 60 damit beschrieben, dafür Sorge zu tragen – unter anderem „durch den Erlass von Anleitungen und durch Raterteilung" –, dass die Rechte und Interessen von Individuen geschützt werden. Wobei sie interessanterweise auch gehalten ist,

> „mit in Betracht zu ziehen, inwieweit die richtige und effektive Nutzung von persönlichen Daten zur Entwicklung neuer Industrien, zur Entwicklung einer lebhaften Marktwirtschaft und zu einer besseren Lebensqualität für das japanische Volk beiträgt".[65]

Ein detaillierter Zuständigkeitskatalog findet sich in Art. 61. Danach ist die DSK u.a. damit betraut,[66] bei der Formulierung und Durchsetzung einer grundsätzlichen nationalen Datenschutzpolitik mitzuwirken.[67] Den weitesten Zuständigkeitsbereich muss man in der Aufsicht betreffend den Umgang mit persönlichen Daten im Sinne des GSpI sehen, inklusive der Mediation und Beschwerdeführung darüber, Art. 61, Ziff. ii). Letztlich alle Dinge, welche Angelegenheiten betreffen, die eine bilaterale oder internationale Zusammenarbeit mit anderen Jurisdiktionen angehen.[68]

Art. 40 sieht vor, dass die DSK den Verwendern eine Berichtspflicht auferlegen kann – und sie ist weiterhin befugt, eine Vor-Ort-Besichtigung an den Betriebsstätten der Verwender vorzunehmen. Art. 41 lässt als Aufsichtsmaßnahmen den Erlass einer Anweisung, 指導 *shidō*, und eine Raterteilung, 助言 *jogen*, zu. Als die beiden striktesten Maßnahmen sieht Art. 42 die Empfehlung, 勧告 *kankoku*, und die Anordnung, 命令 *meirei*, vor.

---

64 Nach Art. 49 Abs. 3 des Gesetzes zur Einrichtung des Kabinettsbüros, 内閣設置法 *Naikaku setchi-hō*, Gesetz Nr. 809/1999, ist dieses befugt, solche Kommissionen und Agenturen einzurichten.

65 Vgl. Art. 60, Hs. 2. Diese gesetzgeberische Vorgabe der Einbeziehung von Prinzipien und Gedanken nationalwirtschaftlicher wie auch strukturwirtschaftlicher Interessen Japans bei der Ausformulierung der jeweiligen Pflichtenkataloge in den Leitlinien war schon in der ersten Generation von DSK-Leitlinien im Vorlauf auf das GSpI 2017 evident geworden. Trotz der gesetzlich an sich vorgegebenen Neutralitätspflicht der DSK war schon damals der Einfluss der Wirtschaftslobby deutlich spürbar.

66 Die Auflistung ist nicht erschöpfend, sie umfasst auch in mehreren Unterpunkten die Mitwirkung der DSK betreffend Daten, die nach dem *My-number*-Gesetz, vgl. Fn. 30, gehalten werden, mithin Stellen der staatlichen Verwaltung.

67 So Art. 61, Ziff. i).

68 Vgl. Art. 61, Ziff. viii).

Die graduell leichtere Maßnahme einer „Empfehlung“, 勧告 *kankoku*, steht der DSK dann offen, wenn Verwender gegen eine oder mehrere einen ganzen Katalog ausmachenden, in Abs. 1 aufgeführten Vorschriften des GSpI verstoßen haben. Wegen der relativen Bedeutung seien diese (zusammen mit einer Kurzbeschreibung) hier kurz aufgezählt:

