

Neuerungen im Datenschutz

EU-DSGVO

14. Juli 2018

startklar
rose müller

Bei der Kelter 5
74321 Bietigheim-Bissingen

Persönliche Informationen

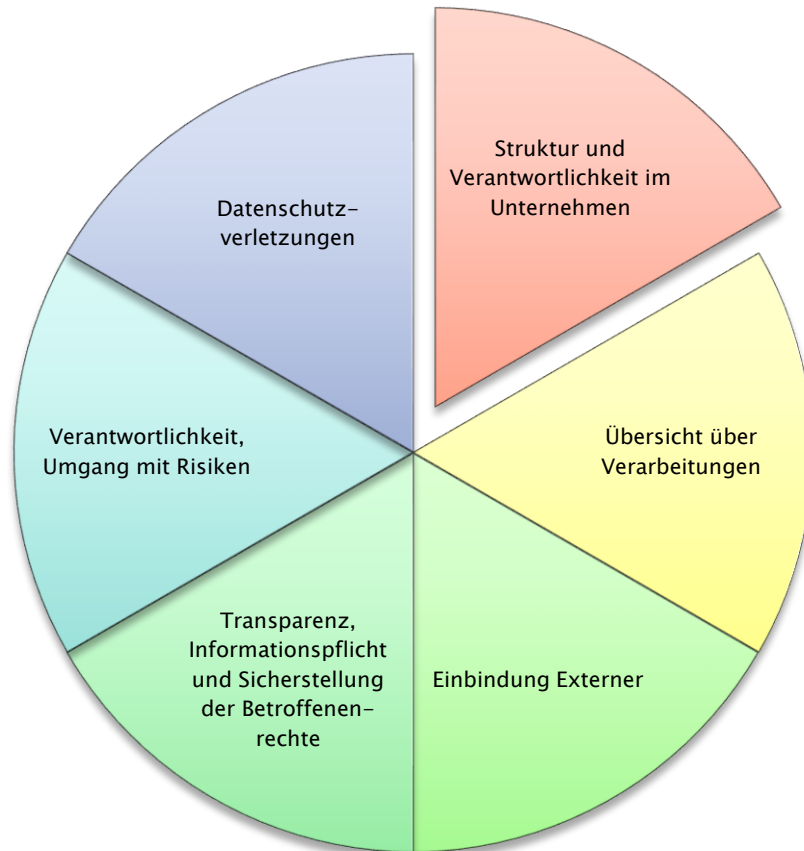


- ▶ Familienstand: verheiratet, keine Kinder
- ▶ Jahrgang: 1962
- ▶ Ausbildung:
 - 1981 – 1986: Informatik-Studium an der FH Karlsruhe
 - Abschluß: Dipl.Inform. (FH)
 - 2010+2016: Zertifizierung externe Datenschutzbeauftragte
- ▶ Berufserfahrung:
 - Von 1986 – 2010
 - Programmiererin, Systemanalytikerin, Projektleiterin, Teamleiterin, Assistentin der Bereichsleitung
 - Seit Oktober 2010 selbstständig als
 - externe Datenschutzbeauftragte
 - u.a.

EU-DSGVO

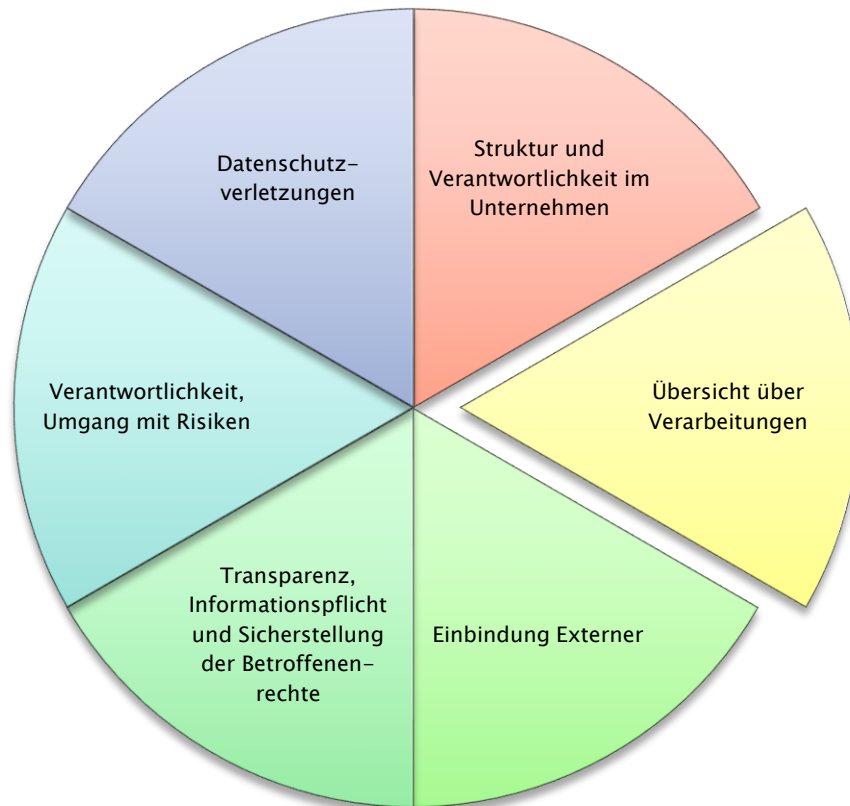
- ▶ Seit 25. Mai 2018
 - DSGVO:
 - europaweite Datenschutzgrundverordnung
 - Verbot mit Erlaubnisvorbehalt
 - BDSG 2018:
 - Nationale Ergänzung zu bestimmten Themen
 - Beschäftigten-Datenschutz
 - Datenschutz für öffentliche Einrichtungen (auch LDSGs)
 - Datenschutzbeauftragter

