Keine Auswirkungen des Corona-Virus auf die Frist für die Meldung eines Data Breach

Grundsätzliches

Geschieht ein Data Breach, daher eine Verletzung des Schutzes personenbezogener Daten, gilt es für den Verantwortlichen der Datenverarbeitung **schnell zu reagieren**. Die Meldung an die Datenschutzbehörde hat **unverzüglich**, **möglichst binnen 72 Stunden nach Kenntnis von der Datenschutzverletzung** zu erfolgen (Art 33 Abs 1 DSGVO).

Ein derartiger **Data Breach** kann die **Verletzung der Vertraulichkeit, der Integrität** oder der **Verfügbarkeit von personenbezogenen Daten** sein.

Abhängig vom Risiko, welches mit dem **Data Breach** einhergeht, hat der Verantwortliche folgende **Maßnahmen** zu setzen:

- Bei **keinem Risiko** für die betroffene Person ist der Data Breach zu **dokumentieren** (Art 33 Abs 5 DSGVO),
- Bei einem **gegebenen Risiko** hat der Verantwortliche unverzüglich, möglichst binnen 72 Stunden diesen der Datenschutzbehörde **zu melden** (Art 33 DSGVO).
- Bei einem **hohen Risiko** für die betroffenen Personen hat der Verantwortliche sowohl eine **Meldung** an die Datenschutzbehörde (unverzüglich, möglichst binnen 72 Stunden) zu erstatten und die betroffenen Personen zu **informieren**.(Art 34 DSGVO)

Um ein „Gefühl“ dafür zu bekommen, welche Maßnahme zu setzen ist, wird auf folgenden Beitrag verweisen: https://www.dataprotect.at/data-breaches/

Änderungen durch das 2.COVID-19-Gesetzespaket

Im Rahmen des 2.COVID-19-Gesetzespaket wurde ein **umfassendes gesetzliches Fristen-Moratorium** für Zivilverfahren, strafgerichtliche Verfahren aber auch Verwaltungsverfahren beschlossen.

Fristen können nicht ablaufen (dh enden) und werden automatisch verlängert bzw. beginnen am **1. Mai 2020 neu zu laufen**.

Dieses beinhaltet unter anderem die **Unterbrechung von Fristen in gerichtlichen** Verfahren sowie auch die Unterbrechung von **Fristen in Verwaltungsverfahren**.

Nicht umfasst ist meiner Ansicht nach jedoch die **72 Stunden Frist** zur Meldung von Verletzungen des Schutzes personenbezogener Daten **gem Art 33 DSGVO**.

Im Verfahren vor der Datenschutzbehörde als **Verwaltungsbehörde** sind vor allem das AVG (Allgemeines Verwaltungsverfahrensgesetz) und das VStG (Verwaltungsstrafgesetz) anzuwenden; in beiden Gesetzn kommt es zur oben erwähnten Fristenhemmung.

Die **Frist** des **Art 33 Ab 1 DSGVO** ist jedoch von dieser **Fristenhemmung nicht betroffen**, da die DSGVO als **europäsche Norm** einen **Anwendungsvorrang** vor den nationalen Gesetzen (insbes. dem AVG) genießt.

Einfach gesagt:

Ein nationales Gesetz (COVID-19 Gesetz) kann eine europäische Verordnung nicht ändern und eine Öffnungsklausel zur Frist des Art 33 Abs 1 DSGVO gibt es nicht.

Unverzüglichkeit der Meldung

Entsprechend des Gesetzestextes (DSGVO) hat eine Meldung an die Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, zu geschehen. Ausdrücklich vorgesehen ist jedoch auch, dass einer verspätete Meldung eine **Begründung für die Verzögerung** beizufügen ist. (Art 33 Abs 1 DSGVO)

Den Hintergrund für die Unverzüglichkeit bzw die 72 Stunden Frist liefert ErwG 85, welcher davon ausgeht, dass es bei nicht rechtzeitiger und angemessener Reaktion zu einem physischen, materiellen oder immateriellen Schaden für natürliche Personen kommen kann. Als Beispiel für einen derartigen Schaden wird etwa ein Identitätsdiebstahl angeführt.