Art. 16 (Beschränkung betreffend die Nutzung von Daten);
Art. 17 (korrekter Erhalt von Daten);
Art. 18 (Bekanntgabe der Nutzung vor/bei Erhalt von Daten);
Art. 20 (einzurichtende Sicherheitsvorkehrungen);
Art. 21 (personelle Überwachung);
Art. 22 (Überwachung Dritter);
Art. 23 {jedoch nicht dessen Abs. 4} (Beschränkungen betreffend die Weitergabe an Dritte);
Art. 24 (grenzüberschreitende Weitergabe);
Art. 25 (Aufzeichnungspflicht bei Weitergabe an Dritte);
Art. 26 {nicht jedoch dessen Abs. 2} (Bestätigungspflicht von Daten erhaltenden Verwendern);
Art. 27 (Bekanntgabeverpflichtung hinsichtlich vorgehaltener Daten);
Art. 28 {nicht jedoch dessen Abs. 1} (Pflicht zur Reaktion auf Offenlegungsverlangen Betroffener);
Art. 29 Abs. 2 oder 3 (Pflicht zur Reaktion auf Korrekturverlangen);
Art. 30 Abs. 2, 3 oder 4 (Pflicht zur Reaktion auf Untersagungsverlangen der Weiternutzung von Daten);
Art. 33 Abs. 2 (Festlegungsermessen von Gebühren) und
Art. 36 {jedoch nicht dessen Abs. 6} (Pflichten von Verwendern anonymisierter Daten).

Eine „Anordnung“, 命令 *meirei*, kann die DSK nach Abs. 2 der gleichen Vorschrift hinsichtlich ebenjener obigen Tatbestände dann erteilen, wenn eine gravierende Verletzung von Rechten von Individuen trotz der Tatsache droht, dass die DSK dem Verwender gegenüber schon eine „Empfehlung“ nach Abs. 1 ausgesprochen hatte, dieser der Empfehlung aber nicht hinreichend gefolgt ist oder ihr gar nicht entsprochen hat. Trotz des generellen Charakters aller dieser Vorschriften betreffend Maßnahmen gegen Verwender als *Kann*-Bestimmungen muss man sich in Erinnerung rufen, dass das Nichtbeachten von angeordneten Maßnahmen der DSK nach Art. 40 Abs. 1 wie auch Art. 42 Abs. 2 und Abs. 3 strafbewehrt ist.

Mit der Novellierung zum GSpI 2020 haben eine Reihe neuer Vorschriften Eingang gefunden, welche der Erleichterung der Anwendung oder Vollstreckung von Maßnahmen der DSK dienen. So fehlten bis dahin im GSpI 2017 noch Formvorschriften z. B. betreffend die Zustellung an und den Zugang bei Verwendern von Maßnahmeanordnungen der Kommission. Ebenfalls neu ist

eine Bestimmung, die es der Kommission erlaubt, beim Nichtbeachten, bei Untätigbleiben nach oder Zuwiderhandeln gegen Maßnahmen der DSK die Namen der Verwender oder der Unternehmen zu veröffentlichen.[69]

Betreffend die (hier nachfolgend weiter beschriebenen) privatrechtlich organisierten Agenturen ist die DSK verpflichtet, die erfolgte Akkreditierung solcher Agenturen[70] sowie den Umstand, dass diese eigene *guidelines* erstellt haben[71], öffentlich bekannt zu machen. Sie kann von den Agenturen Berichte anfordern und ihnen konkrete Anweisungen zur Verbesserung ihrer Tätigkeit erteilen.[72] Letztlich ist sie sogar befugt, die Akkreditierung zurückzunehmen[73], wobei es der DSK vorgeschrieben ist, ebendiesen Umstand auch öffentlich bekannt zu machen.

2. Aufsicht durch Datenschutzagenturen des Privatsektors

Privatrechtliche Datenschutzorganisationen sind dafür gedacht, sich freiwillig mitgliedschaftlich zu organisieren. Sie werden durch die Kommission zertifiziert und der Aufgaben-, Rechte- und Pflichtenkatalog ist ihnen durch die DSK vorgegeben. Sie werden in Anwendung der ihnen gewährten Befugnisse und auferlegten Pflichten neben und in Unterstützung der DSK tätig.

Die Agenturen können körperschaftlich organisiert sein, müssen das aber nicht.[74] Als Mitglieder sieht das GSpI in Art. 51 vor, dass diese Verwender i. S. d. Gesetzes sind (sich also Verwender zusammengeschlossen haben) – entweder als konstitutive Mitglieder der Agentur oder als assoziierte Mitglieder.[75] Die Organisation muss bei der DSK einen Antrag auf Zulassung stellen.[76] Dabei ist ihr durch Leitlinien der DSK auferlegt, gewissermaßen als Zweckbestimmung anzugeben und in ihren Statuten aufzuführen, dass sie es sich „zur Aufgabe macht“, drei im GSpI ausdrücklich benannte „Dienste zu leisten“, die direkt im Zusammenhang mit dem Schutz persönlicher Daten durch Verwender stehen. Ist der Antrag erfolgreich, kann sie eine Akkreditierung durch die DSK erreichen.