Allgemeine Fragen



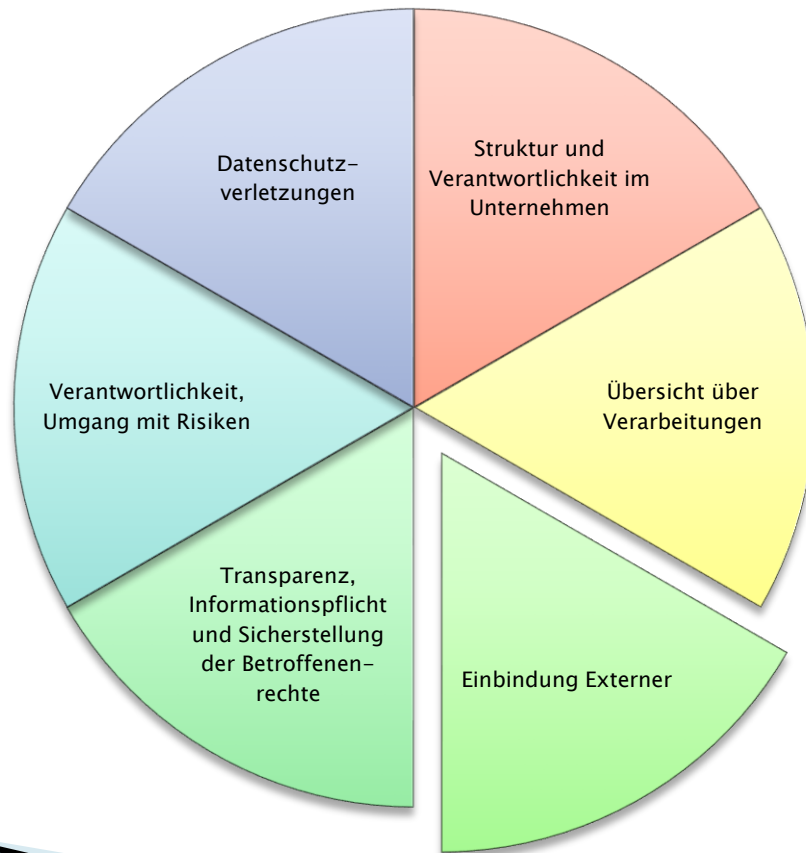
- ▶ Gibt es das Bewusstsein im Verein, dass Datenschutz Chefsache ist, beispielsweise durch
 - Vorhandensein einer Datenschutzordnung
 - Beschreibung der Datenschutzziele
 - Regelung der Verantwortlichkeiten
 - Bewusstsein über Datenschutzrisiken
 - Transparenz über Zielkonflikte (bei Unternehmen z.B. zwischen Marketing- und Rechtsabteilung)
- ▶ Verfügt Ihr Verein über einen Datenschutzbeauftragten?

