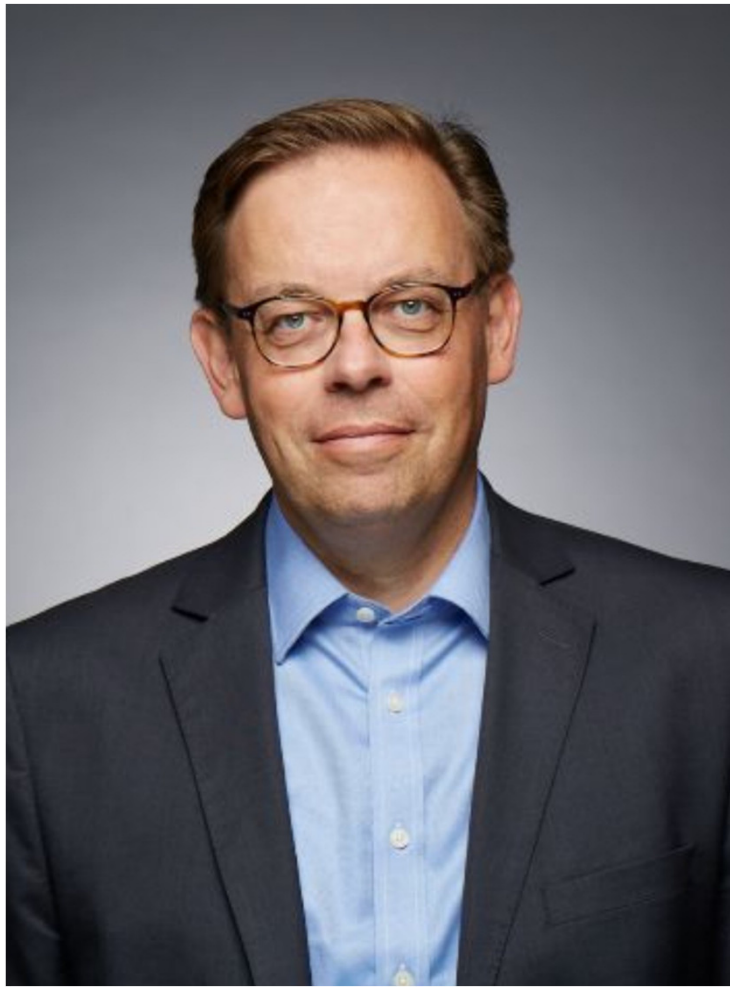
DORNBACH
Unsere Kompetenz – Ihre Zukunft

UNSERE KOMPETENZ - IHRE ZUKUNFT

Hamburger Sport-Kongress 2018

03.11.2018 in Hamburg



DORNBACH GMBH RECHTSANWALTSGESELLSCHAFT

Der Referent:

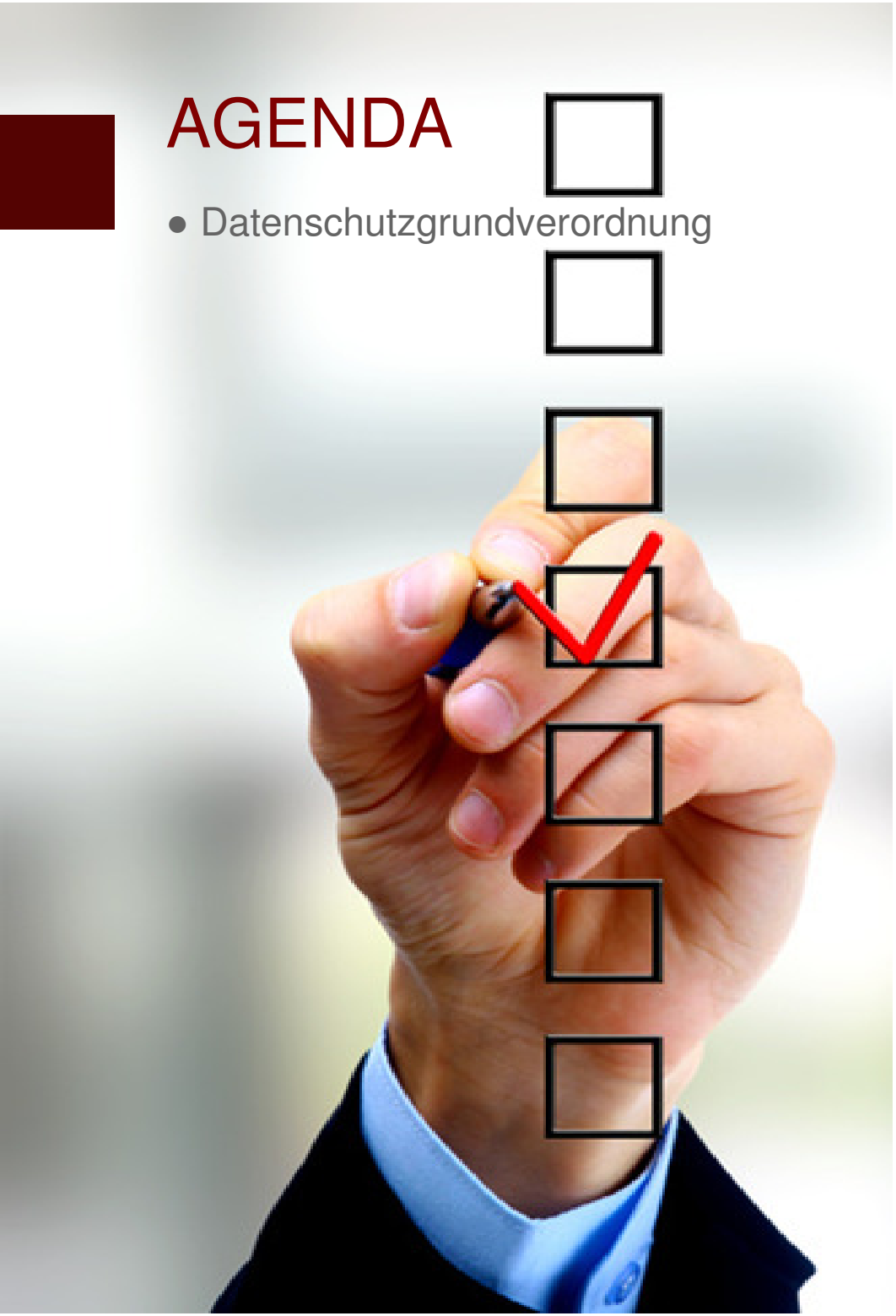
Ralf Wickert
Fachanwalt für Steuerrecht
Fachanwalt für Arbeitsrecht

Anton-Jordan-Straße 1
56070 Koblenz

Tel.: +49 261 9431 142
Email: rwickert@dornbach.de

AGENDA

- Datenschutzgrundverordnung



DORNBACH
Unsere Kompetenz – Ihre Zukunft

- **Einführung und Überblick**
- **Änderungen durch die DS-GVO**
- **Wie funktioniert Datenschutz?**
- **Wer benötigt einen betrieblichen Datenschutzbeauftragten?**
- **Welche personenbezogenen Daten dürfen verarbeitet werden?**
- **Welche Informationspflichten treffen Betriebe?**
- **Was passiert bei einer Datenpanne?**
- **Welche organisatorischen Maßnahmen sind zu treffen?**

Einführung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Überblick

- DS-GVO ist am 25.05.2018 automatisch in Kraft getreten (deutsches Umsetzungsgesetz ist nicht erforderlich), vgl. Art. 99 DS-GVO. BDSG alt sowie Bisherige Landesdatenschutzgesetze treten außer Kraft.
- DS-GVO wirkt unmittelbar und zwingend sowohl für private als auch für öffentliche Stellen (teilweise Privilegien für Justiz und Polizei). DS-GVO besteht aus 99 Artikeln und 173 Erwägungsgründen.
- Erwägungsgründe sind vergleichbar mit Gesetzesbegründung im deutschen Gesetzgebungsverfahren
- DS-GVO enthält einen Mindestschutz, der europaweit gelten soll.
- DS-GVO enthält an verschiedenen Stellen sog. Öffnungsklauseln für den nationalen Gesetzgeber.
- Folge: In Deutschland wurde BDSG (neu) verabschiedet, um nationalen Regelungsspielraum festzulegen und Öffnungsklauseln der DS-GVO auszuschöpfen

Checkliste Änderungen DS-GVO

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Die wichtigsten Änderungen im Überblick

- Drastisch erhöhte Bußgelder
- Erweiterte zivilrechtliche Haftung
- Stark erweiterte Dokumentations- und Nachweispflichten
- Datenschutz-Folgeabschätzung statt der Vorabkontrolle nach BDSG
- Risikobasierter Datenschutz
- Sehr stark erweiterte Transparenzanforderungen
- Datenschutz durch Technik
- Datenschutz durch Voreinstellungen
- Erweiterte Meldepflichten bei Datenpannen
- Verschärfte Löschvorschriften
- Recht auf Vergessenwerden (im Internet)
- Striktere Regelungen bei Zweckänderungen
- Grundsätzlich möglicher Datenaustausch im Konzern.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Verein in der Systematik des Datenschutzes