---

69 So der revidierte Art. 42 Abs. 4 GSpI 2020. Dahin gehend darf man die im sozioökonomischen Umfeld Japans vorhandene und im Vergleich mit Europa eher als extrem zu bezeichnende Stigmatisierungswirkung solcher namentlichen Benennung von Unternehmen durch staatliche Stellen wie auch in den Medien nicht unterschätzen.

70 Art. 47 Abs. 3.

71 Art. 53 Abs. 3.

72 Artt. 56, 57.

73 Art. 58 Abs. 1.

74 Vgl. Art. 47 Abs. 1, der festlegt, dass eine personenrechtliche Vereinigung dann einen Vertreter zu bestellen und zu benennen hat.

75 対象事業者 *taishō jigyō-sha*.

76 Art. 47 Abs. 2.

Die in Art. 47 Abs. 1 aufgeführten Aufgabenkreise bestehen einerseits darin, die Aktivitäten rund um die Behandlung von Beschwerden, welche Betroffene nach Art. 52 erhoben haben, näher zu regeln. Andererseits soll Agenturmitgliedern Informationen betreffend alle Dinge, welche im Zusammenhang mit konkreten datenschutzrechtlichen Fragestellungen stehen, und generell darüber hinaus „den Agenturmitgliedern die notwendigen Dienste anzubieten“ vermittelt werden, damit diese ihren Pflichten zum Schutz persönlicher Informationen korrekt nachkommen können.

Eine Aufgabenbeschreibung dahin gehend, auf welche Weise die Agentur in selbstkontrollierender Art gegenüber Verwendern aufzutreten und zu handeln hat, findet sich in Art. 52 Abs. 1 näher erläutert. Dort ist als eine zwingende Bestimmung formuliert, dass die Agentur bei Beschwerden den Betroffenen (also den Beschwerdeführern) Konsultation anbieten und ihnen notwendige Ratschläge erteilen soll. Dass sie sodann Tatsachenfeststellungen bezüglich der Beschwerde treffen und den Beschwerdegegner (d.h. den Verwender) von dem Inhalt der Beschwerde informieren und von diesem eine schnelle Lösung verlangen kann. Die Agentur kann weiterhin nach Abs. 2, wenn sie denn eine Notwendigkeit zum Handeln festgestellt hat, von dem von der Beschwerde betroffenen Verwender mündliche oder schriftliche Erklärungen, zusammen mit der Vorlage von sachverhaltsklärenden Unterlagen, fordern.

V. AUSBLICK

Ganz im Gegensatz zu früheren Zeiten[77], als Darstellungen zu eher begrenzten Rechtsgebieten des japanischen Rechts für eine zwar überschaubare, aber eher längere Geltungsdauer gut waren, ist zu erwarten, dass der nächste Bericht über Datenschutzrecht in Japan eher früher als später notwendig werden wird. Beziehungsweise mindestens eine Aktualisierung. Das ist schon beim Abfassen dieser Abhandlung offenbar geworden. Denn wie dargestellt hat sich die Datenschutzkommission selbst als Ziel auferlegt, in für Japan sehr kurzen Abständen neue Denk- und Regelungsansätze zu schaffen. Sei es, um bestehende oder neu aufkommende Problemkreise zu erfassen.[78] Oder qua der ihr, der DSK, gewährten Regelungskompetenz solche entweder im Weg von revidierten Leitlinien zu regeln – oder aber, um dem Gesetzgeber durch konkrete Vorschläge bei der Rechtsentwicklung zur Hand zu gehen.

---

77 Man denke an die 80er- oder 90er-Jahre hinsichtlich der sich hinschleppenden gesetzgeberischen Aktivitäten (oder der Rechts- und Rechtsprechungsentwicklung) z.B. im Umwelt- oder Bankrecht.

