Verschärfung der Datenschutzregelungen in Japan

In Japan fehlte es lange am Bewusstsein für Datenschutz. Inzwischen hat man den Schutz personenbezogener Daten verschärft und EU-spezifische Sonderregeln eingeführt.

Von Mikio Tanaka

Seit 1. Februar ist das EU-Japan Freihandelsabkommen in Kraft. Laut Prognosen könnten Import und Export zwischen den beiden Regionen, die zusammen ein Drittel der weltweiten Wirtschaftsleistung stemmen, um bis zu 30 Prozent zunehmen. Damit einhergehend steigt auch der Austausch von Daten, einschließlich persönlicher Daten. Zuletzt haben sowohl die EU als auch Japan den Schutz personenbezogener Daten verschärft. Allerdings gibt es grundlegende Unterschiede in der Einstellung zum Datenschutz in Japan und Europa und entsprechend in der Formulierung der Gesetze.

In Japan fehlte es lange am Bewusstsein, dass Privatpersonen ein Recht auf Schutz der Privatsphäre haben. Die Notwendigkeit, diese gesetzlich zu schützen, ergab sich erst nach einer Empfehlung der OECD 1980. Diese bezog sich sowohl auf den öffentlichen als auch auf den privaten Sektor und führte acht Jahre später zur Einführung von Datenschutzregelungen im öffentlichen Bereich. Im privaten Sektor dagegen verzögerte sich die Einführung, weil man Auswirkungen auf wirtschaftliche Aktivitäten befürchtete. Man beschränkte sich zunächst auf rechtlich unverbindliche Richtlinien der jeweils zuständigen Ministerien. Durch die Weiterentwicklung der Rechtsprechung in Japan wurde zwar ein gewisser Schutz der Privatsphäre gewährt, sie wurde jedoch nicht als grundlegendes Menschenrecht angesehen. Im Zuge der zunehmenden Vernetzung, Digitalisierung und Internationalisierung der Wirtschaft erkannte man in Japan jedoch die Notwenigkeit, mit internationalen Standards Schritt zu halten. So wurde 2003 das Gesetz zum Schutz der persönlichen Informationen (GSpI) eingeführt.

Das Ziel des GSpI ist es, die (datenbezogenen) Rechte des Einzelnen unter Berücksichtigung der Nutzbarkeit der persönlichen Daten (§1) zu schützen. Dabei ist das Verhältnis zwischen Datennutzung und Schutz ausgewogen. Im GSpI des Jahres 2003 wurde noch der effektiven Nutzung der Daten ein größeres Gewicht als dem Schutz beigemessen. Entsprechend war es in Sachen Rechtsschutz noch in vielerlei Hinsicht unzulänglich:

- Unternehmen, die Daten von 5.000 oder weniger Personen verarbeiteten, waren ausgenommen
- Die Arten von „sensiblen" Informationen waren eingegrenzt
- Für den Erwerb von Daten von Dritten gab es nur eine abstrakte Bestimmung, die besagte, dass diese nicht unrechtmäßig erworben werden dürfen
- Die meisten wichtigen Leitlinien waren kompliziert und größtenteils nicht verbindlich; es gab kein einheitliches, mit starken Kompetenzen ausgestattetes Vollstreckungsorgan

2015 wurde das GSpI umfassend reformiert. Da die Industrie Zugriff auf gesammelte Daten benötigte, um sie als „Big Data" auszuwerten, hat man deren zustimmungslose Weitergabe an Dritte unter bestimmten Bedingungen ermöglicht, etwa durch Anonymisierung. Zugleich wurde aber der Schutz personenbezogener Daten verschärft. So gibt es keine Ausnahme mehr für relativ kleine Datenmengen. Bei der Weitergabe der Daten an Dritte – die betreffenden Personen müssen zustimmen, wenn die Daten nicht anonymisiert sind – sind die weiter-

Weitere wesentliche Unterschiede zwischen dem Gesetz zum Schutz der persönlichen Informationen (GSpI) und der Datenschutz-Grundverordnung (DSGVO):

