Datenschutz beim Betrieb globaler Mitarbeiterdatenbanken

Japan hat sein Datenschutzgesetz im Mai 2017 reformiert, in Europa tritt eine neue Verordnung im Mai 2018 in Kraft. International tätige Unternehmen müssen dies berücksichtigen, wenn sie Mitarbeiterdaten verwalten.

Von Dr. Tobias Schiebe und Ulrich Kirchhoff, unter Mitwirkung von Takashi Yoneyama

Neben Kundendaten stellen Mitarbeiterdaten die am häufigsten von Unternehmen erhobenen und verarbeiteten personenbezogenen Daten dar. Multinationale Konzerne nutzen diese Daten nicht nur, um die Kommunikation zwischen den Gruppengesellschaften zu optimieren, sondern auch, um neue Personalentwicklungskonzepte anzubieten, zum Beispiel E-Learning-Plattformen oder Bonus- und Belohnungssysteme. Dabei sind je nach Land unterschiedliche Datenschutzregelungen zu beachten.

Das reformierte japanische Datenschutzrecht

Das im Mai 2017 grundlegend reformierte japanische Datenschutzgesetz (Act of Protection of Personal Information, APPI) beinhaltet keine Sondervorschriften für die Erhebung und Verarbeitung von Arbeitnehmerdaten. Allerdings wird die Auslegung der APPI-Vorschriften im Bereich der Mitarbeiterdaten durch eine Richtlinie des Ministeriums für Gesundheit, Arbeit und Soziales konkretisiert. Diese ist nicht rechtsverbindlich, wird aber in der Praxis befolgt.

Grundsätzlich gilt für die Verarbeitung von allgemeinen Mitarbeiterdaten, wie Name, Adresse und Geburtsdatum, dass keine Zustimmung erforderlich ist. Das Unternehmen muss den Mitarbeiter nur über den Verwendungszweck („Purpose of Use“) und die Art der genutzten Daten informieren. Die Daten dürfen aber ohne ausdrückliche Zustimmung weder über den Verwendungszweck hinaus verwendet noch an ein anderes Unternehmen übermittelt werden.

Besondere Regeln gelten für sensible personenbezogene Daten. Das sind alle Daten, die zu einer Diskriminierung des Arbeitnehmers führen könnten, zum Beispiel über Herkunft, Glauben, Gesundheit oder etwaige Vorstrafen. Diese dürfen nur mit vorheriger Zustimmung des Mitarbeiters eingeholt und verarbeitet werden.

Der Mitarbeiter muss auch vorher zustimmen, soweit allgemeine und sensible Mitarbeiterdaten an Konzernunternehmen im In- und Ausland übertragen werden sollen. Eine Ausnahme gilt, wenn das Unternehmen in Japan ansässig und als gemeinsamer Nutzer („Joint User“) im oben beschriebenen Verwendungszweck („Purpose of Use“) festgelegt ist. Ist die gemeinsame Nutzung nicht vorgesehen, können Unternehmen entweder aktiv den Mitarbeiter um Zustimmung bitten („Opt-in“) oder den Mitarbeiter vor der Übertragung über Details des Datentransfers informieren und ihm die Möglichkeit zum Widerspruch geben („Opt-out“).

Sitzen Gruppenunternehmen oder Datendienstleister, an die die Daten übertragen werden sollen, im Ausland,

müssen nach dem reformierten APPI die Mitarbeiter dem Datentransfer grundsätzlich vorher zustimmen. Dazu müssen sie über das Land, in dem der Empfänger ist, ausdrücklich vorab informiert werden.

Ist eine Zustimmung nicht einholbar, kann das Unternehmen alternativ mit dem Empfänger eine Vereinbarung schließen, wonach die Einhaltung des japanischen Datenschutzniveaus gewährleistet wird. Ein Datentransfer ins Ausland ist nur dann ohne Zustimmung und ohne Abschluss einer Datentransfervereinbarung möglich, soweit das die Daten empfangende Unternehmen in einem Land ansässig ist, das dem japanischen Datenschutzniveau entsprechende Regeln vorweisen kann. Bisher sind allerdings noch keine Länder, die aus Sicht Japans als „datensicher" gelten, bestimmt worden.

Neue EU-Datenschutzgrundverordnung ab Mai 2018

Die europäischen Datenschutzregelungen werden zum 25. Mai 2018 mit dem Inkrafttreten der Allgemeinen Datenschutzgrundverordnung (General Data Protection Regulation, GDPR) ebenfalls reformiert. Das Thema Arbeitnehmerdaten regelt die GDPR nicht explizit, sondern überlässt es den Mitgliedstaaten, dieses näher auszugestalten. Deutschland hat bereits am 5. Juli 2017 das neue Bundesdatenschutzgesetz („BDSG-neu") erlassen, welches die GDPR ergänzt, konkretisiert und modifiziert. Es tritt zeitgleich mit der GDPR in Kraft.