78 So die noch ausstehende Lösung betreffend die Einfügung in das pazifisch-asiatische datenschützende Regime im Rahmen der APEC-Gemeinschaft.

Anders als in Europa, wo sich die Diskussion um den Datenschutz nach der DSGVO und ersten Erfahrungen mit dieser eher beruhigt hat, wird die Rechtsentwicklung in Japan noch durch kurzfristig sich ereignende Entwicklungen gehen.

Der Autor wagt sogar die Vorhersage, dass Japan sich womöglich progressiv auf eine inzwischen zwar international schon reichlich diskutierte, aber derzeit noch recht unreife und heutigen Gedankenansätzen diametral gegenüberstehende Lösung für den Schutz von persönlichen Daten hinbewegen wird.

Diskutiert werden derzeit mehrere Ansätze. Hingewiesen sei hier auf zwei schon ernsthaft diskutierte Vorschläge. Das ist einmal die Einrichtung eines Systems, in dem es Betroffene selbst in der Hand haben, welche Daten wem zugänglich gemacht werden dürfen. Das System würde Datensubjekten als eine Softwarelösung zur Verfügung gestellt. Einzig und allein die dort von ihnen selbst eingestellten Daten würden im Einzelfall herausgegeben oder auf Anfrage oder Antrag „freigegeben" werden. Ein zweiter Gedankenansatz, dem derzeit vermehrt Chancen eingeräumt werden, scheint die Einrichtung und Unterhaltung einer Daten-Bank (oder besser „Bank für Daten"), japanisch 情報銀行 *jōhō ginkō*, zu sein. Daten würden dabei einem privatwirtschaftlich organisierten Unternehmen als Diensteanbieter auf vertraglicher Basis zur Verfügung gestellt. Unterschiedliche (gedacht ist an vier bis fünf) Einzelkategorien von Daten würden von den Datensubjekten dabei von Beginn an eingestuft, das reicht dann von „freien Daten" (z. B. jederzeit und an jedermann frei weiterzugeben) bis hin zu einer Kategorie „nur nach persönlich im Einzelfall einzuholender Genehmigung weitergebbar". Beide vorgenannten Systeme würden auch bestehende Sonder- oder ausschließliche Zugriffsrechte für staatliche Stellen erfassen und regeln können.

Wie gesagt, an dem Themenkreis Datenschutz in Japan interessierte Leser dürfen sich wohl eher früher als später auf eine aktualisierte Darstellung einstellen.

ZUSAMMENFASSUNG

Vom ersten, etwas „zahnlosen" Datenschutzgesetz aus dem Jahr 2003 (in Kraft getreten 2005) bis zu der hier geschilderten Rechtslage im Jahr 2022 ist eine ganze Reihe von Jahren ins Land gegangen. Was weder für Japan noch hinsichtlich anderer Länder speziell erstaunt. Bedingt durch offenbar gewordene, dann vermehrt in den Medien angeprangerte akute Probleme im Umgang mit persönlichen Daten und eine darauf folgende lebhafte gesellschaftliche Diskussion kam schließlich Bewegung in die Gesetzgebung. Nicht unterschätzt werden darf dabei aber, dass stärker verbraucherschützende legislative Maßnahmen in

wichtigen Handelspartnerländern Japans, insbesondere in der Form der europäischen DSGVO, verstärkend bzw. beschleunigend zu einer umfassenden Revision hin zu einem wirklich effektiven Datenschutzgesetz geführt haben.

Diese Abhandlung stellt in konzentrierter Form die wichtigsten Aspekte zum japanischen Datenschutzregime des neu aufgenommenen Kapitels „Datenschutz" des Autors für die Neuauflage des „Handbuch Japanisches Handels- und Wirtschaftsrecht" dar, das sich derzeit in der Endredaktion befindet. Aufgezeigt wird die Entwicklung von jenem ersten Datenschutzgesetz bis zu der inzwischen schon wieder in revidierter Form seit Mitte 2022 in Kraft befindlichen geltenden Fassung, mithin das hier so genannte GSpI 2020.