	DSGVO (EU)	GSpI (Japan)
1) Rechtscharakter eines grundlegenden Menschenrechts?	Ja	Nein. Diese Tatsache dürfte Einfluss auf die unter 3) bis 5) genannten Unterschiede haben.
2) Räumlicher Anwendungsbereich	Anwendung auf Regionen außerhalb der EU möglich	Anwendung auf Regionen außerhalb Japans möglich
3) Freiheit des Widerrufs der Einwilligung	Klar formulierte Regelung	Keine klar formulierte Regelung
4) Recht auf Datenübertragbarkeit	Die betroffene Person hat unter bestimmten Umständen das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln (§20).	Das GSpI erkennt das Recht auf Datenübertragbarkeit nicht an. Ein solches Recht könnte ein Mittel werden, mit dem sich Privatpersonen zumindest in gewissem Maße den großen Informationsplattformen wie etwa Google oder Facebook widersetzen können.
5) Sanktionen	Bei Verstößen werden Geldbußen von bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes verhängt, je nachdem, welcher der Beträge höher ist (§83 Abs. 5). Diese theoretisch möglichen und extrem hohen Sanktionsmaximalbeträge haben auch in Japan zunächst eine stark abschreckende Wirkung entfaltet.	Die Weitergabe oder der Diebstahl personenbezogener Informationen zum Zweck der Erzielung illegaler Gewinne für sich selbst oder Dritte wird in Japan mit einer Freiheitstrafe mit Arbeitszwang von bis zu einem Jahr oder einer Geldstrafe von bis zu 500.000 Yen (ca. 4.200 Euro) geahndet (§83). Angesichts der üblichen Strafrechtspraxis in Japan ist allerdings schwer vorstellbar, dass diese Art von Verbrechen tatsächlich zu Freiheitsstrafen führen wird. Der Höchststrafbetrag von 4.200 Euro ist im Vergleich zur DSGVO sehr niedrig.

Quelle: Eigene Darstellung

gebende Partei und der Drittempfänger der Daten verpflichtet, die Namen der Beteiligten sowie den Nutzungszweck aufzuzeichnen und für eine bestimmte Zeit aufzubewahren, um die Rückverfolgbarkeit zu gewährleisten. Zur Überwachung gibt es nun eine staatliche Kommission.

In Europa hingegen gipfelte die EU-Datenschutzrichtlinie von 1995 schließlich in der für die EU einheitlich geltenden und verschärften Datenschutz-Grundverordnung (DSGVO, in Kraft seit 25. Mai 2018). Daraufhin wurde auch in Japan eine weitere Stärkung des GSpI erwogen. Damit das Schutzniveau von der EU-Kommission als „angemessen" im Sinne des §45 DSGVO anerkannt würde, hat Japan am 7. September 2018 EU-Zusatzvorschriften erlassen, die sich auf Informationen aus der EU beschränken. Die Anerkennung ist gegenseitig, so dass kein zusätzliches Verfahren nötig ist, wenn personenbezogene Daten aus der EU nach Japan oder umgekehrt übermittelt werden.

Wesentliche Eckpunkte der EU-Zusatzvorschriften:

(1) Daten zum Beispiel zur sexuellen Orientierung oder zur Mitgliedschaft in Gewerkschaften, die nicht unter „besonders sensible Informationen" des GSpI fallen, werden im Zusammenhang mit der EU als „besonders sensible Informationen" behandelt. Daher ist es grundsätzlich verboten, diese ohne vorherige Einwilligung des Betreffenden einzuholen. Bei einer Einwilligung gibt es jedoch keine Beschränkung hinsichtlich der Verwendung (§ 23 Abs. 2 GSpI). In diesem Punkt ist die Bestimmung der DSGVO (§ 9), die eine Verarbeitung sensibler personenbezogener Daten prinzipiell verbietet, immer noch strikter.

(2) „Im Besitz personenbezogener Informationen" gemäß GSpI bedeutet, dass der Datenverarbeitende befugt ist, Daten offenzulegen, inhaltlich zu korrigieren, zu ergänzen und zu löschen sowie die Nutzung und Weitergabe an Dritte einzustellen. Ausgenommen sind Daten, die öffentliches Interesse oder sonstige Rechte verletzten, oder Daten, die innerhalb von sechs Monaten gelöscht werden. In den EU-Zusatzvorschriften wird diese Sechsmonatsregelung jedoch aufgehoben, so dass solche Daten auch in Japan als personenbezogene Daten behandelt werden.

(3) Gemäß den EU-Zusatzvorschriften muss ein Datenverarbeitender bei der Weiterleitung von Daten aus der EU an Dritte außer Japan im Prinzip die Einwilligung der betroffenen Person für eine solche Weitergabe im Voraus einholen. ■

Mikio Tanaka
ist Partner und Rechtsanwalt mit japanischer Volljuristzulassung bei City-Yuwa Partners in Tokio.

E-Mail: mikio.tanaka@city-yuwa.com