Auch weist der genannte Erwägungsgrund darauf hin, dass eine **Schrittweise-Meldung** möglich ist. Diese Schrittweise-Meldung ist insbesondere dann durchzuführen, wenn detaillierte Informationen etwa zu der Zahl der betroffenen oder Anzahl der betroffenen Datensätze noch fehlen. Wurde daher

eine Datenschutzverletzung eindeutig festgestellt, ist aber deren Ausmaß noch nicht bekannt, empfiehlt sich eine Schrittweise-Meldung an die Datenschutzbehörde. Diese stellt auch sicher, dass die genannte Frist gewahrt bleibt.

Verzögerte Meldung

Auch wenn die DSGVO die Möglichkeit einer verzögerten Meldung vorsieht, sollte dies keinesfalls die Regel, sondern vielmehr die Ausnahme darstellten. Die Art 29 Datenschutzgruppe führt als Beispiel, wann eine derartige Meldung zulässig sein kann, ein Zusammenkommen mehrerer vergleichbarer Verletzungen in einem kurzen Zeitraum an.

Die Strafdrohung einer verzögerten Meldung nach der DSGVO beträgt bis zu € 10 Mio oder bis zu 2% des gesamten jährlichen Jahresumsatzes. Bei der Strafzumessung sind von der Behörde jedoch auch „andere“ erschwerende oder mildernde Umstände zu berücksichtigen.

Ein Geldstrafe nach DSGVO wird von der Datenschutzbehörde auf Grundlage des § 5 VStG zu verhängt, wobei seit der Rechtslage nach dem 1.1.2019 die **Behörde das Verschulden nachzuweisen** hat, und sich nicht mehr der Beschuldige „frei zu beweisen“ hat, wenn die Strafdrohung über EUR 50.000,-- liegt. (siehe zB Pkt. III.11 des Straferkenntnisses der DSB iS Videoüberwachung). Die Vermutung des Verschuldens (§ 5 Abs 1 VStG) greift seit 1.1.2019 nur mehr bei Verwaltungsstraftaten mit einer Strafdrohung von unter EUR 50.000,--

Wenn daher der Verantwortliche **aufgrund der Auswirkungen von COVID-19** an der **Meldung gehindert war** oder die **Frist** des Art 33 Abs 1 DSGVO **versäumt** hat, dann wird die **Datenschutzbehörde** mit großer Wahrscheinlichkeit **keine Strafe** verhängen. In der Begründung für die Verzögerung sollte jedoch deutlich auf diese berücksichtigungswürdigen Umstände hingewiesen werden.

Resümee

Ein nicht bekannter Data Breach kann ohnehin nicht gemeldet werden. Wenn eine entscheidungsbefugte Person Kenntnis von der Datenschutzverletzung hat, dann besteht jedenfalls die **Meldepflicht**.

Wenn daher im Unternehmen noch eine derartige Struktur vorhanden ist, um einen Data Breach zu entdecken bzw. auf Entscheidungsträgerebene Kenntnis davon zu erlangen, wird es jedoch meiner Ansicht nach jedem Betroffenen auch möglich sein, die Meldung an die Datenschutzbehörde binnen 72 Stunden ab Kenntnis des Data Breach zu erstatten. Dies insbesondere deshalb, da etwa mangels weiterer Informationen eine **Schrittweise-Meldung** zulässig sein wird.

Auch ist davon auszugehen, dass die Datenschutzbehörde einzelfallbezogen die individuellen Umstände der aktuellen Situation berücksichtigen wird. Dies auch unter dem Gesichtspunkt, dass nicht nur der Betrieb in meldepflichtigen Unternehmen stark eingeschränkt ist, sondern auch der Dienstbetrieb der Datenschützbehörde eingeschränkt ist.

In **einer (verspäteten) Meldung** ist jedenfalls eine **Begründung** für die Verspätung anzugeben.