- **<u>Rechtslage nach DS-GVO</u>**
- → **„Verantwortlicher“**:

  - natürliche Personen

  - juristische Personen

  - Behörden und Einrichtungen
- → Keine Differenzierung danach, ob sie privatrechtlich oder öffentlich rechtlich organsiert sind. Jeder Verein unterfällt der DS-GVO.
- → DS-GVO enthält **kein** Konzernprivileg (Art. 22 Abs. 3a der Entwurfsfassung des DS-GVO enthielt Konzernprivileg)
- → EG 48: Innerhalb einer „Vereinsgruppe“ wird „berechtigtes Interesse“ an der Übermittlung von Daten für interne Verwaltungszwecke.
- ACHTUNG: Nach EuGH ist Verein für Fanpage z.B. bei Facebook verantwortlich!

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Der Datenschutzbeauftragte im Verein

Bisherige Rechtslage

- **§ 4f BDSG: Verein musste Datenschutzbeauftragten bestellen, wenn:**
  - mindestens 10 „Personen“ ständig mit der Verarbeitung automatisierter Daten beschäftigt sind
  - oder mindestens 20 „Personen“ Daten auf andere Weise als automatisiert verarbeiten (in der Praxis irrelevant).

- **Interner/externer Datenschutzbeauftragter**
  - Interner Datenschutzbeauftragter hat besonderen Kündigungsschutz (§ 4f Absatz 3 Satz 5 BDSG
  - Weisungsfreiheit und Verantwortlichkeit gegenüber Leitung des Vereins

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Der Datenschutzbeauftragte im Verein

Rechtslage nach DS-GVO

- → Beachte: § 38 BDSG neu gilt nur für „nichtöffentliche Stellen“, also nach § 2 Abs. 4 BDSG *neu* private Rechtsträger (d.h. Verein). Auch hier gilt die 10-Personen-Grenze.

→ Datenschutzbeauftragter nach Art. 37 DS-GVO unterliegt keinem besonderen Kündigungsschutz

- Aber: § 38 Abs. 2 iVm. § 6 Abs. 4 BDSG *neu* führt zu Kündigungsschutz, wenn Bestellpflicht aus § 38 BDSG folgt.
- Fraglich: Kündigungsschutz auch, wenn Bestellpflicht originär aus Art. 37 DS-GVO folgt? Nach dem Wortlaut nicht der Fall.
- Abberufung nur aus wichtigem Grund iSv. § 626 BGB.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Der Datenschutzbeauftragte im Verein

- Neben § 38 BDSG neu gibt es auch eine Bestellpflicht direkt aus Art. 37 DS-GVO, wenn:

  - Kerntätigkeit des Vereins „Überwachung“ von Personen (bei Sportvereinen nicht der Fall) oder
  - Kerntätigkeit in der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DS-GVO (bei Sportvereinen allenfalls in Zusammenhang mit Behindertensport denkbar)

- Nach Art. 37 Abs. 2 DS-GVO können „**Vereinsgruppen**“ gemeinsamen Datenschutzbeauftragten bestellen.

  → Voraussetzungen können bei größeren Organisationen vorliegen.

  → **Verstoß gegen Bestellungspflicht:**

  Art. 83 Abs. 4 lit. a) DS-GVO: **Bußgeld** (Obergrenze – theoretisch – 10 Mio EUR). In der Praxis ist jedenfalls eine empfindliche Bebußung zu erwarten.

- Bußgeldtatbestand gilt auch bei Bestellpflicht nach BDSG *neu*.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Personenbezogene Daten

Rechtslage nach DS-GVO

- **Art. 4 Nr. 1 DS-GVO: Information mit Bezug zu einer bestimmten oder bestimmbaren natürlichen Person**
- **- Fraglich auch hier: Relativer oder objektiver Personenbezug?**
  - Reicht Erkenntnismöglichkeit des Verantwortlichen?
  - Reicht irgendeine Erkenntnismöglichkeit?
  - EG 26: Maßgeblich soll sein, welche Mittel der Verantwortliche „nach allgemeinem Ermessen wahrscheinlich einsetzen“ wird.

