Ein Jahr danach….

Waren 18.10.2019

RA Lukas Mempel
Konzerndatenschutzbeauftragter
Datenschutz und Datensicherheit
Sana Kliniken AG

Das Wesentliche in Kürze!

KEINE PANIK – Im Wesentlichen bleibt alles wie es war…
nur irgendwie schöner…

- Eine Reihe organisatorischer, prozessualer und technischer Änderungen wurden eingeführt. Diese sind in Ihren Unternehmen von den datenverarbeitenden Bereichen zu erfassen und zu dokumentieren.
- Datenschutz ist Chefsache – was sich in einer unternehmens-/ (konzern-)weit geltenden Datenschutzstrategie wiederspiegeln sollte…
- Im Falle der Datenerfassung bestehen Informations- und Hinweispflichten, welche im Einzelfall zu prüfen und entsprechend zu beachten sind.
- Die Betroffenenrechte wurden erheblich gestärkt und Auskunftspflichten normiert.
- Verfahren der Verarbeitung von Daten sind in einem Verzeichnis zu erfassen und ggf. eine Datenschutz-Folgenabschätzung durchzuführen.
- Datenschutzverstöße sind unverzüglich zu erfassen und binnen einer Frist von 72 Stunden gegenüber der zuständigen Aufsichtsbehörde zu melden.
- Die DSGVO weitet darüber hinaus die Haftungsrisiken deutlich aus. Sanktionsmöglichkeiten wurden verschärft. Bei Datenschutzverstößen drohen Unternehmen drastisch erhöhte Bußgelder von bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten weltweiten Vorjahresumsatzes.

EU Datenschutzgrundverordnung

Einwilligung / Widerruf - Artikel 7 EU DSGVO

- **Einwilligung:**
- **Bisher rechtskonform eingeholte Einwilligungen behalten ihre Gültigkeit**
- Das Ersuchen um Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist
- **Form:**
  - Kein explizites Schriftformerfordernis mehr; Einwilligung im elektronischen Format grds. möglich
  - Einwilligung über eine Website möglich – beachte Protokollierung!
  - Vor Einholung der Einwilligung im Rahmen der AGB wird abgeraten!
  - Empfehlenswert ist visuelle Hervorhebung des Einwilligungstextes
- **Protokollierung:**
  - Speicherung des Einwilligungstextes zusammen mit einem zuverlässigen Identifikationsmerkmal und dem dazugehörigen Eingabezeitpunkt („timestamp“) - Identifizierungsmerkmal kann z.B. E-Mail-Adresse sein
  - Double-Opt-In-Verfahren zum rechtssicheren Nachweis empfehlenswert
- **Beweislast** für die wirksamen Einwilligung liegt beim Unternehmen

EU Datenschutzgrundverordnung

Umgang mit besonderen personenbezogenen Daten

– Artikel 9 EU DSGVO / § 22 BDSG (n.F.)

- **Ausnahmen welche die Verarbeitung ermöglichen - Artikel 9 Abs. 2 EU DSGVO; z.B.:**
  - Einwilligung der betroffenen Person oder
  - Verarbeitung ist erforderlich um Rechte ausüben bzw. Pflichten nachkommen zu können, die sich z.B. aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes ergeben …
  - Verarbeitung ist zum Schutz lebenswichtiger Interessen notwendig oder
  - ….
- **Verpflichtungen, sofern besondere personenbezogene Daten verarbeitet werden - siehe Artikel 32 und 35 der EU DSGVO sowie § 22 BDSG (n.F.):**
  - Geeignete technisch organisatorische Maßnahmen (beispielhafte Aufzählung in § 22 BDSG (n.F.)),
  - Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
  - Wenn möglich Pseudonymisierung personenbezogener Daten,
  - Verschlüsselung personenbezogener Daten,
  - Spezifisch für Deutschland: Benennung Datenschutzbeauftragter.

