Prof. Dr. Rolf Lauser

Dr.-Gerhard-Hanke-Weg 31
85221 Dachau
Tel.: 08131/511750
Fax: 08131/511619
rolf@lauser-nhk.de

Von der Industrie- und Handelskammer für München und Oberbayern öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung im kaufmännisch-administrativen Bereich sowie Datenschutz und Datensicherheit

Dachau, März 2018

Hinweise zur DSGVO (Langform)

1. Die **Europäische Datenschutzgrundverordnung** (EU-DSGVO, im Folgenden DSGVO) **wird am 25.05.2018 gültig** und löst die EU-Datenschutz-Richtlinie (95/46/EG) und das Bundesdatenschutzgesetzt BDSG ab. Allerdings ist die DSGVO keine umfassende Datenschutz-Norm für die EU-Staaten. **Sie enthält mehrere sog. Öffnungsklauseln, die es den Nationalstaaten ermöglicht, definierte Datenschutz-Bereiche nationalstaatlich zu regeln**. Daraus folgt, dass es wohl auch zukünftig EU-weit keine wirklich identischen Datenschutzregeln geben wird.

2. **Neben der DSGVO existiert weiterhin die EU-e-Privacy-Richtlinie** (2002/58/EG) **als Europäische Grundlage des Telemediengesetzes** (TMG = Datenschutzgesetz für Internet-basierende Dienste wie E-Mail und WWW). Die EU beabsichtigt in Zukunft die e-Privacy-Richtlinie zu novellieren, was dann wohl auch eine Novellierung des TMG nach sich ziehen wird (Termine dafür sind derzeit nicht abzusehen).

3. Neben dem TMG werden **in Deutschland auch weiterhin Datenschutzregelungen außerhalb der DSGVO** bestehen bleiben. Dazu gehören beispielsweise Datenschutz-regeln im Rahmen der Sozialgesetzbücher (SGB), des Telekommunikationsgesetzes (TKG) sowie alle datenschutzrelevanten Regelungen im Bereich des öffentlichen Rechts. Auch der § 7 (2) UWG (Gesetz gegen den unlauteren Wettbewerb), in dem die wesentlichen Rahmenbedingungen der Telefon- und E-Mail-Werbung geregelt sind, bleibt bestehen.

4. **Für den Datenschutz in der Privatwirtschaft, der auch Vereine zugerechnet werden, sind vor allem zwei Öffnungsklauseln von Bedeutung**: Einerseits geht es um den **betrieblichen Datenschutzbeauftragten**, andererseits um den **Beschäftigten-Datenschutz,** wozu auch die Videoüberwachung von Arbeitsplätzen gehört. Diese Be-

reiche wurden zwischenzeitlich national geregelt, wobei im Beschäftigten-Datenschutz die inhaltlichen Regelungen des § 32 BDSG weitgehend unverändert übernommen wurden. Auch der betriebliche Datenschutzbeauftragte wird in Deutschland für Organisationen, in denen mehr als 10 Personen Zugriff auf personenbezogene Daten haben, weiterhin verpflichtend sein. Allerdings werden sich die Aufgaben des betrieblichen Datenschutzbeauftragten gemäß Art. 39 DSGVO künftig ändern.

5. Die **Erlaubnistatbestände der DSGVO für die Erhebung und Verarbeitung personenbezogener Daten entsprechen**, bis auf das Wording, **weitgehend den Erlaubnistatbeständen des alten BDSG**. Deshalb ist dieser Bereich der DSGVO für deutsche Organisationen relativ einfach umzusetzen. Allerdings sollte man den Dokumentations- und Organisations-Aufwand nicht unterschätzen.

6. **Auskunftsrechte** (Art. 15 DSGVO), **Berichtigungsrechte** (Art. 16 DSGVO) und **Rechte auf Einschränkung der Verarbeitung** (= Sperren, Art. 18 DSGVO) **entsprechen weitgehend den Regelungen des alten BDSG**, wobei dem **Recht auf Löschung** (Recht auf Vergessen werden, Art. 17 DSGVO) eine **höhere Bedeutung** zukommt als im bisherigen § 35 (2) BDSG.
   Ein **neues Betroffenen-Recht ist das „Recht auf Datenübertragbarkeit“** (Art. 20 DSGVO). Hierbei geht es um den „Umzug“ von Profilen und Datenbeständen von einer verantwortlichen Stelle an eine andere (beispielsweise von LinkedIn zu XING).