    Also: Hinweis auf relativen Personenbezug
  - EG 30: IP-Adresse soll nicht zwingend personenbezogenes Datum sein. Aber in der Regel anzunehmen (Datenerhebung bei Besuch der Webseite des Sportvereins)
- **Künftige technologische Entwicklung ist zu berücksichtigen**

Fotos im Datenschutz

DORNBACH
Unsere Kompetenz – Ihre Zukunft

- **Bis DS-GVO: KUG war neben BDSG anwendbar, da spezielle Regelung im Bereich der Fotografien**
- **Ab Inkrafttreten der DS-GVO: Grundsätzlicher Regelvorrang der DS-GVO als europäische Verordnung mit unmittelbarer Geltung in den Mitgliedstaaten**
  - DS-GVO enthält keine allgemeine Öffnungsklausel für KUG
  - Digitale Fotos sind Fälle automatisierter Verarbeitung im Sinne von Art. 2 DS-GVO
- **OLG Köln (18.06.2018): Im journalistischen Bereich bleiben Fotos weiterhin privilegiert – KUG ist anwendbar – *Sportberichterstattung in der Lokalpresse***
- **Außerhalb Art. 85 DS-GVO?**
  - Teilweise: KUG gilt nicht, sondern nur DS-GVO
  - Teilweise (z.B. Andrea Vosshoff BfDI): KUG gilt im Bereich der Fotografien weiter
- **Jedenfalls zentrale Pflicht: Transparenzgebot**

Fotos im Datenschutz

DORNBACH
Unsere Kompetenz – Ihre Zukunft

- **Folge für Sportvereine**
  - Fotos im journalistischen Bereich = KUG bleibt jedenfalls anwendbar! Privilegierung insb. in Fällen von § 23 KUG
  - Fotos im nicht-journalistischen Bereich (z.B. Webseite des Sportvereins) = Selbst wenn Maßstab die DS-GVO wäre und KUG nicht gelten würde
- **Rechtsgrundlage nach Art 6 DS-GVO erforderlich (Einwilligung oder häufig berechtigte Interessen)**
- **Immer: Transparenzgebot von Art. 5 DS-GVO erfüllen (Foto-Banner)**
  - Wird fotografiert ? (Opt-Out)
  - Wer (Verantwortlicher) fotografiert?
  - Wozu wird fotografiert? (Webseite/Soziale Medien etc.)

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Zentrale Grundsätze der Datenverarbeitung

Art. 5 DS-GVO beschreibt die zentralen Grundsätze der Datenverarbeitung nach der DS-GVO:

- → Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz.
- → Zweckbindung
- → Datenminimierung
- → Richtigkeit
- → Speicherbegrenzung
- → Integrität und Vertraulichkeit.

- Folge der Transparenzpflicht ist die Datenschutzerklärung der Webseite (Welche Datenverarbeitung erfolgt bei Besuch der Webseite – insb. Cookies/Analysetools/Google Maps etc). Dies muss transparent gemacht werden!

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Grundsätzliche Systematik der Rechtsgrundlagen

Grundprinzip des Datenschutzes ist das Verbot mit Erlaubnisvorbehalt

- Inhalt: Die Nutzung fremder Daten ist verboten, es sei denn:

  - der Betroffene hat eingewilligt oder

  - es gibt einen gesetzlichen Erlaubnistatbestand.

- Dieses Grundprinzip findet sich in Art. 5 und 6 DS-GVO unverändert (Argument: Verankerung im Grundrechtsschutzsystem des Grundgesetz oder der europäischen Grundrechte)

- DS-GVO: Grundsätzliche Sperrwirkung für nationale Gesetze, es sei denn Öffnungsklausel greift.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Die Einwilligungserklärung

- **Rechtslage nach DS-GVO**
- Einwilligungserklärung ist nach Art. 6 Abs. 1 lit. a) DS-GVO zentraler Erlaubnistatbestand.
- - EG 32: elektronische oder mündliche Form ist zulässig! Aber bei Mündlichkeit natürlich Nachweisproblem
- - EG 32: Erforderlich: „eindeutige bestätigende Handlung“
  - „bereits angekreuzte Kästchen oder Untätigkeit reicht nicht“
  - Anders noch BGH (NJW 2008, 3055; NJW 2010, 864): Zulässigkeit sog. *Opt-Out Lösungen*
  - Folge: Überprüfung von website-Inhalten (z.B. Beitrittserklärungen oder Bestellvorgängen etwa bei Fortbildungsveranstaltungen).
- - EG 32: Auch die Auswahl technischer Einstellungen kann Einwilligung folgen lassen (z.B. Verwendung von sog. Cookies iSv. Art. 5 Abs. 3 Satz 1 der ePrivacy-RL durch Browsereinstellungen).

