DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Diplom-Informatiker Werner Hülsmann

Datenschutz im Verein Umsetzung der DSGVO

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Agenda

0	Vorstellung
1	Das neue Datenschutzrecht in Europa
2	DSGVO – Umsetzung in 10 Schritten
3	Hilfsmittel

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Agenda

0	Vorstellung
1	Das neue Datenschutzrecht in Europa
2	DSGVO – Umsetzung in 10 Schritten
3	Hilfsmittel

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Diplom-Informatiker Werner Hülsmann

1982 – 1988	Studium der Informatik an der TU Darmstadt - Schwerpunkt Datenschutzrecht
1988 – 1991	Softwareentwickler bei der Telenorma GmbH, Frankfurt (Main)
1992 – 1999	Wissenschaftlicher Mitarbeiter und Referatsleiter Technik beim Landesbeauftragten für DS der Freien Hansestadt Bremen
1999 – 2001	Datenschutz- und Technologieberatung bei ForBIT e.V. in Hamburg
Seit 1999	selbständiger Datenschutzberater (Datenschutzconsulting.eu)
2001 – 2003	Projektmanager Dataprotection bei der Telegate AG (Martinsried)
2003 – 2009 und seit 2014	Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz (DVD) e.V., Bonn - www.datenschutzverein.de
2004	Gründung von Datenschutzwissen.de – Organisation und Leitung von Datenschutzseminaren
Seit 2004	beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich/technisch)
Seit 2010	Expert for legal and technical evaluations for the European Privacy Seal (http://www.european-privacy-seal.eu/)
Seit 09/2017	Member of the Commission Multistakeholder expert group to support the application of Regulation (EU) 2016/679 (GDPR)

Datenschutz – was ist das?

- Datenschutz schützt nicht die Daten, sondern dient dem Schutz der Privatsphäre sowie der Grundrechte und Grundfreiheiten der betroffenen Personen.
- Datenschutz ist keine moderne Erfindung, sondern gibt es bereits seit der Antike (z.B. im Hippokratischen Eid).
- Datenschutz ist ein Menschenrecht.
- Der Datenschutz – das Recht auf informationelle Selbstbestimmung – wurde 1983 vom BVerfG aus den Grundrechten der Art. 1 und 2 des Grundgesetzes abgeleitet.
- Datenschutz ist bereits seit 2009 auch in der Europäischen Grundrechtecharta verankert.

Was sind personenbezogene Daten?

Personenbezogene Daten sind gemäß Art. 4 Ziff. 1 DSGVO

- „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;
- als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;“

Die Datenschutzgrundsätze der DSGVO

Art. 5 Abs. 1 fordert, dass personenbezogene Daten nach den folgenden Grundsätzen verarbeitet werden müssen:

- „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“
- „Zweckbindung“
- „Datenminimierung“
- „Richtigkeit“
- „Speicherbegrenzung“
- „Integrität und Vertraulichkeit“

Art. 5 Abs. 2 DSGVO regelt:

- „Der Verantwortliche ist für die Einhaltung des Absat-zes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO)

Die Verarbeitung personenbezogener Daten ist „nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist“:

- **die wirksame Einwilligung der betroffenen Person liegt vor**
- **die Verarbeitung dient der Erfüllung eines Vertrags mit der betroffenen Person oder vorvertraglicher Maßnahmen auf Initiative der betroffenen Person**
- **die Verarbeitung ist zur Erfüllung gesetzlicher Verpflichtungen erforderlich**
- *„die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer an-deren natürlichen Person zu schützen“*
- *„die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde “*
- **„die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“**

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Agenda

0	Vorstellung
1	Das neue Datenschutzrecht in Europa
2	DSGVO – Umsetzung in 10 Schritten
3	Hilfsmittel

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Gliederung

1.1	Das neue Datenschutzrecht in Europa
1.2	Was ändert sich durch die DSGVO?
1.3	Das neue Bundesdatenschutzgesetz

Das neue Datenschutzrecht in Europa

- Die EU Datenschutz-Grundverordnung (**DSGVO,** auch DS-GVO)
  - ist ein großer Schritt in der Aktualisierung und Vereinheitlichung des europäischen Datenschutzrechts
  - wurde am 04. Mai 2016 im EU-Amtsblatt veröffentlicht.
  - Sie gilt ab dem 25. Mai 2018.
  - Sie gilt direkt auch für **alle Unternehmen, Vereine, Institutionen** innerhalb (und auch für einige außerhalb) der **EU** und des Europäischen Wirtschaftsraums (**EWR**)
    - und führt daher zu einheitlicheren Wettbewerbsbedingung
- Die DSGVO enthält einige sogenannte **Öffnungsklauseln (eigentlich: Konkretisierungs- und Regulierungsklauseln)**.
  - In einigen Bereichen müssen die **Nationalstaaten** diese „Öffnungsklauseln“ mit eigenen Regelungen ausfüllen.
  - In anderen Bereichen können sie die „Öffnungsklauseln“ nutzen um bewährte Datenschutzregelungen im nationalen Recht zu erhalten.

