Doppelte Meldepflicht bei Datenschutzpannen eines Auftragsverarbeiters?

Sehr geehrte Datenschutz-Kunden,

das Thema Auftragsverarbeitung war bereits mehrfach Bestandteil meiner Kundeninformation und Dauerthema bei meinen Datenschutzberatungen. Warum wende ich mich nun abermals an Sie? Leider gibt es immer wieder Unklarheiten, was der simple Satz bedeutet: DER VERANTWORTLICHE BLEIBT AUCH FÜR ALLE VERARBEITUNGSVORGÄNGE DES VON IHM BEAUFTRAGTEN AUFTRAGSVERARBEITERS VERANTWORTLICH. Das persönliche Rechtsempfinden ("Ist doch nicht unsere Schuld, wenn die ...", "Was können wir dafür, dass bei unserem Dienstleister ..." etc.) ist an dieser Stelle nicht gefragt.

Heute geht es um einen Aspekt (von vielen), was "Verantwortlichkeit" bedeutet: Nämlich um die Meldepflicht von Datenschutzpannen bei der zuständigen Aufsichtsbehörde. Art. 33 EU-DSGVO sieht hierfür eine eindeutige Meldekette vor: Der Auftragsverarbeiter meldet dem Verantwortlichen (also seinem Auftraggeber), dieser meldet an die Aufsichtsbehörde. Ist die Datenschutzpanne bei einem Subunternehmer des Auftragsverarbeiters passiert, so verlängert sich die Meldekette entsprechend.

Ein aktueller Fall

In meinem aktuellen Beispielfall wurde ein Dienstleister für die Verbrauchserfassung und -abrechnung für Heizung und Warmwasser Opfer eines sogenannten Hackerangriffs (eventuell haben Sie in den Medien hierüber bereits Kenntnis erlangt). Der Dienstleister ist als Auftragsverarbeiter für eine Vielzahl von Haus- und Immobilienverwaltungen in Deutschland, aber auch über die Staatsgrenze hinaus, tätig. Und es liegt natürlich in der Natur eines solchen Angriffs, dass bestimmte Details erst nach genauer Analyse des Angriffsszenarios, der (mutmaßlich) betroffenen Personengruppe, der (mutmaßlich) abgegriffenen Datenkategorien und etlicher technischer Details ermittelt werden können. Der Auftragsverarbeiter hat sich dafür entschieden, den Vorfall zeitnah der für seinen Firmensitz zuständigen Aufsichtsbehörde zu melden und die gewonnenen Erkenntnisse dieser zur Verfügung zu stellen. Parallel wurde durch den Auftragsverarbeiter Anzeige erstattet, so dass auch Fachleute von Strafverfolgungsbehörden ihre Kompetenz einbringen können. Damit kein falsches Bild entsteht: Natürlich wurden auch die Auftraggeber informiert. Wie zeitnah und vollständig entzieht sich meiner Kenntnis, aber ich gehe positiv davon aus, dass die zu diesem Zeitpunkt vorliegenden Erkenntnisse vollumfänglich und korrekt weitergereicht wurden.

...

Volker Baron (Dipl.-Geograph / IT-Systemelektroniker) – **Tel.:** +49 89 18923500 – **Fax:** +49 89 18923501
Büro: Haydnstraße 2, 80336 München – **E-Mail:** volker.baron@baron-consult.de – **Internet:** www.baron-consult.de
Finanzamt München I, USt-ID: DE 216791626
Bankverbindung: Münchner Bank eG, IBAN: DE84 7019 0000 0000 3389 15, BIC: GENODEF1M01

Muss vom Verantwortlichen dann nochmals gemeldet werden?

Als Datenschutzbeauftragter (in diesem Fall nicht des Dienstleisters ...) kenne ich natürlich die Meldekette des Art. 33 EU-DSGVO, als verantwortungsbewusster Datenschutzbeauftragter habe ich mir aber durchaus die Frage gestellt, ob eine zusätzliche Meldung von jedem einzelnen Auftraggeber Sinn macht. Zeit also, mal wieder mit dem Beratungsteam des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) zu diskutieren. Meine Argumente gegen eine zusätzliche Meldepflicht können auch Sie sicher nachvollziehen:

1. Im vorliegenden Fall wurde die Datenschutzpanne der für den Firmensitz des Auftragsverarbeiters zuständigen Aufsichtsbehörde gemeldet. Die Auftraggeber sind aber über das gesamte Bundesgebiet verteilt, so dass bei Einhaltung der Meldekette 16 verschiedene Aufsichtsbehörden involviert wären.
2. Selbst wenn die zuständige Aufsichtsbehörde dieselbe wäre würde ein erheblicher Mehraufwand für die Behörde entstehen, wenn jeder Auftraggeber [des Abrechnungsdienstleisters] die Meldung durchführen würde und diese Meldungen getrennt abgearbeitet werden müssten.
3. Da im vorliegenden Fall unterschiedliche Aufsichtsbehörden involviert wären würde die Koordination der Bearbeitung erschwert, da die einzelne Behörde jeweils nur über einen Teil der Sachverhalte zur Datenschutzpanne informiert wäre, nämlich über den Teil, der den einzelnen Verantwortlichen betrifft. Der Auftragsverarbeiter selbst ist gegebenenfalls der bessere Ansprechpartner, weil er über die meisten Informationen zum Vorfall verfügt.

