Secur-Data Betriebsberatungsges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at

DSG-Info-Service

Jänner 2014 Ausgabe Nr. 75

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Mit dem vorliegenden DSG-Info-Service wollen wir Sie über den aktuellen Stand der Diskussion zur EU-Datenschutz-Grundverordnung sowie über Neuerungen im österreichischen Datenschutzrecht informieren.
Im Zusammenhang mit der Schaffung einer neuen Standardanwendung „SA036 Hinweisgebersystem gemäß § 99g BWG" (besser bekannt unter dem Begriff „Whistleblowing"), die allerdings nur für Kreditinstitute und CRR-Wertpapierfirmen verwendet werden kann, und moderner Managementkonzepte, die das Thema „Whistleblowing" als integralen Bestandteil des Risikomanagements ansehen, gehen wir auf die datenschutzrechtlichen Problemkreise bei der Einführung eines solchen Systems ein.

1. EU-Datenschutz-Grundverordnung

In der Ausgabe Nr. 74 unseres DSG-Info-Services hatten wir Sie über den aktuellen Diskussionsstand der EU-Datenschutz-Grundverordnung informiert. Am 21. Oktober 2013 hat der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europaparlaments unter dem Vorsitz des deutschen Grünen-Politikers Jan-Philipp Albrecht den „Entwurf zur Änderung der durch die EU-Kommission vorgelegten Datenschutz-Grundverordnung (KOM(2012) 11, DS-GVO)" angenommen und die Aufnahme von Verhandlungen mit dem Rat der Europäischen Union gemäß Art. 70 beschlossen.

Es ist erstaunlich, mit welchem Tempo der vom parlamentarischen Berichterstatter Albrecht erstellte Kompromissvorschlag angenommen wurde. Statt einer geplanten Sitzungsdauer von 4 Stunden dauerte die Sitzung nur 10 Minuten. Der verabschiedete Entwurf berücksichtigt ca. 5.000 Änderungsvorschläge des europäischen Parlaments auf den Vorschlag der europäischen Kommission. Albrecht erhielt ein Verhandlungsmandat für die Trilog-Gespräche (Rat/Kommission/Parlament).

Wir gehen bewusst nicht auf die einzelnen Details dieses Kompromissvorschlags ein (mit einer Ausnahme: der Kompromissvorschlag sieht unter anderem eine Erhöhung des Strafrahmens bei schweren Datenschutzverstößen von ursprünglich 1 Million Euro bzw. 2 % des weltweiten Konzernumsatzes eines Unternehmens auf utopische 100 Millionen bzw. 5 % des weltweiten Umsatzes vor), da es derzeit laufend Beratungen in den 28 Mitgliedstaaten gibt, die nur sehr schleppend vorangehen, und weitere Änderungen zu erwarten sind. Über einzelne Bestimmungen herrscht noch überhaupt keine Einigkeit.

Staaten wie Dänemark, Ungarn, Slowenien und das nicht unbedingt datenschutzfreundliche Großbritannien blockieren derzeit die Verhand-

lungen. Auch Deutschland steht auf der Bremse. So will der deutsche Bundesinnenminister Thomas de Maizière die staatliche Datenverarbeitung aus dem Vorschlag der EU-Datenschutz-Grundverordnung überhaupt ausklammern, da seiner Meinung nach der Schutz des Bürgers vor Datenschutzverletzungen durch den Staat bereits sehr hoch entwickelt ist!

Die Novelle werde nicht mehr vor der Europawahl im Mai – in Österreich findet diese am 25. Mai 2014 statt – verabschiedet werden, führte sogar die EU-Justizkommissarin Reding kürzlich vor einem Treffen der EU-Justizminister aus.

Wir werden Sie über den Stand der Diskussion weiter am Laufenden halten.