Das neue Datenschutzrecht in Europa (2)

- Gleichzeitig mit dem Gültigwerden der **DSGVO**
  - tritt am 25. Mai 2018 das neue Bundesdatenschutzgesetz (**BDSG-neu**) in Kraft und
  - wird das derzeit und bis dahin gültige Bundesdatenschutzgesetz (BDSG-alt) aufgehoben
  - **DSGVO und BDSG-neu (Teil 1 und Teil 2)** ersetzen **zusammen** das BDSG-alt!
- Auch im **Online-Bereich** wird der Datenschutz auf europäischer Ebene aktualisiert.
  - Die derzeit auf EU-Ebene geltende EU-ePrivacy-Richtlinie soll entsprechend eines Vorschlag der EU-Kommission ebenfalls durch eine direkt geltende EU-ePrivacy-Verordnung (**EU-ePriv-VO**) abgelöst werden.
    - Hierzu hat die EU-Kommission am 10. Januar 2017 einen Entwurf vorgestellt.
    - Hierzu hat das EU-Parlament bereits im Oktober 2017 seine Stellungnahme beschlossen.
    - Der EU-Ministerrat berät allerdings noch immer.
  - Nach der ursprünglichen Vorstellung der EU-Kommission sollte auch die EU-ePriv-VO am 25. Mai 2018 gültig werden. Dies wird nach aktuellen Informationen aber nicht mir nicht vor 2019 geschehen

Gliederung

1.1 Das neue Datenschutzrecht in Europa
1.2 Was ändert sich durch die DSGVO?
1.3 Das neue Bundesdatenschutzgesetz

Was ist neu in der DSGVO?

Vier wesentliche Änderungen sind:

- Die Dokumentationspflichten werden deutlich ausgeweitet (vgl. Art.5 Abs.2 DSGVO)
  - „Nachweispflicht“ – eine Art Beweislastumkehr: Die verarbeitende Stelle muss nachweisen können, dass ihre Verarbeitung personenbezogener Daten datenschutzkonform ist.
- Die Betroffenenrechte werden deutlich ausgeweitet und es wird eine Reaktionsfrist verbindlich festgelegt (vgl. Art. 12-23 DSGVO)
- Es werden neue Bußgeldtatbestände eingeführt
- Die Bußgelder erhöhen sich drastisch auf bis zu 20 Mio € oder für Unternehmen bis zu 4 % des weltweiten Jahresumsatzes, je nach dem, welcher Betrag höher ist.

Was ist neu in der DSGVO? (2)

Weitere wichtige Änderungen sind u.a.

- Die Datenschutz-Folgenabschätzung ersetzt die bisherige Vorabkontrolle und ist deutlich umfangreicher.
- Eine Abschätzung der Risiken für die Freiheiten und Grundrechte der betroffenen Personen ist an vielen Stellen der DSGVO erforderlich.
- Privacy by Design, privacy by default (Stichwort: Datenminimierung) werden verbindlich.
- Die Pflichten für Auftrags(daten)verarbeiter werden umfangreicher, u.a. müssen Auftrags(daten)verarbeiter auch ein Verzeichnis von Verarbeitungstätigkeiten führen.
- Bei zu ungenauer Beauftragung können Auftrags(daten)verarbeiter ebenfalls zu Verantwortlichen werden.

Änderungen bei den Rechten der Betroffenen

- Die Informations- und Auskunftspflichten werden deutlich umfangreicher.
- Neu sind
  - Recht auf „Vergessenwerden“ als Erweiterung des Rechts auf Löschen
  - Recht auf Datenübertragbarkeit
- Das Widerspruchsrecht aus Art. 21 – u.a. Widerspruch gegen die Nutzung der personenbezogenen Daten für werbliche Zwecke – kann bei Internetnutzung auch durch „automatisierter Verfahren“ ausgeübt werden. D.h. etwaige von Website- oder App-NutzerInnen aktivierte „Do-not-Track“-Optionen müssen berücksichtigt werden.
- Es wird ein verbindliche Reaktionszeit von **einem** Monat eingeführt. Einmalig kann diese Frist um zwei Monate verlängert werden. Die betroffene Person ist hiervon innerhalb des ersten Monats zu unter Angabe der Gründe zu informieren.

