Zusammenfassende Anmerkungen EU-Datenschutzgrundverordnung
Stand: 26.03.2018

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

Zusammenfassung DSGVO für Vereine

ZUSAMMENFASSENDE ANMERKUNGEN ZUR EU-DATENSCHUTZGRUNDVERORDNUNG

1. Die EU-Datenschutzgrundverordnung (DSGVO) wird am 25.05.2018 gültig und löst damit die EU-Datenschutz-Richtlinie (95/46/EG) und das Bundesdatenschutzgesetz alte Fassung (BDSG a.F.) ab. Allerdings stellt die DSGVO keine umfassende Datenschutz-Norm für die EU-Staaten dar, da die DSGVO mehrere sog. Öffnungsklauseln umfasst, durch die dann den Nationalstaaten die Möglichkeit gegeben wird, im Rahmen dieser Öffnungsklauseln 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 derzeit weiterhin die die EU-e-Privacy-Richtlinie (2002/58/EG), die die Europäische Grundlage des TMG (Telemediengesetz = Datenschutzgesetz für Internet-basierende Dienste, wie E-Mail und WWW) darstellt. Das TMG wird deshalb bis auf weiteres existieren. Die EU beabsichtigt in Zukunft die e-Privacy-Richtlinie zu novellieren, was dann wohl auch eine Novelle des TMG nach sich ziehen wird. Termine für dieses Vorhaben sind derzeit nicht abzusehen.

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

4. Im Bereich des betrieblichen Datenschutzes sind vor allem zwei Öffnungsklauseln von Bedeutung. Dabei handelt es sich einerseits um den betrieblichen Datenschutzbeauftragten und andererseits um den Beschäftigten-Datenschutz, wozu auch die Videoüberwachung von Arbeitsplätzen gehört. Diese Bereiche wurden zwischenzeitlich national im BDSG neue Fassung (n.F.) geregelt, wobei im Beschäftigten-Datenschutz die ursprünglichen Regelungen des § 32 BDSG a.F. inhaltlich 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 zukünftig ändern.

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

5. Die Erlaubnistatbestände (Erlaubnis zur Verarbeitung personenbezogener Daten aufgrund von Rechtsvorschriften oder Einwilligungen) der DSGVO für die Erhebung und Verarbeitung personenbezogener Daten entsprechen, bis auf die Wortwahl, weitgehend den Erlaubnistatbeständen die im BDSG a.F. definiert sind. Von daher gesehen wird dieser Bereich der DSGVO für Deutsche Organisationen relativ einfach umsetzbar sein, wobei allerdings der zu erwartende Dokumentations- und Organisationsaufwand nicht unterschätzt werden sollte.

6. Auskunftsrechte (Art. 15 DSGVO), Berichtigungsrechte (Art. 16 DSGVO), und Rechte auf Einschränkung der Verarbeitung, d.h. Sperren (Art. 18 DSGVO) entsprechen weitgehend den Regelungen des BDSG a.F., wobei dem Recht auf Löschung, d.h. Recht auf Vergessen (Art. 17 DSGVO) eine höhere Bedeutung zukommt, als dem bisherigen § 20 Abs. 2 BDSG.

   Ein neues Betroffenen-Recht stellt das Recht auf Datenübertragbarkeit (Art. 20 DSGVO) dar. Hierbei geht es um den „Umzug" von Profilen und Datenbeständen eines Betroffenen von einem Verantwortlichen (bislang verantwortliche Stelle nach BDSG a.F.) zu einem anderen Verantwortlichen (u.a. juristische Personen, wie Vereine, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden), also beispielsweise von LinkedIn zu XING.

7. Eine Neuerung der DSGVO ist das Recht auf Vergessenwerden (Art. 17 DSGVO). D.h. alle IT-Prozesse müssen zukünftig eine physische Löschung von Daten ermöglichen. Dies bringt aber Probleme: so stellt sich beispielsweise die Frage, wie diese Löschfunktion bei Daten, die auf revisionssicheren Datenträgern gespeichert sind, realisiert werden soll, ohne dass die Revisionssicherheit verhindert wird.

8. Die Transparenzpflicht der Verantwortlichen wurde stark ausgeweitet. Grundlage dafür sind die Modalitäten der Datenerhebung und -verarbeitung aus Art. 5 Abs. 1 DSGVO, die auf den Prinzipien von Rechtmäßigkeit, Treu und Glauben, Zweckbindung, Angemessenheit bzw. Datenminimierung, Richtigkeit, Speicherdauerbegrenzung und Integrität bzw. Schutz und Vertraulichkeit beruhen.

9. Aus dieser erweiterten Transparenzpflicht resultiert dann, dass Datenschutzerklärungen zukünftig sehr viel ausführlicher sein werden, als dies bisher der Fall war.
   So muss bspw. zukünftig in der Datenschutzerklärung der Datenschutzbeauftragte samt seien Kommunikationsadressen genannt werden. Auch die Speicherdauer muss transparent dargelegt werden. Wichtig ist darüber hinaus, dass zukünftig in Datenschutzerklärungen immer auf etwaige Änderungen/Erweiterungen des Verarbeitungszweckes hingewiesen wird. Nur unter dieser Bedingung ist zukünftig, unter Beachtung der Informationspflicht des Verantwortlichen, eine Zweck-Änderung/-Erweiterung möglich.

