DATENSCHUTZ IM GESUNDHEITSSEKTOR – UMGANG MIT DATENPANNEN

Tim Wybitul, Certified Information Privacy Professional Europe (CIPP-E), Rechtsanwalt, FA Arbeitsrecht

1. Verletzungen des Schutzes personenbezogener Daten (sog. «Datenpannen») sind nicht selten. Gerade im Unternehmenssektor betreffen Datenpannen oft große Mengen sensibler Informationen. Hierzu zählen etwa Gesundheitsdaten und andere nach Art. 9 Abs. 1 DSGVO besonders geschützte Daten.

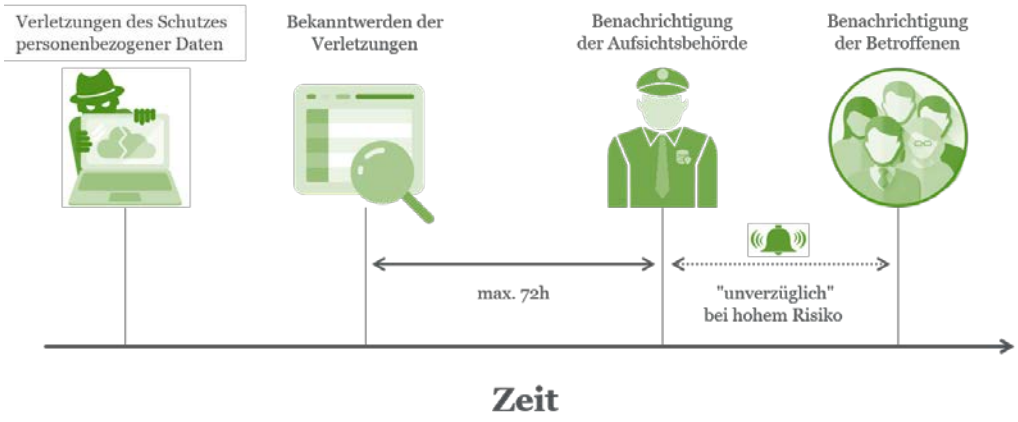
2. Im Gesundheitssektor sind die Auswirkungen von Verletzungen des Schutzes personenbezogener Daten häufig besonders gravierend. Gerade Gesundheitsdaten beinhalten meist sehr sensible Informationen über die Betroffenen. Oft sind die Kosten bei Datenpannen im Gesundheitssektor im Vergleich zu anderen Branchen besonders hoch.

3. Die unmittelbaren Rechtsfolgen bei der Verletzung des Schutzes personenbezogener Daten betreffen im Kern um Benachrichtigungspflichten gegenüber den **Datenschutz-Aufsichtsbehörden** sowie den **Betroffenen**.

4. Die Benachrichtigungspflichten existieren nicht erst seit dem Inkrafttreten der Datenschutz-Grundverordnung («**DS-GVO**»). Bereits im Jahre 2009 wurde in das damalige Bundesdatenschutzgesetz («**BDSG aF**») eine Meldepflicht in den § 42a aufgenommen. Vorbild waren die aus dem angloamerikanischen Recht bekannten *security breach notification laws*, welche erstmals in 2002 in Kalifornien zur Anwendung kamen.

5. Die Benachrichtigungspflichten bei der Verletzung personenbezogener Daten sind nunmehr im Art. 33, 34 DS-GVO zu finden. Die Meldepflicht dient der Minimierung der negativen Auswirkungen von Datenschutzverletzungen für die Betroffenen, gleichzeitig tragen sie so zu einem vorbeugenden Schutz der informationellen Selbstbestimmung bei.

6. Visualisierung des zeitlichen Ablaufs:



7. Grundsätzlich muss jede Verletzung an die Aufsichtsbehörden innerhalb von 72h gemeldet werden. Gegenüber den Betroffenen «unverzüglich» und nur, wenn ein «hohes Risiko für die Rechte und Freiheiten» derer besteht. Wann ein solches «hohes Risiko» vorliegt, ist in der Literatur sehr umstritten. Einschlägige Gerichtsentscheidungen existieren bisher nicht. Als Auslegungshilfe dienen ferner die Stellungnahmen der Datenschutz-Aufsichtsbehörden. Diese

sind allerdings nicht bindend. Folglich sind die Voraussetzungen der Benachrichtigungspflichten für den Rechtsanwender unklar.

8. Dies ist für Unternehmen mit einem hohen Risiko verbunden. Denn verstößt der Verantwortliche gegen seine Pflichten nach Art. 33 bzw. Art. 34 DS-GVO, kann die zuständige Datenschutzaufsichtsbehörden dies gem. Art. 83 Abs. 4 lit. a) DS-GVO mit einem Bußgeld sanktionieren.

9. Gem. § 43 Abs. 4 BDSG kann eine Meldung von Datenpannen an die Aufsichtsbehörde oder an die betroffene Person nach Art. 33, 34 DS-GVO in einem Verfahren nach dem OWiG gegen den Meldepflichtigen ohne Zustimmung nicht verwendet werden (umfassendes Verwertungsverbot). Es ist allerdings fraglich, ob § 43 Abs. 4 BDSG über diejenigen Verfahrensgarantien hinausgeht, die europarechtlich geboten und zulässig sind (insbesondere, ob die Öffnungsklausel des Art. 83 Abs. 8 DS-GVO einschlägig ist). Die Folge wäre, dass das umfassende Verwendungsverbot europarechtswidrig wäre.

10. Gerade für Unternehmen im Gesundheitssektor ist es dringend geboten, umfassende Vorbereitungen für den Umgang mit Datenpannen zu treffen. Insbesondere sind die betriebsinternen Zuständigkeiten zu klären und Ablaufpläne zu erstellen. In größeren Unternehmen bietet sich die Bildung sog. *Response Teams* an. Ferner sind die Mitarbeiter für das Themengebiet zu sensibilisieren und Problembewusstsein zu schulen.

* * *