Die Antwort ist eindeutig

Soeben habe ich die sehr ausführliche Antwort des BayLDA erhalten (den vollständigen Text der Antwort habe ich Ihnen in der Fußnote bereitgestellt[1])):

"...
'Muss der Verantwortliche jetzt den gleichen Vorfall nochmals an die Aufsichtsbehörde melden?'
Ja, jeder Verantwortliche nach DS-GVO hat eine Datenschutzverletzung der zuständigen Datenschutzaufsichtsbehörde zu melden, wenn die bekannten Voraussetzungen aus Art. 33 DS-GVO erfüllt sind. Eine Meldung eines Auftragsverarbeiters ersetzt nicht die Meldung eines Verantwortlichen. Ein solcher Dienstleiser verarbeitet die Daten schließlich nur im Auftrag, sodass eine Risikobewertung tatsächlich nur vom Verantwortlichen durchgeführt werden kann, da dieser die Verantwortung über die Datenverarbeitung mit allen Konsequenzen (sowohl sicherheitstechnisch als auch rechtlich) weiterhin besitzt. Sollte es bei einem Auftragsverarbeiter zu einem Vorfall kommen, hat dieser die Informationen darüber entsprechend an den Verantwortlichen weiterzureichen, damit dieser seiner eigenen Dokumentations- und Meldeverpflichtungen nachkommen kann. ..."

In den weiteren Ausführungen bestätigt das BayLDA die "enormen Personalengpässe in unserer Behörde", legt aber zugleich dar, dass es nicht unüblich ist, "dass beim BayLDA viele Meldungen eingehen, die sich auf den gleichen Sachverhalt beziehen (z. B. Sicherheitsvorfall bei Auftragsverarbeiter, Supply-Chain-Attacke, Schwachstelle in Standardsoftware)." Auch für die länderübergreifende Verarbeitung von Vorfällen bestünden geeignete Verfahren. Von der Meldeverpflichtung des Verantwortlichen kann daher in keinem Fall abgewichen werden.

...

Was bedeutet das für Sie?

- Wählen Sie Ihre Auftragsverarbeiter sorgfältig aus. Machen Sie eine Aktennotiz, warum Sie sich für genau diesen Auftragsverarbeiter entschieden haben bzw. warum Sie zu dem Ergebnis gelangt sind, dass dieser für die Datenverarbeitung geeignet ist.
- Prüfen Sie, welche personenbezogenen Daten Sie dem Auftragsverarbeiter zur Verfügung stellen. Bedenken Sie hierbei den Grundsatz der Datensparsamkeit (Art. 5 Abs. 1 c EU-DSGVO)
- Schließen Sie mit dem Auftragsverarbeiter vor der ersten Weitergabe personenbezogener Daten einen vollständigen und rechtskonformen Vertrag zur Auftragsverarbeitung ab. Von vielen (größeren bzw. international operierenden) Auftragsverarbeitern wird ein solches "Rechtsinstrument" nur in Form einer einseitigen Willenserklärung bereitgestellt. Prüfen Sie in diesen Fällen, wie Sie davon Kenntnis erlangen, wenn die Willenserklärung einseitig geändert wird.
- Prüfen Sie bitte, ob für alle Ihre Dienstleister im Bereich Datenverarbeitung ein Vertrag zur Auftragsverarbeitung vorliegt, sofern diese nicht aufgrund ihres Berufsstandes oder ihrer Tätigkeiten selbst zum Verantwortlichen werden.
- Wird Ihnen eine Datenschutzpanne bei einem Ihrer Auftragsverarbeiter bekannt, so prüfen sie deren Meldepflicht unverzüglich. Dies gilt auch, wenn Sie nicht durch den Auftragsverarbeiter, sondern durch Dritte vom Vorfall Kenntnis erlangt haben. Liegt ein meldepflichtiger Vorfall vor, so informieren Sie die Aufsichtsbehörde innerhalt der nach Art. 33 EU-DSGVO vorgesehenen Frist (72 Stunden). Bitte beachten Sie, dass bereits ein „Risiko für die Rechte und Freiheiten natürlicher Personen“ die Meldepflicht auslöst. Ein hohes Risiko, wie es für andere Maßnahmen vorliegen muss, ist für die Meldepflicht nicht erforderlich.

Ein Vertrag zur Auftragsverarbeitung muss eine hohe Zahl an Mindestanforderungen erfüllen. Für meine Datenschutz-Kunden ist die Prüfung von solchen (deutschsprachigen) Verträgen in den Kosten meiner Bestellung enthalten. Bitte beachten Sie jedoch, dass die sorgfältige Bearbeitung Zeit benötigt und eine Rückantwort gegebenenfalls erst innerhalb einer Woche erfolgen kann.