Nach den allgemeinen Vorgaben der europäischen GDPR ist die Verarbeitung von personenbezogenen Daten nur dann rechtmäßig, wenn ein gesetzlicher Rechtfertigungsgrund vorliegt oder der Mitarbeiter zugestimmt hat. Deutschland hat die möglichen Rechtfertigungsgründe in § 26 Abs. 1. S. 1 BDSG-neu konkretisiert. Danach dürfen personenbezogene Daten von Beschäftigten verarbeitet werden, soweit dies für die Begründung, die Durchführung oder die Beendigung des Beschäftigtenverhältnisses oder zur Interessensvertretung der Beschäftigten erforderlich ist.

Sowohl bei der Erhebung der personenbezogenen Daten beim Arbeitgeber als auch bei der Datenübertragung an die Gruppengesellschaften sind die Interessen des Arbeitgebers gegen die Interessen des betroffenen Arbeitnehmers abzuwägen. Während die Datenerhebung beim Arbeitgeber, etwa zur Dokumentation von Urlaubs- und Fehlzeiten, gerechtfertigt sein kann, ist die Übertragung dieser Daten auf weitere Gruppengesellschaften oft nicht erforderlich.

Prüfung bei Mitarbeiterdatenbanken

Anders als in Japan stellt die Zustimmung des Mitarbeiters zur Datenverarbeitung in Europa oft keine zuverlässige Rechtsgrundlage dar, da die hohen Anforderungen an eine rechtswirksame Zustimmung, wie an das Merkmal der Freiwilligkeit, oft nicht erfüllt werden. In einem Arbeitsverhältnis wird davon ausgegangen, dass der Arbeitnehmer geneigt ist, der Nutzung auch unfreiwillig zuzustimmen, um seinen Arbeitsplatz nicht zu gefährden. Die Freiwilligkeit der Zustimmung dürfte daher regelmäßig nur dann gegeben sein, wenn der Arbeitnehmer von der Datenerhebung profitiert, wie bei der Sammlung von Mitarbeiterdaten für eine Sonderzahlung.

Der Transfer von personenbezogenen Daten an Konzernunternehmen in Ländern außerhalb der EU ist zudem limitiert. Wenn es sich nicht um ein von der EU anerkanntes Drittland handelt, ist es grundsätzlich erforderlich – ähnlich wie nach den japanischen Vorschriften – die Zustimmung des Arbeitnehmers zu dem Datentransfer zu erlangen. Alternativ muss das Unternehmen ein adäquates Datenschutzniveau beim Empfänger auf andere Weise sicherstellen, etwa durch die Verwendung von EU-Standardvertragsklauseln oder „Binding Corporate Rules". Japan wird derzeit noch nicht als sicheres Drittland von der EU anerkannt. Im Sommer dieses Jahres haben sich die EU und Japan aber auf einen gemeinsamen Dialog verständigt, um dieses Ziel bald zu erreichen. Mit einer Entscheidung ist frühestens im ersten Quartal 2018 zu rechnen.

Lokalisierung oder Best Practice

Globale Mitarbeiterdatenbanken, die Daten von Mitarbeitern in Japan und der EU enthalten, sind vor dem Hintergrund der Datenschutzreformen in der EU und Japan auf den Prüfstand zu stellen. Datenschutzrichtlinien und betriebliche Praktiken sind dabei dem jeweiligen Recht anzupassen. Dies gilt insbesondere mit Blick auf die EU dahingehend, dass die Zustimmung des Mitarbeiters nach den EU-Regeln oftmals keine wirksame Rechtsgrundlage darstellt. Eine Alternative zur Lokalisierung kann die Aufstellung einer an der GDPR orientierten, konzernweiten Datenschutzrichtlinie als Best Practice darstellen. Durch einen hohen Datenschutzstandard könnte sich ein Konzern damit auch von Wettbewerbern absetzen. Aus praktischer Sicht empfiehlt es sich in jedem Fall, die in Datenbanken eingestellten Mitarbeiterdaten auf tatsächlich notwendige Daten zu beschränken. Daten für statistische Zwecke sollten anonymisiert werden. ■

Dr. Tobias Schiebe
ist deutscher Rechtsanwalt und registrierter Foreign Attorney bei ARQIS Foreign Law Office Foreign Law Joint Enterprise with TMI Associates in Tokyo.

E-Mail: tobias.schiebe@arqis.com
www.arqis.com