Informationspflichten (Art. 13 DSGVO)

- **Name** und die **Kontaktdaten** des Verantwortlichen
- **Kontaktdaten** des Datenschutzbeauftragten
- die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
- wenn die Verarbeitung auf **berechtigten Interessen (**Art. 6 Abs. 1 Buchstabe f) beruht, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- **Empfänger** oder Kategorien von Empfängern
- die Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland** zu übermitteln und einen Verweis auf die geeigneten oder **angemessenen Garantien** und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

Informationspflichten (Art. 13 DSGVO)

- die **Dauer** der Speicherung
- das Bestehen eines Rechts auf **Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf **Berichtigung** oder **Löschung** oder auf **Einschränkung der Verarbeitung** oder eines **Widerspruchsrechts** gegen die Verarbeitung sowie des **Rechts auf Datenübertragbarkeit**
- das Recht, die **Einwilligung** jederzeit **widerrufen zu können,** wenn die Verarbeitung auf einer Einwilligung beruht
- das Bestehen eines **Beschwerderechts** bei einer **Aufsichtsbehörde**
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss **erforderlich** ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche **Folgen die Nichtbereitstellung** hätte

Informationspflichten (Art. 13 DSGVO)

- das Bestehen einer **automatisierten Entscheidungsfindung** einschließlich **Profiling** - zumindest in diesen Fällen - aussagekräftige Informationen über die **involvierte Logik** sowie die Tragweite und die angestrebten **Auswirkungen** einer derartigen Verarbeitung für die betroffene Person
- beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen **anderen Zweck** weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen **über diesen anderen Zweck** zur Verfügung

Informationspflichten (Art. 14 DSGVO)

- werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zusätzlich zu den Angaben aus Art. 13 DSGVO mit:
  - aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen
- Diese Informationen (Art. 13 und 14) müssen nur einmalig erteilt werden, Änderungen sind aber ebenfalls mitzuteilen.

Anforderungen an die Einwilligung

- Der Verantwortliche (also z.B. das Unternehmen) muss **nachweisen** können, dass die betroffene Person eingewilligt hat.
- Wenn die Einwilligung mit anderen Erklärungen abgegeben werden soll, „muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist."
- Teile der Einwilligung, die gegen die DSGVO verstoßen sind unwirksam.

(vgl. Art. 7 DSGVO)

Freiwilligkeit der Einwilligung

- „Die Einwilligung gilt **nicht** als freiwillig erteilt,
  - wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht **gesondert** eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder
  - wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung **abhängig** ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist."

(Erwägungsgrund 43, Satz 2 DSGVO , Hervorhebungen von mir)

Risikobewertung in der DSGVO

- An vielen Stellen in der DSGVO ist von der Berücksichtigung der **Risiken für die Freiheiten und Grundrechte der betroffenen Personen** die Rede.
  - Art. 24 Abs. 1 - Verantwortung des für die Verarbeitung Verantwortlichen - Erwägungsgründe 74, 75, 76 und 77
  - Artikel 25 Abs. 1 - Datenschutz durch Technikgestaltung und durch datenschutz-freundliche Voreinstellungen
  - Artikel 27 Abs. 2 - Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern
  - Erwägungsgrund 81 (zu Art 28 Auftragsverarbeiter)
  - Artikel 30 Abs. 5 - Verzeichnis von Verarbeitungstätigkeiten
  - Artikel 32 Abs. 1 und 2 - Sicherheit der Verarbeitung – Erwägungsgrund 81

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Risikobewertung in der DSGVO

- Artikel 33 Abs. 1 - Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde – Erwägungsgrund 87
- Artikel 34 Abs. 1, 3 und 4 - Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person – Erwägungsgründe 86 und 87
- Artikel 35 Abs. 1, 7 und 11 - Datenschutz-Folgenabschätzung – Erwägungsgründe 84, 90, 91
- Artikel 36 Abs. 1 und 2 - Vorherige Konsultation (der Aufsichtsbehörde) – Erwägungsgründe 94 und 96
- Artikel 39 Abs. 2 - Aufgaben des Datenschutzbeauftragten
- Erwägungsgrund 98 zu Artikel 40 – Verhaltensregeln

=> Eine Abschätzung der Risiken für die Grundrechte und Freiheiten der betroffenen Personen ist für jede Verarbeitung personenbezogener Daten erforderlich!

