Datenpannen in Japan: Meldepflicht und Schadensbegrenzung

Seit 2022 sieht Japan im Fall von Verletzungen des Schutzes personenbezogener Daten per Gesetz die Erstellung eines detaillierten Meldeberichts an die Aufsichtsbehörde vor. Dabei sind knappe Fristen zu beachten.

Von Sayako Tsukamoto und Kanako Inokuchi

Seit dem 1. April 2022 ist in Japan das novellierte Gesetz über den Schutz personenbezogener Daten in Kraft. Es enthält eine Klausel, die vorschreibt, dass in Fällen, in denen ein erhebliches Risiko der Beeinträchtigung der Rechte und Interessen von Privatpersonen besteht, dies der Aufsichtsbehörde Personal Information Protection Commission (PPC) gemeldet werden muss. Außerdem ist die betroffene Person (Datensubjekt) zu benachrichtigen. Im Umgang mit Datenlecks wird zwar eigentlich nur ein „Überblick" über den Vorfall verlangt, doch in der Praxis sind detaillierte Angaben erforderlich.

1. Verletzungen des Schutzes personenbezogener Daten

Als Verletzung des Schutzes personenbezogener Daten werden Situationen bezeichnet, die die Sicherheit personenbezogener Daten beeinträchtigen, etwa durch Weitergabe, Verlust oder Schädigung von Daten. Ein typisches Beispiel ist der Versand von Dokumenten und Nachrichten an die falsche E-Mail-Adresse. Problematisch ist außerdem, wenn Daten im Internet einsehbar sind, wenn Datenträger gestohlen werden, oder wenn sich jemand unbefugt Zugang zu Daten beschafft und diese stiehlt. Laut dem PPC-Jahresbericht 2022 betrafen 95,1 Prozent aller gemeldeten Verletzungen Daten in Papierform.

2. Meldung an die PPC

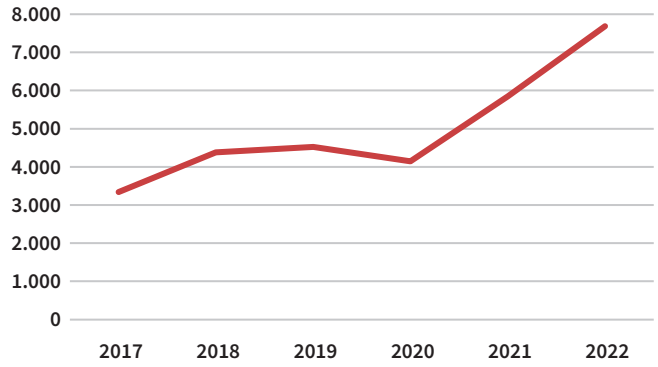
Die Meldepflicht von Datenlecks umfasst auch solche Fälle, in denen eine Datenverletzung noch nicht bestätigt wurde, aber das Risiko besteht, dass eine Datenpanne auftrat. Es werden folgende vier Kategorien von meldepflichtigen Datenschutzverletzungen unterschieden:

Kategorie 1: Sie betreffen sensible Informationen.
Kategorie 2: Es besteht das Risiko, dass eine unbefugte Nutzung der Daten Vermögensschäden für die betroffenen Personen (Datensubjekte) verursacht.
Kategorie 3: Es ist zu befürchten, dass die Verletzung des Datenschutzes mit unlauteren Absichten begangen wurde.
Kategorie 4: Mehr als 1.000 Datensubjekte sind betroffen.

Der Meldebericht muss folgende Informationen enthalten:
- Überblick über die Datenschutzverletzung
- Von der Datenverletzung betroffene personenbezogene Daten
- Anzahl der betroffenen Datenobjekte
- Ursache der Datenpanne
- Vorhandensein eines Folgeschadens oder Gefahr eines Folgeschadens
- Stand der Umsetzung der Maßnahmen zugunsten der Datensubjekte (einschließlich deren Benachrichtigung)
- Stand der Umsetzung der Veröffentlichung (falls die direkte Kontaktaufnahme fehlschlägt, zum Beispiel durch Veröffentlichung im Internet)
- Maßnahmen zur Vermeidung ähnlicher Fälle in der Zukunft

Grundsätzlich ist zweimal Meldung zu erstatten – zunächst ein vorläufiger, danach ein endgültiger Bericht. Die vorläufige Mel-

Anzahl der an die Aufsichtsbehörde gemeldeten Datenlecks



Quelle: Eigene Darstellung auf Grundlage der PPC-Jahresberichte 2017-2022

dung muss innerhalb von drei bis fünf Tagen nach Bekanntwerden der Datenschutzverletzung erfolgen. Sachverhalte, die zum Zeitpunkt der vorläufigen Meldung noch nicht bekannt sind, unklar sind oder noch nicht behandelt wurden, müssen nicht aufgeführt werden.