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Die Einwilligungserklärung

- **<u>Koppelungsverbot, Art. 7 Abs. 4 DS-GVO</u>**
- → Keine Abhängigkeit der Einwilligung bei Vertragserfüllung etwa mit sachfremden Erwägungen.
  - Beispiel: Reduzierte Seminargebühr bei bestimmten Einwilligungen in zulässige Datennutzung (*keine Bezahlung mit eigenen Daten*).
  - EG 43: Bei Kopplung wird fehlende Freiwilligkeit vermutet.

- → Konzept der sog. „Differenzierten Einwilligung“
  - Getrennte Einwilligung bei getrennten Verarbeitungsvorgängen.
  - Keine komplexe Globaleinwilligung
- - Kinder sind nicht einwilligungsfähig.
    - › Altersgrenze grundsätzlich 16 Jahre, Art. 8 Abs. 1 DS-GVO
    - › Öffnungsklausel für nationale Gesetze bis Altersgrenze 13 Jahre.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Weitere Ermächtigungsgrundlagen

- **Rechtslage nach DS-GVO**
- Neue zentrale Norm für die Rechtmäßigkeit der Verarbeitung ist Art. 6 DS-GVO. Danach ist eine Verarbeitung rechtmäßig, wenn einer der folgenden Ermächtigungsgrundlagen gegeben ist:
- → Einwilligung des Betroffenen
- → Verarbeitung ist zur Erfüllung eines vom Betroffenen initiierten Vertrages erforderlich
- → Verarbeitung ist zur Erfüllung rechtlicher Verpflichtungen erforderlich
- → Verarbeitung ist zum Schutz lebenswichtiger Interessen erforderlich
- → Verarbeitung ist zur Erfüllung von öffentlichen Aufgaben erforderlich
- → Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder Dritten erforderlich, sofern nicht die Interessen des Betroffenen überwiegen

  - Notwendigkeit einer Abwägung

  - Bei Kindern werden entgegenstehende Interessen vermutet.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Sonderfall: Werbung

Rechtslage nach DS-GVO

- Die detaillierten Regelungen zur Datenverarbeitung für Werbezwecke fallen weg. Es gibt keine dem § 28 Abs. 3 BDSG vergleichbare Regelung.

→ Folge: Auch Werbung unterliegt künftig den allgemeinen Zulässigkeitsschranken von Art. 6 DS-GVO:

- Einwilligung oder insb.
- Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO

→ Auslegungshilfe in EG 47:

„*Die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.*“

- Bei Kinder- und Jugendsport (Altersgrenze 16 Jahre) ist besondere Vorsicht geboten. Insb. das „berechtigte Interesse“ greift hier kaum.

Vorgehensweise bei der Implementierung der DS-GVO im Verein

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Verzeichnis von Verarbeitungstätigkeiten
Verantwortlicher
gem. Artikel 30 Abs. 1 DSGVO

Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede Titel
Name, Vorname
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Verarbeitungstätigkeit: Benennung: _____ **lfd. Nr.:** ____

Datum der Einführung:	Datum der letzten Änderung:

Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)	
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)	
Optional: Name des eingesetzten Verfahrens	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ ☐ ☐
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ ☐ ☐ Besondere Kategorien personenbezogener Daten (Art. 9): ☐

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ intern (Zugriffsberechtigte) Abteilung/ Funktion
	☐ extern Empfängerkategorie
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO
(Art. 30 Abs. 1 S. 2 lit. g)
Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten", Ziff. 6.7. und 6.8

Verantwortlicher ..... Datum ..... Unterschrift .....

Seite 3 von 3

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Technisch-organisatorische Maßnahmen

Rechtslage nach DS-GVO

- → Eine dem § 9 BDSG iVm. dessen Anlage vergleichbare Norm enthält die DS-GVO nicht. Vielmehr regelt Art. 32 DS-GVO zunächst in allgemeiner Weise die zentralen Schutzziele der Datensicherheit in der automatisierten Verarbeitung:

  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit.

→ Diese zentralen Ziele waren schon im BDSG enthalten!