Datenschutz durch Technikgestaltung Art. 25 Abs. 1 DSGVO

- Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen - wie z.B. Pseudonymisierung -, die dafür ausgelegt sind,
  - die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und
  - die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und
  - die Rechte der betroffenen Personen zu schützen
- Die technischen und organisatorischen Maßnahmen werden getroffen
  - unter Berücksichtigung des Stands der Technik
  - der Implementierungskosten und
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
  - der unterschiedlichen Eintrittswahr-scheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

Datenschutz durch datenschutzfreundliche Voreinstellungen – Art. 25 Abs. 2 DSGVO

- Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen,
  - dass durch Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist.
- Diese Verpflichtung gilt für
  - die Menge der erhobenen personenbezogenen Daten,
  - den Umfang ihrer Verarbeitung,
  - ihre Speicherfrist und
  - ihre Zugänglichkeit
- Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.
- Vgl. auch Erwägungsgrund 78 (https://dsgvo-gesetz.de/erwaegungsgruende/nr-78/)

Sicherheit der Verarbeitung Art. 32 Abs. 1 DSGVO

- Der Verantwortliche und der Auftragsverarbeiter treffen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
- Dies geschieht unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten und
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Sicherheit der Verarbeitung Art. 32 Abs. 1 DSGVO

- Die technischen und organisatorischen Maßnahmen schließen unter anderem Folgendes ein:
  - die Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Sicherheit der Verarbeitung Art. 32 Abs. 2 DSGVO

- Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere
  - durch unbeabsichtigte oder unrechtmäßige Vernichtung,
  - Verlust,
  - Veränderung oder
  - von unbefugter Offenlegung bzw. von unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden

Sicherheit der Verarbeitung Art. 32 Abs. 3 DSGVO

Um die Erfüllung der in Art. 32 DSGVO genannten Anforderungen nachzuweisen können, können

- genehmigte Verhaltensregeln (Art. 40 DSGVO) oder
- genehmigte Zertifizierungsverfahren (Art. 42 DSGVO)

herangezogen werden.

Sicherheit der Verarbeitung Art. 32 Abs. 4 DSGVO

Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass

- ihnen unterstellte natürliche Personen, personenbezogene Daten nur weisungsgebunden verarbeiten

➡ Aus der „Verpflichtung auf das Datengeheimnis“ aus § 5 BDSG-alt wird eine „Verpflichtung auf den Datenschutz“

Gewährleistungsziele in der DSGVO

Schutz- bzw. Gewährleistungsziel	Fundstelle DSGVO
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben	Art. 5, Abs. 1 Buchst. a
Transparenz	Art. 5, Abs. 1 Buchst. a, Art. 13 und Art.14
Zweckbindung	Art. 5, Abs. 1 Buchst. b
Datenminimierung	Art. 5, Abs. 1 Buchst. c
Speicherbegrenzung (Erforderlichkeitsgebot)	Art. 5, Abs. 1 Buchst. e
Richtigkeit	Art. 5, Abs. 1 Buchst. d
Integrität	Art. 5, Abs. 1 Buchst. f, Art. 32, Abs. 1 Buchst. b
Vertraulichkeit	Art. 5, Abs. 1 Buchst. f, Art. 32, Abs. 1 Buchst. b
Verfügbarkeit und Belastbarkeit beim Betrieb	Art. 32, Abs. 1 Buchst. b
Verfügbarkeit bei einem physischen oder technischen Zwischenfall	Art. 32, Abs. 1 Buchst. c

Beispiele für Folgerungen

- Software und Systeme müssen über datenschutzfreundliche Voreinstellungen verfügen.
- Einwilligungen* müssen standardmäßig deaktiviert sein
- Freiwillige Datenfelder müssen als solche gekennzeichnet sein
- Unternehmen sollten auf Softwarehersteller und Dienstleister hinwirken, dass von diesen angebotene Software und Dienstleistungen datenschutzkonform entwickelt werden
  - Dies kann durch entsprechende Anforderungen bei der Ausschreibung oder der Angebotseinholung unterstützt werden
- Es ist künftig erforderlich, die ergriffenen technischen und organisatorischen Maßnahmen zu dokumentieren und den Nachweis zu erbringen, dass sie regelmäßigen daraufhin überprüft werden, ob sie noch ausreichend sind und noch dem Stand der Technik entsprechen.

*) zur Freiwilligkeit von Einwilligungen im Beschäftigungsverhältnis wird auf § 28 Abs. 2 BSDG-neu verwiesen.

Was ändert sich am Direktmarketing (Fundraising) durch die DSGVO?

- Die DSGVO kennt das Listenprivileg des BDSG-alt für die werbliche Nutzung von Daten nicht, aber die DSGVO ermöglicht die werbliche Nutzung personenbezogener Daten im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Buchstabe f:
  - „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden. “ (EWG 47, Satz 7)
  - Damit kann die Auswertung vorhandener personenbezogener Daten im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Buchstabe f zulässig sein, z.B. zur Selektion der Empfänger/innen (aber die Informationspflichten sind zu beachten).
- Diese Aussage gilt in **Bezug auf den Anspracheweg nur** für die **konventionelle** Ansprache per Post, aber nicht für die Ansprache durch das eDirektmarketing, da das eDirektmarketing derzeit durch die ePrivacy-Richtlinie und den entsprechenden nationalen Umsetzungsgesetzen geregelt ist (s.u.).
- Die ePrivacy-Richtlinie wird durch die DSGVO nicht abgeändert. Auch die nationalen Umsetzungsgesetze bleiben (bis auf weiteres*) gültig.