EU Datenschutzgrundverordnung
Umsetzung Data Breach Reporting

- **Meldepflicht gegenüber Aufsichtsbehörden – Artikel 33 EU DSGVO**
- Meldung ist vorzunehmen durch den Verantwortlichen „unverzüglich und möglichst binnen **72 Stunden**, **nachdem** ihm die **Verletzung bekannt wurde**“. Nach Ablauf von 72 Stunden ist Begründung für die verspätete Meldung erforderlich.
- Bestimmung des Fristbeginns: Bloßer Verdacht reicht nicht aus, erforderlich sind tatsächliche Anhaltspunkte für das Bestehen einer hohen Wahrscheinlichkeit einer Verletzung - **ABER**: Unterbliebene Meldung infolge fahrlässiger Unkenntnis der Anhaltspunkte kann als **Verstoß gewertet werden**.
- Mindestanforderungen an Inhalt/Form sind in Art. 33 Abs. 3 EU DSGVO geregelt.
- Vorgeschrieben Dokumentationspflichten lt. Art. 33 Abs. 5 EU DSGVO – deshalb:
  - **Bei der Erstellung der Meldung sollte der DSB einbezogen werden!**
  - Dokumentationspflicht umfasst sowohl melde- als auch nicht meldepflichtige Verstöße!

EU Datenschutzgrundverordnung

Rechte des Betroffenen – Auskunftsrecht – Art. 15 EU DSGVO / § 34 BDSG (n.F.)

- **Erweiterter Umfang des Auskunftsrecht !**
- Auf Antrag sind dem Betroffenen Auskünfte über folgende Umstände zu erteilen:
  - die Verarbeitungszwecke sowie die K[illegible]orien personenbezogener Daten
  - Kategorien von Empfängern, insbes[illegible]mpfängern in Drittländern
  - Information zu bestehenden Rechten des B[illegible]erichtigung, Löschung, Widerspruch etc.)
  - Bestehen eines Beschwerderechts bei einer Aufsichtsb[illegible]
  - verfügbare Informationen über die Herkunft der Daten, wenn di[illegible]zogenen Daten nicht bei der betroffenen Person erhoben werden
  - das Bestehen einer automatisierten Entscheidungsfindung einschließlich „P[illegible]“ und ggf. Informationen über die involvierte Logik sowie die Tragweite einer derartigen Verarbeitung
- Verpflichtung des Verantwortlichen **eine Kopie (in der Regel kostenlos)** beizustellen (weitere Kopien gegen angemessenes Entgelt)
- **Bei elektronischem Antrag** Informationen in einem **gängigen elektronischen Format zur Verfügung stellen,** sofern der Betroffene nichts anderes angibt

Nicht § 630 g BGB

EU Datenschutzgrundverordnung

Haftung und Recht auf Schadenersatz - Artikel 82 EU DSGVO

Art. 82

DSGVO

„**Jede Person**, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, **hat Anspruch auf Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter“.

Ausnahme

Keine Haftung, sofern der Verantwortliche **nachweisen** kann, dass er für den schadenverursachenden Umstand **nicht verantwortlich** ist – die **Beweislast** liegt also **beim Verantwortlichen**, er muss sich entlasten.

Sofern mehrere Stellen für Schaden verantwortlich sind, haften sie gemeinschaftlich. Das bedeutet, dass sich die betroffene Person aussuchen kann, von wem sie den Schaden ersetzt verlangt und dass im Anschluss ein Ausgleich zwischen den Verantwortlichen stattfindet.

Vielen Dank….
Und viel Erfolg!

Ihr Referent

Rechtsanwalt Lukas Mempel

Sana Kliniken AG
Leiter Bereich Datenschutz und Datensicherheit /
Konzerndatenschutzbeauftragter

Nebenberuflich — Anwalt in der Kanzlei Loth und Spuhler, München
Marken- und Wettbewerbsrecht

Arbeitskreisleitung des AK Datenschutz und Interne Revision im DIIR
Mitglied Diverser fach- und branchenspezifischer Arbeitskreise

Mobil: (0)151 57147175

E-Mail: datenschutz@sana.de

Internet: www.sana.de