→ Neues Kriterium: „Belastbarkeit der Systeme“, Art. 32 Abs. 1 lit. b) DS-GVO. Technische Entwicklung der Systeme muss beachtet werden, da die Datensicherheit „*auf Dauer*“ sichergestellt werden muss.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Technisch-organisatorische Maßnahmen

Grundprinzipien technisch organisatorischer Maßnahmen

- → **Zutrittskontrolle**: Verhinderung des Zutritts zu Datenverarbeitungsanlagen durch Unbefugte (Sicherheitszonen/Sperrbereiche/Chipkarten/Schlüsselreglung/ Alarmanlage/Videotechnik).
- → **Zugangskontrolle**: Verhinderung der unbefugten Nutzung von Datenverarbeitungsanlagen (Protokolle/Passwort)
- → **Zugriffskontrolle**: Zugriff nur auf die hierarchisch zugelassenen Daten (Berechtigungskonzept/Mehraugenprinzip/Prüfung der Zugriffsberechtigung)
- → **Weitergabekontrolle**: Vermeidung von Auslesen, Kopieren oder Verändern durch Dritte (Datenverschlüsselung/Postversand/Datenträgervernichtung/Standleitung)
- → **Eingabekontrolle**: Prüfbarkeit, wer wann was verarbeitet hat (Erfassungsbelege/ Protokollierung)
- → **Auftragskontrolle**: Weisungsmäßige Verarbeitung durch Auftragnehmer (Vertrag/ Verfügungsberechtigungen/Verlustregelungen/Kontrollen)
- → **Verfügbarkeitskontrolle**: Schutz der zufälligen Zerstörung (Brand/Wasserschaden) (Sicherungskopien/Notstromaggregate/Katastrophenplan)

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Technisch-organisatorische Maßnahmen

- Der Begriff der technisch-organisatorischen Maßnahmen wird dynamisch verstanden:

→ „geeignete“ technische Maßnahmen

→ unter Berücksichtigung des „*Standes der Technik*“

→ und unter Berücksichtigung der „*Implementierungskosten*“.

- Also: relativer und nicht absoluter Begriff der Datensicherheit. Verhältnismäßigkeit des Aufwandes spielt eine Rolle.

- Nach Art. 32 DS-GVO muss stets der Schutzbedarf der Betroffenen berücksichtigt werden und ein dem Risiko angemessenes Schutzniveau erreicht werden:

→ Art/Umfang/Zweck der Verarbeitung

→ Eintrittswahrscheinlichkeit von Risiken

→ Schwere der Risiken und der möglichen Schäden.

→ Also: Klassifizierung des Schutzbedarfs (*Mittel/Hoch/Sehr hoch*).

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Datenpannen

Rechtslage nach DS-GVO

- → Erhebliche Erweiterung der Informationspflichten bei Datenpannen in Art. 33 und 34 DS-GVO.
- Konzept der abgestuften Meldepflicht
  - Meldung an die Aufsichtsbehörde hat **immer** zu erfolgen, es sei denn, die Datenpanne führt „*voraussichtlich nicht zu einem Risiko für den Betroffenen.*“
  - Umkehr der Beweislast: Meldepflicht ist Regelfall; Ausnahme muss vom Verein dargelegt werden.
  - Problem ist insbesondere, dass Risiken für den Betroffenen kaum abschätzbar, jedenfalls nicht ausschließbar sind.
  - Frist der Meldung: 72 Stunden!
  - Überschreiten nur in Ausnahmefällen

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Datenpannen

Konzept der abgestuften Meldepflicht

→ Meldung an den Betroffenen nur dann, wenn ein „*hohes Risiko*“ für deren Rechte und Freiheiten besteht.

- Frist: Unverzüglich!
- Information muss in „*klarer und einfacher*“ Sprache erfolgen.
- Ausnahme von der Informationspflicht nach Art. 34 Abs. 3 DS-GVO:
  - › Geeignete technische und organisatorische Maßnahmen, insb. eine Verschlüsselung, verhindern Eintritt der Risiken.
  - › Information ist mit unverhältnismäßigem Aufwand verbunden.

- Achtung: Dann aber Pflicht zur öffentlichen Bekanntmachung! (*Super Gau des „Vereinsmarketings“*)

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Datenpannen

- Was muss gemeldet werden? (Art. 33 Abs. 3 DS-GVO)

  → Beschreibung der Art und Folgen der Datenpanne
  → Angabe der betroffenen Daten
  → Angabe der Anzahl der Betroffenen (ungefähr)
  → Name des Datenschutzbeauftragten
  → Beschreibung der getroffenen Maßnahmen

- Ein Verstoß gegen die Meldepflichten löst ein hohes Bußgeld aus (max. 10 Mio EUR).

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Auskunftsrechte der Betroffenen

Rechtslage nach DS-GVO

- Die DS-GVO erweitert in Art. 15 die Auskunftsrechte der Betroffenen, indem sie die Qualität der Information umfangreicher gestaltet:
  - → Ob und welche Daten verarbeitet werden,
  - → Verarbeitungszwecke,
  - → Kategorien verarbeiteter Daten (*neu*),
  - → Datenempfänger bei Übermittlung,
  - → Geplante Speicherdauer (*neu*),
  - → Informationen über Löschungs- Berichtigungs- und Widerspruchsrechte (*neu*),
  - → Information über Beschwerderecht (*neu*),
  - → Herkunft der Daten,
  - → Bestehen automatisierter Entscheidungsfindung (Profiling) (*neu*).
- Auskünfte können schriftlich, mündlich oder elektronisch erteilt werden

  Bevorzugt: EG 63 Satz 4: Fernzugriff!