*) solange die ePrivacy-Richtlinie nicht durch die derzeit im Gesetzgebungsverfahren befindliche EU-ePrivacy-Verordnung ersetzt wird.

Vereinfachte Darstellung Ansprache-wege Direkt-marketing

Anspracheweg	Zulässigkeitsvoraussetzung
Postalisch	Nach Interessenabwägung zulässig bis auf **Widerspruch** (vgl. Art. 6 Abs. 1 Buchstabe f i.V.m. Art. 21 Abs. 2 ff DSGVO und EWG 47 Satz 7 DSGVO)
Telefonisch	Bei **Verbrauchern:** Ausdrückliche Einwilligung (§ 7 UWG) bis auf **Widerruf** der Einwilligung; bei **sonstigen Markteilnehmern:** mutmaßliche Einwilligung
FAX	Ausdrückliche Einwilligung
E-Mail, SMS u.ä.	Ausdrückliche Einwilligung (§ 7 UWG) bis auf **Widerruf** der Einwilligung oder „Vereinfachte Erlaubnis“ nach § 7 Abs. 3 bis auf **Widerspruch**

Gliederung

1.1 Das neue Datenschutzrecht in Europa
1.2 Was ändert sich durch die DSGVO?
1.3 Das neue Bundesdatenschutzgesetz

Struktur des BDSG-neu

- Das am 25. Mai 2018 in Kraft tretende neue Bundesdatenschutzgesetz (BDSG-neu) enthält vier Teile:
  - **Teil 1 - Gemeinsame Bestimmungen**
  - **Teil 2 - Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679**
  - Teil 3 - Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680
  - Teil 4 - Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten
- Für **Unternehmen, Vereine, Institutionen** sind grundsätzlich nur die **Teile 1 und 2** des BDSG-neu relevant.

Auswirkungen des BDSG-neu

Wichtig:

- Im Zweifelsfall geht die DSGVO dem BDSG-neu vor
- Bereichsspezifische Regelungen (die nicht durch die DSGVO verdrängt werden) gehen weiterhin denen des BDSG-neu vor (z.B. Regelungen aus TKG, UWG §7, SGB,…)

Beschäftigtendatenschutz im BDSG-neu

§ 26 BDSG-neu regelt die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

- Hier werden im wesentlichen die bisherigen Regelungen des § 32 BDSG-alt übernommen und diese um Regelungen zur Beurteilung der Freiwilligkeit von Einwilligungen ergänzt.

Beschäftigtendatenschutz im BDSG-neu

„Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere

- die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie
- die Umstände, unter denen die Einwilligung erteilt worden ist,

zu berücksichtigen.

Freiwilligkeit kann insbesondere vorliegen, wenn

- für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder
- Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.“

(§ 26 Abs. 2 Satz 1 und 2 BDSG-neu)

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Benennung von Datenschutz-beauftragten im BDSG-neu

Die bisherigen Regelungen für Unternehmen zur Bestellpflicht und zur Unkündbarkeit eines/einer zu bestellenden Datenschutzbeauftragten aus § 4f BDSG-alt bleiben grundsätzlich erhalten.

- Die Regelung des § 38 BDSG-neu ergänzt die Regelung aus Art. 37 DSGVO unter welchen Bedingungen ein/e DSB verpflichtend zu benennen ist:
  - wenn mindestens 10 Personen in der Regel mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind und
  - unabhängig von der Anzahl der Beschäftigten,
    - wenn Verarbeitungstätigkeiten durch geführt werden, die eine Datenschutzfolgen-Abschätzung erfordern oder
    - wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung

Hinweis: Die DSGVO und das BDSG-neu sowie weitere bereichsspezifische Datenschutzregelungen sind auch dann einzuhalten, wenn kein/e DSB zu benennen ist! – Das galt bereits auch schon für das bisherige BDSG –

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Agenda

0	Vorstellung
1	Das neue Datenschutzrecht in Europa
2	DSGVO – Umsetzung in 10 Schritten
3	Hilfsmittel

DSGVO-Umsetzung – Aufwand?