7. Ein wirkliches **Konzern-Privileg ist auch in der DSGVO nicht vorgesehen**. Lediglich im Beschäftigtendatenschutz wird durch den Erwägungsgrund 48 (für interne Verwaltungszwecke innerhalb eines Konzerns) ein Konstrukt eingeführt, das in Richtung Konzern-Privileg weist. Zu beachten ist hier jedoch eine detaillierte, transparent zu dokumentierende Interessenabwägung als absolute Voraussetzung für eine konzernweite Beschäftigten-Datenverarbeitung.

8. Die **Transparenzpflicht der Verantwortlichen** (= bisherige verantwortliche Stelle) wurde **stark ausgeweitet**. Grundlage sind die Vorgaben für die Datenerhebung und die -Verarbeitung aus Art 5 (1) DSGVO. Diese beruhen auf den Prinzipien von Treu und Glauben, Zweckbindung, Angemessenheit, Richtigkeit, Speicherdauerbegrenzung und Datenintegrität.

9. Diese erweiterte Transparenzpflicht bedingt **künftig sehr viel ausführlichere Datenschutzerklärungen als bisher**. Beispielsweise muss der Datenschutzbeauftragte samt Kommunikationsadressen genannt werden. Auch die Speicherdauer ist transparent darzulegen. Zudem müssen Datenschutzerklärungen künftig immer auf etwaige Änderungen/Erweiterungen des Verarbeitungszweckes hinweisen. Dies ist Informationspflicht des Verantwortlichen und Bedingung für eine Zweck-Änderung/-Erweiterung.

   Hinzuweisen ist auch auf den **Wegfall des sog. Listen-Privilegs** (§ 28 (3) BDSG), nach dem bisher selbst erhobene (Post-)Adressdaten ohne Einwilligung (es besteht lediglich ein Widerspruchsrecht des Betroffenen) für Werbe-/Marketing-Zwecke genutzt werden können. Diese Erleichterung fällt weg, d.h. die Verantwortlichen müssen künftig auch für postalische Werbe-/Marketing-Briefe Einwilligungen einholen. Werbe-/Marketing-Briefe werden wie Werbe-/Marketing-E-Mails oder Telefonwerbung, die gemäß § 7 (2) UWG zu beurteilen sind, behandelt (Vgl. dazu auch die anhängende Handlungsanweisung für die nachträgliche Einholung von Einwilligungen.).

10. Eine Neuerung der DSGVO stellt die **Einführung einer sog. Joint-Controllership** (gemeinsame Verantwortlichkeit mehrerer Verantwortlicher) dar (Art. 26 DSGVO): Mehrere Verantwortliche können künftig für die Erhebung und Verarbeitung der Daten verantwortlich sein. Diese Joint-Controllership ist in der Datenschutzerklärung darzulegen.

11. Neu in der DSGVO ist auch das **„Recht auf Vergessen werden“** (Art. 17 DSGVO). Alle IT-Prozesse müssen künftig eine physische Löschung von Daten ermöglichen. Dies bringt Probleme. So stellt sich z.B. die Frage, wie diese Löschfunktion bei Daten, die auf revisionssicheren Datenträgern gespeichert sind, realisiert werden soll, ohne dass die Revisionssicherheit verhindert wird.

12. Die DSGVO bringt **erhebliche Änderungen bei der Auftragsdatenverarbeitung**, vor allem auf Seiten der Auftragsdatenverarbeiter/Dienstleister. Folgende Rahmenbedingungen werden hier gelten:

    a. Nach Art. 28 DSGVO gelten im Rahmen der Auftragsdatenverarbeitung **künftig gestufte Verantwortlichkeiten**. Danach ist der Auftraggeber (Controller)

für die Überwachung des von ihm beauftragten Dienstleisters (Processor) zuständig. Dieser wiederum ist für die Überwachung seiner Dienstleister verantwortlich, wobei ursprünglicher Auftraggeber (Controller), Dienstleister (Processor) und, soweit eingesetzt, dessen Unterauftragnehmer (Sub-Contractor) gemeinsam das Risiko der Verarbeitung tragen.

b. Künftig reicht eine Information des Dienstleisters an den Auftraggeber/Controller über eingeschaltete Unterauftragnehmer nicht mehr aus. **Vielmehr muss der Auftraggeber der Einschaltung von Unterauftragnehmern durch den Dienstleister zustimmen.**

c. Nach Art. 28 DSGVO ist der **Dienstleister selbst Adressat des Gesetzes**. Er ist künftig dazu verpflichtet, von sich aus die beim Auftraggeber eingeführten und gelebten Datensicherheitsmaßnahmen sowie den dort gegebenen Umgang mit den Daten zu überwachen. Da dieser Punkt insbesondere bei der Auslagerung von Rechnerleistungen in Dienstleistungszentren eine Rolle spielt, ist er für DAV-Sektionen von untergeordneter Bedeutung.