Für Rückfragen stehe ich Ihnen wie immer gerne zur Verfügung.

München, 2022-09-22

Volker Baron

1) Antwort des BayLDA auf meine Anfrage:

Beratung nach Art. 57 Datenschutz-Grundverordnung (DS-GVO)
Aktenzeichen: LDA-1085.4-7313/22-T
Online-Kennung: 267D40AD

Sehr geehrter Herr Baron,
sehr geehrte Damen und Herren,

Sie haben kürzlich bei unserer Behörde eine Beratungsanfrage zum Thema „Meldeverpflichtung bei einer Datenschutzverletzung“ eingereicht, die wir unter dem Aktenzeichen LDA-1085.4-7313/22-T führen.

Ihrer Beschreibung nach beschäftigen Sie sich als externer Datenschutzbeauftragter derzeit intensiv mit einem Sicherheitsvorfall, der sich bei einem Auftragsverarbeiter ... ereignet hat. Die von Ihnen dargestellten Punkte sind aus pragmatischen Gründen sehr gut nachvollziehbar, spiegeln jedoch nicht die Meldeverpflichtungen im Sinne der DS-GVO wider.

Folgendes wollen wir Ihnen zu Ihren Fragen bzw. Ihren Gedanken mitteilen:
„Muss der Verantwortliche jetzt den gleichen Vorfall nochmals an die Aufsichtsbehörde melden?“
Ja, jeder Verantwortliche nach DS-GVO hat eine Datenschutzverletzung der zuständigen Datenschutzaufsichtsbehörde zu melden, wenn die bekannten Voraussetzungen aus Art. 33 DS-GVO erfüllt sind. Eine Meldung eines Auftragsverarbeiters ersetzt nicht die Meldung eines Verantwortlichen. Ein solcher Dienstleiser verarbeitet die Daten schließlich nur im Auftrag, sodass eine Risikobewertung tatsächlich nur vom Verantwortlichen durchgeführt werden kann, da dieser die Verantwortung über die Datenverarbeitung mit allen Konsequenzen (sowohl sicherheitstechnisch als auch rechtlich) weiterhin besitzt. Sollte es bei einem Auftragsverarbeiter zu einem Vorfall kommen, hat dieser die Informationen darüber entsprechend an den Verantwortlichen weiterzureichen, damit dieser seiner eigenen Dokumentations- und Meldeverpflichtungen nachkommen kann (siehe Ihr Punkt 1).

Zu Ihrem Punkt 2: Es ist korrekt, dass eine hohe Anzahl an Meldungen einen sehr hohen Aufwand für die Aufsichtsbehörden darstellt. Jedoch lässt sich dieses Problem nicht so einfach lösen, da ein Auftragsverarbeiter schließlich nicht pauschal für alle seine Auftraggeber (= Verantwortliche) melden kann. Entsprechend ist es nicht unüblich, dass beim BayLDA viele Meldungen eingehen, die sich auf den gleichen Sachverhalt beziehen (z. B. Sicherheitsvorfall bei Auftragsverarbeiter, Supply-Chain-Attacke, Schwachstelle in Standardsoftware).

Zu Ihrem Punkt 3: Da das Szenario „Sicherheitsvorfall bei Auftragsverarbeiter“ nicht selten ist, bestehen bereits Prozesse zum länderübergreifenden Austausch, sofern dies erforderlich ist. Bei einzelnen Meldungen bayerischer Verantwortlicher, die beim BayLDA dazu eingehen, ist es jedoch meistens nicht notwendig, einen solchen Austausch durchzuführen, da ja jeder Verantwortliche im Rahmen seiner Meldung beim BayLDA die erforderlichen Informationen zur Verfügung stellt, die eine datenschutzrechtliche Bewertung zulassen.

Im Ergebnis fassen wir zusammen, dass eine Meldung eines Auftragsverarbeiters nicht die eines Verantwortlichen ersetzt. Im konkreten Fall wissen wir, dass beim Abrechnungsdienstleister ... nicht wenige Auftraggeber von dieser Meldeverpflichtung berührt sein dürften. Aufgrund der bereits von uns durchgeführten allgemeinen Bewertung des Sachverhalts und der gleichzeitigen enormen Personalengpässen in unserer Behörde ist davon auszugehen, dass weitere eingehende Meldungen von Verantwortlichen, die sich genau auf diesen Sachverhalt beziehen, zwar zeitnah gesichtet und bestätigt werden können, jedoch wohl keine detaillierte Prüfungen mehr dazu vorgenommen werden, sofern die Meldeangaben des Verantwortlichen dies zulassen (insbesondere nach der Risikobetrachtung).

Falls Sie für einen bayerischen Verantwortlichen eine Meldung einer Datenschutzverletzung einreichen wollen, können Sie dies unter www.lda.bayern.de/datenschutzverletzung durchführen. Wir betrachten Ihre Anfrage damit als abgeschlossen.

Mit freundlichen Grüßen

...
Referent Cybersicherheit
Bayerisches Landesamt für Datenschutzaufsicht, Promenade 18
91522 Ansbach