Der Aufwand zur Umsetzung der Anforderungen der DSGVO hängt in erster Linie davon ab, in welchem Umfang Sie das **bisherige** Datenschutzrecht bereits umgesetzt haben

- Ein vorhandenes Verfahrensverzeichnis (nach § 4e i.V.m. § 4g, Abs. 2 und 2a BDSG-alt) lässt sich leicht in das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO überführen
- Eine Dokumentation der nach § 9 BDSG-alt nebst Anlage hierzu ergriffenen technischen und organisatorischen Maßnahmen ist eine sehr gute Basis für die Dokumentation der nach Art. 24 und 32 DSGVO erforderlichen Maßnahmen.
- Wenn bereits ADV-Vereinbarungen nach § 11 BDSG-alt mit Dienstleistern bestehen, sollte es leicht möglich sein, mit diesen AV-Vereinbarungen nach Art. 28 DSGVO abzuschließen.

DSGVO-Umsetzung als Projekt

Es empfiehlt sich, die Umsetzung der DSGVO im Verein durch ein **Umsetzungsprojekt** zu begleiten

- Falls noch nicht geschehen: Sensibilisierung von Vorstand, Geschäftsführung und evtl. vorhandenen Beschäftigten
- Analyse der aktuellen Situation um die zu erledigenden Punkte zu identifizieren
- Festlegung der zeitlichen Abläufe und Verantwortlichkeiten in Bezug auf die Umsetzung
  - evtl. unter Einbeziehung externer Ressourcen – sofern noch welche verfügbar sind
- Beginn und Nachverfolgung der Umsetzung

Umsetzung der DSGVO im Verein

- Wenn Sie mit der Umsetzung der DSGVO noch nicht begonnen haben oder gerade am Anfang stehen, werden Sie es kaum noch schaffen, die DSGVO bis zum 25. Mai 2018 zu 95 % umzusetzen, auch nicht zu 90 %.
- Das sollte aber weder dazu führen, dass Sie nun den Kopf in den Sand stecken noch dazu, dass Sie in Panik verfallen.
- Auch hier gilt: **In der Ruhe liegt die Kraft**
- Wir starten daher mit einer **Minimalumsetzung in 10 Schritten!**

Minimalumsetzung der DSGVO

1. Erstellen Sie das Verzeichnis von Verarbeitungstätigkeiten.

- Dieses Verzeichnis ist der Kern oder die Basis Ihres Datenschutzmanagements.
- **Hierzu gibt es vielfältige Hilfsmittel.**
  - Es gibt Leitfäden von der Bitkom und der GDD.
  - Es gibt Muster vom Bayerischen Landesamt für Datenschutzaufsicht, die auch für Verantwortliche außerhalb Bayerns genutzt werden können.
  - Es gibt vorausgefüllte Muster eines Datenschutzanwalts.
  - Siehe: http://vvvt.de oder https://dsgvo.expert/MatV3T

1. Muster für das Verzeichnis von Verar-beitungs-tätigkeiten.

- Auch wenn das Muster vom BayLDA erstellt wurde, ist es bundesweit nutzbar.

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer/ Sozialabgaben ...	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	• Name und Adressen • Eintrittsdatum • Sportbereiche ...	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	28.02.2018	Außendarstellung	• Mitglieder • Webseitenbesucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Minimalumsetzung der DSGVO

2. Benennung eines/einer Datenschutzbeauftragten

- Prüfen Sie, ob Sie eine/n Datenschutzbeauftragten benennen müssen (s.o. bzw. Art. 37 DSGVO und § 38 BDSG-neu)
- Falls ja,
  - überlegen Sie, ob Sie ein Mitglied oder eine/n Beschäftigten für diese Tätigkeit haben oder, ob Sie diese Funktion an eine qualifizierte externe Person übertragen wollen.
  - Suchen Sie die passende Person (intern oder extern)
    - Geschäftsführung und Vorstand scheiden leider aus.
  - Benennen Sie den/die Datenschutzbeauftragte/n – am besten schriftlich
  - Veröffentlichen Sie die Kontaktdaten auf der Website und melden Sie die Kontaktdaten an Ihre zuständige Datenschutzaufsichtsbehörde

Minimalumsetzung der DSGVO

3. Erstellen Sie die Datenschutzhinweise gemäß Art. 13, 14 und 21 DSGVO

- Was sich in den nachfolgend genannten Datenschutzhinweisen enthalten sein muss, ergibt sich direkt aus den Art. 13, 14 und 21 DSGVO (s.o.)
- Überarbeiten Sie Ihre Datenschutzhinweise auf Ihrer Website.
- Erstellen Sie die Datenschutzhinweise auch für Ihre Mitglieder, Ihre LieferantInnen (darunter gibt es sicher auch Einzelunternehmer oder es sind zumindest Ansprechpersonen in Ihrem EDV-System hinterlegt) und auch für Ihre Beschäftigten und BewerberInnen.
- Evtl. können Sie sich auch an den Datenschutzhinweisen orientieren, die Sie von Ihrer Bank erhalten haben.
- In diesen Informationen sind die Kontaktdaten des/der Datenschutz-beauftragten anzugeben. Wenn Sie keinen benennen müssen, geben Sie dies am besten auch an (dies erspart entsprechende Nachfragen).