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Auskunftsrechte der Betroffenen

- Ergänzend: Informationspflicht aus Art. 13 DS-GVO betrifft Information des Betroffenen zum Zeitpunkt (!) der Datenerhebung bei ihm selbst u.a.

  → Name und Kontaktdaten des Verantwortlichen (Verein)
  → Kontaktdaten des Datenschutzbeauftragten
  → Falls Ermächtigung aus Art. 6 Abs. 1 lit f) DS-GVO folgt: Dokumentation der berechtigten Interessen
  → Empfänger bei Datenübermittlung
  → Speicherdauer
  → Hinweis auf Auskunftsrechte
  → Hinweis auf Recht zum Widerruf der Einwilligung
  → Hinweis auf Beschwerderecht

- Beachte: Bei Zweckänderung muss auch hierüber (erneut) informiert werden, Art. 13 Abs. 3 DS-GVO.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Auskunftsrechte der Betroffenen

- Ergänzend: Informationspflichten aus Art. 14 DS-GVO betrifft Informationen, wenn Daten **nicht** beim Betroffenen erhoben werden.

→ Name und Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten

→ Zwecke und Rechtsgrundlage der Verarbeitung

→ Kategorien verarbeiteter Daten

→ Dauer der Speicherung

→ Darstellung der berechtigten Interessen bei Anwendung von Art. 6 Abs. 1 lit. f) DS-GVO

→ Hinweis auf Auskunfts- und Löschungsrechte

→ Möglichkeit des Widerrufs der Einwilligung bei vorliegender Einwilligung

→ Hinweis auf Beschwerderecht

→ Herkunft (Quelle) der Daten

→ Bestehen automatisierter Entscheidungsfindungen (einschließlich Profiling).

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Auftragsdatenverarbeitung

Grundsätzliche Vorbemerkung

→ Die Auftragsdatenverarbeitung betrifft Fälle, in denen der Verein an Dritte (idR. Dienstleister) Daten übermittelt, damit dieser auf Weisung des Vereins tätig wird (Bsp. Lettershop zur Versendung von Einladungen zur MV).

→ Auftragsdatenverarbeitung ist von der sog. Funktionsübertragung abzugrenzen. Bei der Funktionsübertragung agiert der Dritte selbständig und nicht als „*verlängerter Arm*“ des Vereins.

→ Abgrenzung zu gemeinschaftlicher Verarbeitung im Sinne von Art. 26 DS-GVO (sog. *joint controllership*).

- Beispiel: Konzernübergreifende Beschäftigungsdaten.

- ABER: Art. 26 DS-GVO ist keine Ermächtigungsgrundlage.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Auftragsdatenverarbeitung

Rechtslage nach DS-GVO

- Art. 28 DS-GVO greift das Konzept der Auftragsdatenverarbeitung auf.

→ Erforderlich nach Art. 28 Abs. 1 DS-GVO ist zunächst die Prüfung der Geeignetheit des Auftragsdatenverarbeiters. Dieser muss die Gewähr effektiven Datenschutzes bei sich selbst bieten.

- Beleg einer solchen Geeignetheit können sein:
  - genehmigte Verhaltensregeln des Auftragnehmers nach Art. 40 DS-GVO
  - Zertifizierungen nach Art. 42 DS-GVO
  - Einzelfallprüfung durch Auftraggeber

→ Abschluss eines Vertrags mit gesetzlichem Inhalt (neu: auch elektronisch)

- Inhalt des Vertrages ist weitestgehend deckungsgleich mit DS-GVO
- Auftragnehmer muss aber insb. die Maßnahmen darstellen, die er zur Datensicherheit ergreift.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Recht auf Löschung

- Verein als Verantwortlicher sollte ein Löschungskonzept erstellen!

→ Nach Art. 13 Abs. 2 lit. a) DS-GVO muss Betroffener grundsätzlich über die (individuelle) Dauer der Speicherung seiner Daten informiert werden.

- Voraussetzung wäre eine individualisierte Ermittlung und Aufzeichnung von Speicherfristen für jeden Betroffenen.

- Dies ist in Massenprozessen illusorisch!