2. Änderung der Standard- und Musterverordnung 2004

Mit der Datenschutzanpassungs-Verordnung 2013 (BGBl. Nr. II 2013/213 vom 19. Juli 2013) erfolgten Änderungen nachfolgender Standardanwendungen für den öffentlichen Bereich:

- SA005 Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts
- SA008 Personenstandsbücher
- SA009 Staatsbürgerschaftsevidenz

Darüber hinaus wurden die beiden folgenden Standardanwendungen neu geschaffen:

- SA008a Personenstandsregister
- SA009a Staatsbürgerschaftsregister

Mit BGBl. Nr. II 2013/514 vom 30. Dezember 2013 erfolgte eine weitere Änderung der Standard- und Musterverordnung 2004. Noch knapp vor Jahresende wurde die bereits in der Einleitung erwähnte

- SA036 Hinweisgebersysteme gemäß § 99g BWG

für Kreditinstitute und CRR-Wertpapierfirmen geschaffen.

Details können der Homepage der Datenschutzbehörde (www.dsb.gv.at) entnommen werden.

3. Whistleblowing

Vor allem die US-amerikanischen börsennotierten Konzerne sind aufgrund der Bestimmungen des Sarbanes-Oxley Act (SOX) aus dem Jahr 2002 gesetzlich gezwungen, auch bei ihren europäischen Tochtergesellschaften sogenannte Whistleblowing-Systeme einzurichten. Dabei werden die Mitarbeiter verpflichtet, das Fehlverhalten von Kollegen den Vorgesetzten zu melden.

Grundsätzlich gibt es zwei unterschiedliche technische Systeme: Die Einrichtung einer Whistleblowing-Hotline via Telefon, oder das Auflegen von Meldeformularen, die über das Internet angeboten werden.

Dass die Implementierung von Whistleblowing-Systemen aus datenschutzrechtlicher Sicht einige Probleme aufwirft, bedarf wohl keiner weiteren Erläuterung. Im Einzelnen werden vor der Einrichtung eines solchen Systems folgende Problemkreise zu prüfen sein:

- Rechtsgrundlage
- Grundsatz der Datenverwendung
- Datensicherheitsmaßnahmen
- DVR-Meldung
- Arbeitsrecht

Die folgenden Ausführungen behandeln Gesichtspunkte, die bei der Ausführung der oben-

genannten Problemkreise zu berücksichtigen sind.

1. Rechtsgrundlage

Die Datenschutzkommission (ab 1. Jänner 2014 Datenschutzbehörde) anerkannte bis zu ihrer Auflösung grundsätzlich ein überwiegendes Aufgabeninteresse eines Unternehmens an der Einführung einer Whistleblowing-Hotline, d.h. als Rechtsgrundlage kann § 8 Abs. 1 Z 4 DSG 2000 herangezogen werden. Als weitere Rechtsgrundlage kann der interne „Code of Conduct" eingesetzt werden, sowie nach Auffassung des Verfassers auch das Übereinkommen der Vereinten Nationen gegen Korruption (BGBl. Nr. III 47/2006).

Bei Tochtergesellschaften US-amerikanischer Konzerne wird als Rechtsgrundlage der bereits erwähnte Sarbanes-Oxley Act anerkannt. Allerdings ist eine detaillierte Beschreibung des Systems erforderlich, wobei die Meldung auf das Aufzeigen „erheblicher" Missstände eingeschränkt und diese auf definierte Bereiche eingegrenzt werden sollten.

Die bisher bei der DSK eingereichten Meldungen verwendeten die im WP 117 der 29er-Datenschutzgruppe[1]) angeführten Bereiche, und zwar: Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität. Der Schwerpunkt der datenschutzrechtlichen Vorschriften liegt naturgemäß beim Schutz der Personen, die durch ein Verfahren zur Meldung von Missständen belastet werden.