Der Endbericht muss grundsätzlich innerhalb von 30 Tagen (oder innerhalb von 60 Tagen im Fall von Kategorie 3) nach Bekanntwerden der Datenschutzverletzung eingereicht werden. Er muss alle genannten Aspekte enthalten. Die Fristen werden streng gehandhabt. Bei Nichteinhaltung kann die PPC entsprechende Anweisungen oder Empfehlungen geben oder Korrekturmaßnahmen anordnen. Bei meldepflichtigen Datenschutzverletzungen sind die Datensubjekte grundsätzlich zu benachrichtigen.

3. Praktischer Umgang mit Datenschutzverletzungen

1) Meldung an die verantwortlichen Personen

Fehlgeleitete Dokumente oder E-Mails gehören zum Alltag. Wenn jedoch die Person, der der Fehler unterlaufen ist, nichts unternimmt, ist das Unternehmen nicht in der Lage, den Vorfall zu erfassen. Dann besteht die Gefahr, dass das Unternehmen, obwohl es meldepflichtig ist, keinen Bericht an die PPC erstattet. Daher ist es – unabhängig vom Ausmaß der Datenverletzung – notwendig, dass jeder Fall den Verantwortlichen gemeldet wird, damit diese die nächsten Schritte einleiten können.

2) Untersuchung des Sachverhalts

Der Bericht an die PPC soll einen „Überblick" über den Vorfall geben. Tatsächlich handelt es sich aber mitnichten um einen oberflächlichen „Überblick", sondern eine detaillierte Darstellung des Sachverhalts. Dazu zählen die Personen, die die Datenschutzverletzung entdeckt haben, der Ursprung der Verletzung, der chronologische Hergang des Vorfalls und der Stand der Untersuchung durch externe Sachverständige wie Forensik-Dienstleister. Zu den Fakten, die so rasch wie möglich geklärt werden müssen, zählen die Daten, die verletzt wurden (ob die Datenverletzungen zum Beispiel sensible personenbezogene Daten enthielten) sowie die Anzahl der betroffenen Personen (ob mehr als 1.000 Personen betroffen waren), da diese Informationen auch für die Entscheidung erforderlich sind, ob der Vorfall meldepflichtig ist.

3) Ermittlung der Ursache

In der Meldung an die PPC muss die Ursache der Datenschutzverletzung im Detail erläutert werden. Die Ermittlung der Ursache hängt letztlich mit der Ableitung von Maßnahmen zur künftigen Vermeidung ähnlicher Fälle zusammen. Daher sollte die Ermittlung konkret und präzise erfolgen. Sinnvoll ist es auch, die Unterstützung durch externe Experten in Anspruch zu nehmen.

4) Prüfung und Umsetzung von Maßnahmen zur Verhinderung erneuter Verstöße

Die PPC verlangt, dass der Bericht nicht nur konkrete Maßnahmen zur künftigen Vermeidung von Datenlecks beschreibt, sondern auch einen Zeitplan für die Umsetzung und den voraussichtlichen Abschluss der Maßnahmen enthält. Daher müssen konkret umsetzbare Maßnahmen zur Verhinderung erneuter Vorfälle ausgearbeitet werden.

5) Maßnahmen zur Verhinderung der Schadensausbreitung

Tritt eine Datenpanne auf, gilt es so rasch wie möglich Maßnahmen zur Schadensbegrenzung zu ergreifen. Breitet sich das Problem aus, schadet dies dem Ruf des Unternehmens. Die Identifizierung möglicher Folgeschäden ist in dem Zusammenhang ebenfalls wichtig.

4. Erstellung eines Reaktionsplans

Einhergehend mit der Einführung der Meldepflicht an die PPC wurden detaillierte Richtlinien und Formulare für die Berichte geschaffen. Es hat sich jedoch gezeigt, dass es sich aufgrund der geforderten Angaben und zeitlichen Fristen schwierig gestaltet, angemessen mit Datenschutzverletzungen umzugehen, wenn man erst aktiv wird, nachdem eine Verletzung eingetreten ist.

Um rasch reagieren zu können, müssen Unternehmen auch in Japan – ähnlich wie unter der deutschen Datenschutz-Grundverordnung – personell, organisatorisch und technisch entsprechend aufgestellt sein. Dazu gehören auch Schulungen. Es ist wichtig, eine Liste mit externen Experten für die technische Unterstützung und von externen Rechtsanwälten für die Rechtsberatung zu erstellen, und darauf basierend einen umfassenden Reaktionsplan zu erarbeiten. ■

Sayako Tsukamoto
ist Partnerin und Rechtsanwältin mit japanischer Volljuristzulassung bei City-Yuwa Partners in Tokio.

✉ sayako.tsukamoto@city-yuwa.com

Kanako Inokuchi
ist Rechtsanwältin mit Spezialisierung auf Datenschutz und geistiges Eigentum in Japan.

✉ kanako.inokuchi@city-yuwa.com