d. **Auftragsdatenverarbeitung erfordert auch weiterhin eine vertragliche Grundlage** (Art. 28 (3) DSGVO). Inhaltlich kann sich dieser Vertrag an den bisher in Deutschland üblichen ADV-Verträgen (§ 11 BDSG) orientieren. Lediglich das Wording und der bisherige Paragraphenbezug müssen der DSGVO angepasst werden.

e. Die Auftragsdatenverarbeiter müssen ihre Sicherheitstechnik laufend dem aktuellen Stand der Technik anpassen. Es wird für deutsche Organisationen deshalb sinnvoll sein, sich an den technischen und organisatorischen Maßnahmen der Anlage zu § 9 BDSG zu orientieren.

f. **Bei Auftragsdatenverarbeitung mit einem Dienstleister in Drittstaaten ist eine zweistufige Prüfung durchzuführen**. Zunächst muss die Übermittlung der Daten überhaupt zulässig sein. Sodann ist zu prüfen, ob beim Dienstleister im Drittstaat ein hinreichendes Datenschutz- und -Sicherheits-Niveau gegeben ist. Dies kann anhand eines Angemessenheitsbeschlusses der EU oder dem Abschluss der EU-Standard-Vertragsklauseln geschehen. Für US-

Amerikanische Dienstleister gibt es zusätzlich die Sonderregelung des EU-US-PrivacyShield.

13. Die DSGVO lastet den Verantwortlichen **eine Vielzahl von Dokumentationspflichten** auf. Gemäß Art. 30 DSGVO muss der Verantwortliche alle Prozesse, in denen personenbezogene Daten verarbeitet werden, in einem Verzeichnis der Verarbeitungstätigkeiten dokumentieren. Gemäß Art. 32 DSGVO besteht auch hinsichtlich der technischen und organisatorischen Datensicherheitsmaßnahmen Dokumentationspflicht. Auf Anforderung sind diese Dokumentationen der zuständigen Aufsichtsbehörde vorzulegen.

14. Nach der DSGVO sind **Bußgeld-Androhungen an die Verantwortlichen sehr viel höher** als nach dem BDSG. Bei bestimmten Verstößen liegt die Bußgeld-Androhung bei bis zu € 10 Mio, bzw. 2% des globalen Jahresumsatzes. Für Verstöße mit größeren Folgen sind sogar bis € 20 Mio, bzw. 4% des jährlichen globalen Umsatzes des Verantwortlichen oder im Falle der Auftragsdatenverarbeitung gemeinsam für den Auftraggeber und Dienstleister angedroht.

Dachau, 7. März 2018
Prof. Dr. Rolf Lauser

Anlage: Generelle Handlungsanweisung für die nachträgliche Einholung von Einwilligungen

Ändern sich Datenschutzerklärungen, z.B. bedingt durch den Einsatz von neuen/geänderten Softwareanwendungen, die erweiterte Datenerhebungen erfordern oder durch Änderungen im Bereich der Datenschutzgesetze, so erfordert dies neue Einwilligungen durch die Betroffenen. Für die Einholung dieser neuen Einwilligungen bietet sich das folgende Vorgehen an:

- Überarbeiten Sie die Datenschutzerklärung gemäß der neuen Anforderungen der Softwareanwendung bzw. der Gesetzesänderung und nutzen Sie diese neuen Datenschutzerklärungen für alle Neu-Beitretenden
  *Anmerkung: Wenn die vom Bundesverband im Dezember 2017 zur Verfügung gestellte Datenschutzerklärung verwendet wird, gibt es derzeit **keinen** Handlungsbedarf (Stand: 7.3.2018).*
- Setzen Sie den Bestandsmitgliedern eine Widerspruchsfrist, z.B. 3 Wochen.
- Informieren Sie die Bestandsmitglieder darüber, dass die Sektion, soweit nach Ablauf der gesetzten Frist kein Widerspruch eingegangen ist, dies als Einwilligung in die neue Datenschutzerklärung wertet.
- Eingegangene Widersprüche sind zu beachten. D.h. wird einer Klausel der neuen Datenschutzerklärung widersprochen, so ist dies gegenüber dem widersprechenden Mitglied zu beachten.
- Dokumentieren Sie den gesamten Prozess, z.B. durch Archivierung des Informationsschreibens, der Adressaten des Informationsschreibens und der eingegangenen Widersprüche.