Minimalumsetzung der DSGVO

4. Legen Sie fest, wer in Ihrem Verein für die Umsetzung des Datenschutzes verantwortlich ist.

- **Nein**, das ist **nicht** der oder die Datenschutzbeauftragte.
- Der oder die Datenschutzbeauftragte berät den Verein nur und überwacht die Einhaltung des Datenschutzes
- Diese für den Datenschutz verantwortliche Person kann jemand aus dem Vorstand oder der Geschäftsführung des Vereins sein.

Minimalumsetzung der DSGVO

5. Dokumentieren Sie die technischen und organisatorischen Maßnahmen zur Datensicherheit

- Aktualisieren Sie Ihre datenschutz-relevanten Dokumente auf den aktuellen Stand oder erstellen Sie diese.
- Versehen Sie diese Dokumente mit Datum und Versionsnummer
- Zu diesen Dokumenten gehören insbesondere:
  - Netzwerkübersicht, Soft- und Hardwareübersicht
  - Datenschutzrichtlinien, Arbeitsanweisungen, ggfls. Betriebs- oder Dienstvereinbarungen
  - Festlegung der Verantwortlichkeiten
  - Dokumentation der weiteren technischen und organisatorischen Maßnahmen zur Datensicherheit nach Art. 24 und 32 DSGVO – Eine Untermenge hiervon sind die IT-Sicherheitsmaßnahmen

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Minimalumsetzung der DSGVO

6. Sorgen Sie für korrekte Beauftragung Ihrer Dienstleister

- Verschaffen Sie sich auch einen Überblick welche Dienstleister Sie im Zusammenhang mit der Verarbeitung personenbezogener Daten beauftragt haben (hierzu gehört auch die Akten- und Datenträgervernichtung, der Newsletterversand, etc.)
- Sorgen Sie dafür, dass Sie für die Dienstleistungen, die eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO sind, eine Vereinbarung zur Auftragsverarbeitung abschließen.
- Entsprechende Muster und Leitfäden sind verlinkt unter https://dsgvo.expert/MatAV

Minimalumsetzung der DSGVO

7. Prüfen Sie Ihre Einwilligungsformulare

- Falls Sie mit Einwilligungen arbeiten, prüfen Sie, ob Ihre Einwilligungsformulare den Anforderungen aus Art. 7 DSGVO (und ggfls. den Anforderungen des Art. 8 DSGVO) genügen.
- Passen Sie Ihre Einwilligungsformulare bei Bedarf an.
- Stellen Sie sicher, dass die betroffenen Personen darüber informiert werden, in welche Art der Datenverarbeitung Sie einwilligen und zu welchen Zwecken Sie die Einwilligung erheben.
- Auf das Recht die Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen muss unbedingt hingewiesen werden.
- Es dürfen keine Ankreuzfelder für Einwilligungen im Voraus angekreuzt sein oder gar als Pflichtfelder gekennzeichnet sein

Minimalumsetzung der DSGVO

8. Frühjahrsputz

- Räumen Sie Ihre Mitgliederdatenbanken, Ihre Personalakten und ihre sonstigen Sammlungen personenbezogener Daten auf.
- Löschen Sie Daten, deren gesetzlichen Aufbewahrungspflichten abgelaufen sind – oder bei denen es keine gibt –, wenn es keine nachvollziehbaren Gründe gibt, warum Sie die Daten noch für die – in dem Verzeichnis von Verarbeitungstätigkeiten – festgelegten Zwecke benötigen.
- Vernichten Sie Altakten, die Sie nicht mehr benötigen. Wenn Sie eine externe Firma beauftragen: Das ist eine Auftragsverarbeitung nach Art. 28 DSGVO. Schließen also eine entsprechen AV-Vereinbarung ab und vergewissern Sie sich, dass die technischen und organisatorischen Maßnahmen der Aktenvernichtungsfirma der Sensibilität der zu vernichtenden Akten oder Datenträgern entsprechen.
- Starten Sie ein Projekt zur Erstellung eins Lösch- und Anonymisierungskonzepts