Deshalb: Art. 17 Abs. 2 lit. a) DS-GVO: Festlegung allgemeiner Kriterien für die Dauer der Speicherung der Daten (d.i. Löschungsfristen).

→ Zur Erfüllung der Auskunftsrechte sollte also ein allgemeines Löschungskonzept erstellt werden.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Beschäftigtendatenschutz

Regelungsgehalt von § 26 BDSG *neu*

→ § 26 Abs. 1 Satz 1 BDSG *neu* entspricht im Wesentlichen dem bisherigen § 32 Abs. 1 Satz 1 BDSG. Neu ist die Möglichkeit der Verarbeitung von Beschäftigtendaten zur Erfüllung der sich aus Gesetz, Tarifvertrag oder Betriebsvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Arbeitnehmer.

→ § 26 Abs. 2 BDSG *neu* regelt die Einwilligung im Beschäftigungsverhältnis und hier insbesondere Kriterien zur Freiwilligkeit der Einwilligung (z.B. Zeitpunkt der Erteilung der Einwilligung etwa vor Abschluss des Arbeitsvertrages).

→ Nach § 26 Abs. 3 BDSG *neu* dürfen auch besondere Kategorien personenbezogener Daten für das Beschäftigungsverhältnis verarbeitet werden. Voraussetzung ist, dass die Verarbeitung für

- Arbeitsrecht

- soziale Sicherheit und Sozialschutz erforderlich ist.

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Beschäftigtendatenschutz

Regelungsgehalt von § 26 BDSG *neu*

→ § 26 Abs. 4 BDSG *neu* sichert die Verarbeitung von Beschäftigtendaten auf Basis von Kollektivvereinbarungen (Tarifverträge und Betriebsvereinbarungen) ab.

→ Die zentralen Grundsätze der Datenverarbeitung aus Art. 5 DS-GVO stehen nicht zur Disposition der Vertragsparteien, § 26 Abs. 5 BDSG *neu.*

→ Die Beteiligungsrechte von Gewerkschaften und Betriebsräten aus Spezialgesetzen (TVG, BetrVG) bleiben gesichert, § 26 Abs. 6 BDSG *neu*.

→ Wie schon nach bisherigem Recht umfasst der Datenschutz im Arbeitsrecht neben der automatisierten Verarbeitung auch nicht automatisierte Verarbeitung (Personalakte, Arbeitspapiere).

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Maßnahmenplan für Vereinsvorstände

1. **Bestandsaufnahme**

- Wer ist eigenständiger Verantwortlicher?
- Ist ein Datenschutzbeauftragter bestellt?
- Welche Dokumentationen und Verfahrensverzeichnisse existieren?
- Auf Basis welcher Rechtsgrundlagen (Einwilligung/Gesetz/Vertrag) werden die zentralen Verarbeitungsprozesse durchgeführt?
- Werden besondere Arten personenbezogener Daten verarbeitet?
- Welche Auftragsdatenverarbeitungen liegen vor?
- Wie sind die technisch-organisatorischen Maßnahmen ausgestaltet?
- Gab es in der Vergangenheit Sicherheitslücken?

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Maßnahmenplan für Vereinsvorstände

2. Handlungsbedarf feststellen

- Überprüfung bestehender Einwilligungen
- Überprüfung der Voraussetzungen anderer Ermächtigungsgrundlagen im Sinne von Art. 6 DS-GVO (insb. des berechtigten Interesses)
- Sind Kinder involviert?
- Können insb. Auskunftsrechte der Betroffenen erfüllt werden (Vorhalten von Dokumentationen)?
- Technikeinstellungen prüfen, insb. Voreinstellungen.
- Auftragsdatenverarbeitungen überprüfen?
- Welche Datenschutz-Folgeabschätzungen sind notwendig?
- Gibt es ein Löschungskonzept?
- Sind Verzeichnisse von Verarbeitungstätigkeiten notwendig?

Datenschutz-Grundverordnung

DORNBACH
Unsere Kompetenz – Ihre Zukunft

Maßnahmenplan für Vereinsvorstände

- Gibt es einen Reaktionsplan für Meldungen von Datenpannen?
- Besteht ein angemessenes technisches Schutzniveau?
- Welche Daten werden öffentlich bekannt gemacht (Stichwort: Recht auf Vergessenwerden)?
- Sind Verhaltensregelungen oder ähnliche Zertifizierung sinnvoll?

DORNBACH
Unsere Kompetenz – Ihre Zukunft

UNSERE KOMPETENZ - IHRE ZUKUNFT

Vielen Dank!

www.dornbach.de