Japan hat sich bemüht, regelungsmäßig alles in einem einzigen Gesetzeswerk unterzubringen, was fast gelungen ist. Und was zumindest mit der geltenden Fassung dazu geführt hat, dass man Japan ein am internationalen Standard gemessen nun recht effektives Regime betreffend Datenschutz (i.S.v. Schutz persönlicher Daten) bescheinigen kann. Die genannte Einschränkung des „fast" Gelingens bezieht sich auf die Tatsache, dass die absolute Mehrzahl der Detailvorschriften sich nicht im Gesetzestext selbst findet, sondern in einer relativ großen Zahl von umfangreichen und sehr technisch formulierten Leitlinien (guidelines).

Folgend auf eine Darstellung der Struktur des GSpI und Einzelhinweise zu den für die Praxis so wichtigen guidelines and anderen Verwaltungsanweisungen wird etwas detaillierter auf einige wichtige Begriffsbestimmungen von Datenkategorien eingegangen, wobei einige im Wortlaut in deutscher Übertragung angeboten werden. Daran schließen sich Ausführungen zu den „Verwendern" von Daten auferlegten Pflichten einerseits und jenen den Datensubjekten eingeräumten Rechten andererseits an. Die Problematik und gesetzliche Erfassung von grenzüberschreitenden Datenversendungen und ein Kurzüberblick über die strafrechtliche Erfassung und Ahndung von Rechtsverletzungen folgen. Um eine Darstellung des Datenschutzregimes von Japan abzurunden, findet sich abschließend eine Schilderung der Struktur, Aufgaben und Kompetenzen der japanischen Datenschutzkommission einerseits und (mehreren) der im Weg eines „soft law approach" eingerichteten, von der Datenschutzkommission akkreditierten und von dieser überwachten Datenschutzorganisationen des Privatsektors andererseits, denen als Quasi-Hilfsorgan für Verwender von Daten Pflichten auferlegt werden, die aber auch regulativ gegenüber ihren Mitgliedern tätig werden dürfen.

SUMMARY

Quite a few years had passed since the year 2005, i.e. from the coming into force of the initial Japanese Data Protection Act, which by some was described as having being rather 'toothless' – until the one as it stands now in its revised

version in effect since about mid-2022. This relatively long timespan was generally not too long when considering the past legislative development speed in Japan. However, due to an increasingly high number of cases widely covered in the media and an ensuing discussion in society about the negative effects on consumers, the legislative process received a push. While on the other hand the indirect pressure on Japan resulting from the introduction of a strong consumer-oriented data protection regime in the form of new laws and regulations (like the European GDPO) in some of the important trade partner countries likely may have accelerated the process even more.

This paper represents an abridged and adjusted version of the author's newly inserted chapter on Japan's personal data protection regime to be published in the forthcoming 2nd edition of the "Handbuch Japanisches Handels- und Wirtschaftsrecht". It shows the development from Japan's first data protection law via its first major 2017 revision until the recently already first revised version (within just 3+ years) of the current Personal Data Protection Act, herein referred to as GSpI.

The Japanese legislators aimed at bringing 'everything data protection' into one piece of an legislative act – in which they almost succeeded. As far as the latest version in effect since mid-2022 is concerned, one can say that Japan has now built a comprehensive and effective regime on the protection of personal data. The one slightly weakening point being that quite a large number of important regulatory matter finds detailed regulation in separate 'Guidelines' issued by the Data Protection Agency rather that in the Act itself.

Following a description of the structure of the GSpI and mention, to a limited detail, of the Guidelines and also other administrative regulations which can be and have been issued by the Data Protection Agency, the article provides German-language translations of some key definitions of what constitutes 'personal data' (or 'personal information') and other data categories, together with some elaboration on what actually is and can be regarded as 'personal data'. There follows a description of the main duties and obligations of data users on the one hand and the corresponding rights of data subjects on the other. A further part deals with the problems of cross-border transmission of data, the special requirements and the particular care that must be taken both by transmitters of data to overseas third parties and by these overseas recipients.

Finally, to provide a rounded picture of the Japanese data protection regime, the article closes with a description of the regulatory framework and the administration by the Japanese Data Protection Agency: its structure, aims and competences. And it describes the establishment, the function and the various forms of administrative tools it may administer and which had been granted to it by the Act.