Minimalumsetzung der DSGVO

9. Folgearbeiten

- Da Sie bis zum 25. Mai 2018 vermutlich nicht alle genannten Punkte abarbeiten können und es evtl. auch noch weiteren Umsetzungsbedarf geben könnte, sollten Sie sich – rechtzeitig vor dem 25. Mai 2018 – einen Zeitplan erstellen, bis wann Sie weitere wesentliche Punkte zur Umsetzung der DSGVO erledigt haben wollen.
- Evtl. ist es sinnvoll im 3. Quartal ein Datenschutzaudit (extern oder intern) durchzuführen, damit Sie eine Übersicht erhalten, wie Ihr aktueller Umsetzungsstand ist und welche Tätigkeiten noch erforderlich sind.
  - Ja, es wäre sinnvoll, dies eigentlich als erstes zu erledigen. Aber wenn Sie hierbei auf externe Unterstützung angewiesen sein sollten, dürfte es kaum möglich sein, hier noch zeitnah eine qualifizierte Kraft beauftragen zu können.
- Arbeiten Sie diesen Plan systematisch, in aller Ruhe, aber auch konsequent ab.
- Denken Sie daran: 2019/2020 wird die ePrivacy-Verordnung kommen. Auch diese hat vermutlich Auswirkungen auf Ihre Website!

Minimalumsetzung der DSGVO

10. Regelmäßige Revision

- Prüfen Sie regelmäßig – am besten einmal jährlich –
  - ob Ihre Datenschutzdokumentation noch aktuell ist,
  - ob Ihr Verzeichnis der Verarbeitungstätigkeiten noch aktuelle und vollständig ist
  - ob Ihre Dienstleisterübersicht noch aktuelle und vollständig ist,
  - ob die technischen und organisatorischen Maßnahmen noch ausreichend sind und noch dem – inzwischen evtl. weiterentwickelten – Stand der Technik entsprechen
  - ob Ihre Beschäftigten und ehrenamtlich tätigen Mitglieder eine Auffrischung oder Sensibilisierung zum Datenschutz benötigen (manches gerät ja im Laufe der Zeit vielleicht in Vergessenheit)
  - ob Ihre Datenschutzorganisation über ausreichende Ressourcen verfügt und die Aufgabenzuordnung im Datenschutz noch Ihren Anforderungen entspricht.

Resümee

- Wenn Sie die vorgenannten 10 Punkte in Ruhe aber konsequent umsetzen, ist der Grad der Umsetzung der DSGVO am 25. Mai 2018 vermutlich deutlich unter 95 %. Aber Sie können – sollte ein Mitglied oder gar die Aufsichtsbehörde nachfragen – zumindest nachweisen, dass Sie einige wesentliche Punkte bereits erledigt haben und in den anderen Bereichen auf einen guten Weg sind.
- Sie sollten allerdings die verbleibende Zeit nutzen und alle möglichen Ressourcen mobilisieren, um möglichst viele der genannten Arbeitspakete anzugehen und soweit wie möglich umzusetzen
- Zu diesen Ressourcen können – auch jetzt noch – externe Ressourcen gehören.
- Gerade für die Zeit nach dem 25. Mai 2018 sollten Sie sich bereits jetzt Gedanken machen, ob Sie externe Unterstützung in Anspruch nehmen wollen und sich gegebenenfalls jetzt schon um Angebote kümmern und entsprechende Aufträge erteilen. Dann sind Sie auf der sicheren Seiten wenn andere Unternehmen durch Nachrichten über erste Bußgelder aufwachen und plötzlich doch noch aktiv werden.

Agenda

0 Vorstellung
1 Das neue Datenschutzrecht in Europa
2 DSGVO – Umsetzung in 10 Schritten
3 Hilfsmittel

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Hilfsmittel zur Umsetzung

- Hilfsmittel zur Umsetzung sind unter https://dsgvo.expert/material verlinkt.
- Hier finden Sie Materialien
  - zur Auftrags(daten)verarbeitung
  - zum BDSG-neu
  - zum Datenschutz im Verein: **https://dsgvo.expert/Verein**
  - Zur DSGVO-Umsetzung für kleine, mittlere und Kleinst-Unternehmen und im Verein: **https://dsgvo.expert/Mat-KMU**
  - zur Datenschutz-Folgenabschätzung
  - zum Verzeichnis von Verarbeitungstätigkeiten
  - zur Videoüberwachung

  und einiges mehr

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Noch Fragen?

Werner Hülsmann – Datenschutzwissen.de

- Münchener Str. 101 / Geb. 01
  85737 Ismaning
  Tel.: 089 / 51 30 569-7, FAX: -8
- Pappelhof 12
  14478 Potsdam
  Tel. 030 / 22 43 84 36

Mobil: 0177 / 28 28 681

E-Mail: wh@datenschutzwissen.de

https://DSGVO.expert & https://datenschutzwissen.de