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

Hinzuweisen ist auch auf den zukünftigen Wegfall des sog. Listen-Privilegs nach § 28 Abs. 3 BDSG a.F.. Bisher können selbst erhobene (Post-)Adressdaten, ohne Einwilligung (es besteht lediglich ein Widerspruchsrecht des Betroffenen) für Werbe-/Marketing-Zwecke genutzt werden. Diese Erleichterung wird ab 25.05.2018 unwiderruflich wegfallen. D.h. zukünftig müssen sich die Verantwortlichen auch für postalische Werbe-/Marketing-Briefe Einwilligungen einholen. Werbe-/Marketing-Briefe werden also zukünftig wie Werbe-/Marketing-E-Mails oder Telefonwerbung, die gemäß § 7 Abs. 2 UWG zu beurteilen sind, behandelt.

10. Ein wirkliches Konzern-Privileg ist auch in der DSGVO nicht vorgesehen. Lediglich im Beschäftigtendatenschutz wird durch den Erwägungsgrund 48 zur DSGVO (für interne Verwaltungszwecke innerhalb eines Konzerns) ein Konstrukt eingeführt, das in Richtung Konzernprivileg weist. Allerdings muss hier beachtet werden, dass eine detaillierte Interessenabwägung, die transparent dokumentiert werden muss, eine absolute Voraussetzung für eine konzernweite Beschäftigten-Datenverarbeitung darstellt.

11. Eine Neuerung der DSGVO stellt die Einführung einer sog. Joint-Controllership (gemeinsame Verantwortlichkeit mehrerer Verantwortlicher) dar (Art. 26 DSGVO). D.h. zukünftig können mehrere Verantwortliche für die Erhebung und Verarbeitung der Daten verantwortlich sein. Diese Joint-Controllership muss dann aber in der Datenschutzerklärung dargelegt werden.

12. Im Bereich der Auftragsdatenverarbeitung wird die DSGVO erhebliche Änderungen bewirken, vor allem auch auf Seiten der Auftragsdatenverarbeiter/Dienstleister. Im Einzelnen werden hier zukünftig die folgenden Rahmenbedingungen gelten:

    a. Nach den Vorgaben des Art. 28 DSGVO gelten im Rahmen der Auftragsdatenverarbeitung zukünftig gestufte Verantwortlichkeiten. Danach ist der Auftraggeber (der 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 (Operator) und, soweit eingesetzt, dessen Unterauftragnehmer (Sub-Contractor) gemeinsam das Risiko der Verarbeitung tragen.

    b. Zukünftig reicht eine Information des Dienstleisters an den Auftraggeber über eingeschaltete Unterauftragnehmer nicht mehr aus. Vielmehr ist es nach der DSGVO erforderlich, dass der Auftraggeber der Einschaltung von Unterauftragnehmern durch den Dienstleister zustimmt.

    c. Der Dienstleister ist nach Art. 28 DSGVO selbst Adressat des Gesetzes. D.h. zukünftig ist dieser verpflichtet, von sich aus die beim Auftraggeber eingeführten und gelebten Datensicherheitsmaßnahmen und den dort gegebenen Umgang mit den Daten zu überwachen.

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

d. Auftragsdatenverarbeitung erfordert auch zukünftig eine vertragliche Grundlage (Art. 28 Abs.3 DSGVO). Inhaltlich kann sich dieser Vertrag zweifellos an den bisher in Deutschland üblichen Auftragsdatenverarbeitungsverträgen (ADV-Verträgen) nach § 11 BDSG a.F. orientieren. Lediglich der Wortlaut und der bisherige Paragraphenbezug muss den Gegebenheiten der DSGVO angepasst werden.

e. Die Auftragsdatenverarbeiter (Dienstleister) müssen nach der DSGVO die bei ihnen realisierte Sicherheitstechnik laufend dem aktuellen Stand der Technik anpassen. Es wird für deutsche Organisationen deshalb sinnvoll sein, sich an den technischen und organisatorischen Maßnahmen (TOM) der Anlage zu § 9 BDSG a.F. zu orientieren.

f. Bei Auftragsdatenverarbeitung mit einem Dienstleister in Drittstaaten ist eine zweistufige Prüfung durchzuführen. Zunächst einmal 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-Privacy-Shield.

13. Die DSGVO lastet den Verantwortlichen eine Vielzahl von Dokumentationspflichten auf. So sind vom Verantwortlichen gemäß Art. 30 DSGVO alle Prozesse, in denen personenbezogene Daten verarbeitet werden, in einem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren. Auch sind zukünftig gemäß Art. 32 DSGVO die ergriffenen technischen und organisatorischen Datensicherheitsmaßnahmen zu dokumentieren.
    Diese Dokumentationen sind auf Anforderung der zuständigen Aufsichtsbehörde vorzulegen.

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