2. Grundsätze der Datenverwendung

Wie bei jeder Datenanwendung ist auch bei der Einführung einer Whistleblowing-Hotline eine Prüfung der Verhältnismäßigkeit durchzuführen. Die 29er-Datenschutzgruppe leitet aus diesem Titel folgende Grundsätze ab:

- Sowohl der Personenkreis der Anzeigeberechtigten wie auch jener der angezeigt werden kann, ist zahlenmäßig zu begrenzen.
- In besonderen Fällen können alle Mitarbeiter als Beschuldigte umfasst sein.
- Es darf keine anonymen Anzeiger geben, der Anzeiger muss zumindest bestimmbar sein.
- Anonymität ist auch insofern keine gute Lösung, da eine erhobene Beschwerde schwierig zu überprüfen ist, wenn keine Möglichkeit besteht, Anschlussfragen zu stellen. Weiters besteht die Gefahr der Vernaderung sowie die Gefahr, dass im Unternehmen eine Kultur böswilliger Meldungen entsteht.
  Auch widerspricht die anonyme Meldung dem Datenschutzgrundsatz, dass personenbezogene Daten nur nach Treu und Glauben erhoben werden dürfen.
  Die bisherigen Entscheidungen der DSK führen allerdings in diesem Zusammenhang aus: „Die Erstattung anonymer Anzeigen ist zwar grundsätzlich möglich, darf jedoch vom Auftraggeber nicht gefördert werden".
  Dem Beschuldigten muss Zugang zu den Anschuldigungen gewährt werden. Die Identität des Anzeigers darf nur dann offengelegt werden, wenn sich herausstellt, dass die Meldung bewusst falsch erstattet wurde. Ansonsten ist dem Anzeiger volle Vertraulichkeit zu gewähren.
- Die Aufbewahrungsdauer ist zu beschränken. Die DSK akzeptierte 2 Monate nach Abschluss des Verfahrens.

3. Datensicherheitsmaßnahmen

Auf die Datensicherheitsmaßnahmen ist besonderes Augenmerk zu legen. Vor allem gilt dies, wenn ein Dienstleister mit dem Betrieb der Whistleblowing-Hotline beauftragt werden soll.

Wichtig ist die Einrichtung einer zentralen Stelle, die für die Handhabung der Meldungen der Hinweisgeber und die Durchführung der

[1]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf

Untersuchung verantwortlich ist. Die Zugriffsrechte sind auf diese Stelle zu beschränken.

4. DVR-Meldung

Eine Whistleblowing-Hotline unterliegt grundsätzlich der Meldepflicht der §§ 17 ff DSG 2000 sowie der Vorabkontrolle des § 18 Abs. 2 DSG 2000.

Bei den bisherigen Meldungen wurde folgende Bezeichnung der Datenanwendung gewählt: „Internes Verfahren zur Erfassung von Meldungen über mutmaßliche Missstände im Unternehmen in den Bereichen Rechnungslegung, interne Rechnungskontrolle, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität".

Die Meldung umfasst 3 Betroffenenkreise:

- Hinweisgeber, die ihre Identität offengelegt haben,
- im Hinweis genannte Personen, sowie
- andere Personen (Zeugen oder sonstige Auskunftspersonen).

5. Arbeitsrechtliche Würdigung

Wird durch die Whistleblowing-Hotline ein Zustand ununterbrochener Kontrolle erreicht, so besteht kein Zweifel, dass die Menschenwürde berührt wird und somit eine Zustimmung des Betriebsrates (§ 96 Abs. 1 Z 3 ArbVG) bzw. im Falle des Fehlens eines solchen die Zustimmung jedes einzelnen Mitarbeiters (§ 10 AVRAG) erforderlich ist.

Wird das System jedoch so eingeschränkt, dass nur bei Vorliegen eines konkreten Verdachts auf Unregelmäßigkeiten die Entscheidungsträger alarmiert werden, um eine entsprechende Klärung herbeizuführen, liegt kein Kontrollsystem iSd ArbVG vor. In diesem Fall ist daher der Abschluss einer Betriebsvereinbarung bzw. die Zustimmung jedes einzelnen Mitarbeiters entbehrlich.

••••