Allgemeine Fragen



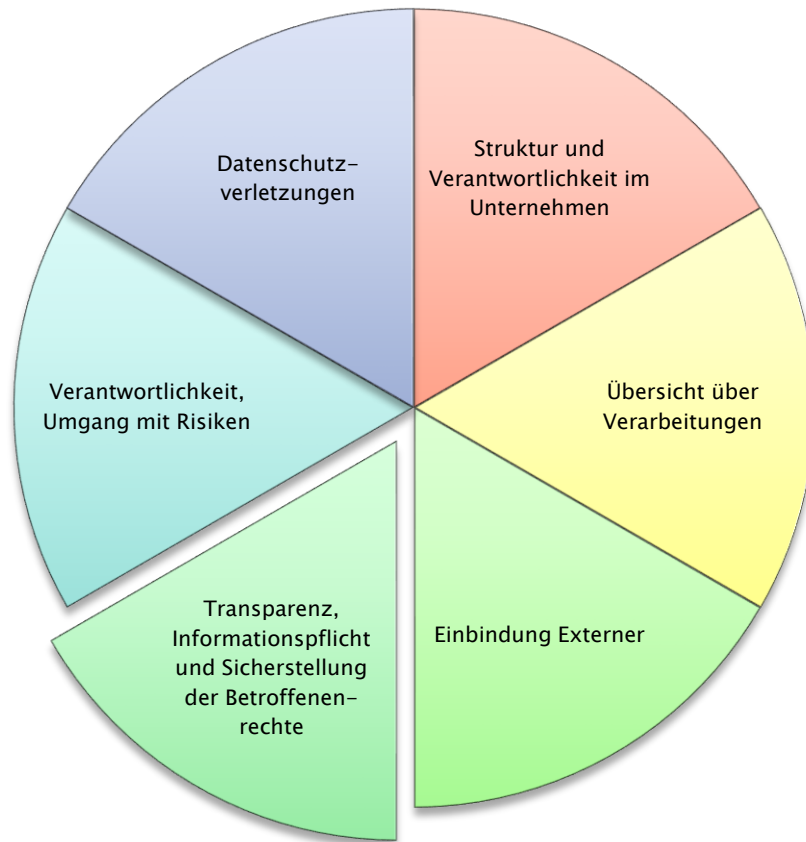
- ▶ Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO?
 - Wenn nein, warum nicht? Ist das dokumentiert?
 - Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Verein Berücksichtigung finden (Privacy by Design – Art. 25 DS-GVO)?

Allgemeine Fragen



- ▶ Haben Sie Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden?
 - Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter?
 - Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?

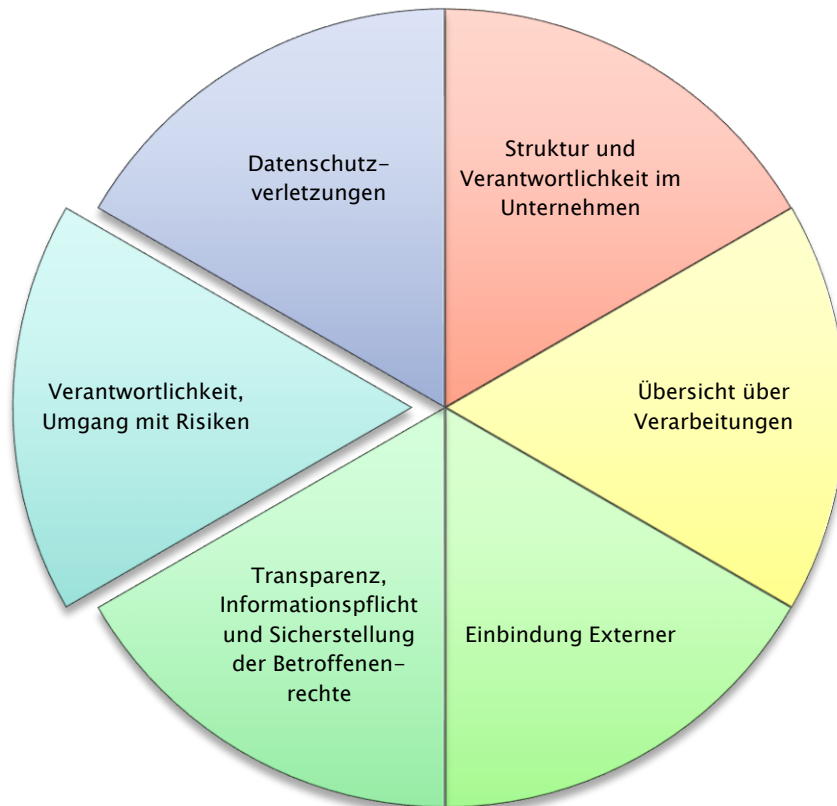
Allgemeine Fragen



► Fragestellungen

- Information der betroffenen Personen bei der Datenerhebung
- Datenübermittlung in Drittländer
- Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität
- automatisierte Entscheidungsfindung einschließlich Profiling
- Nutzung „Kunden“daten für Werbung

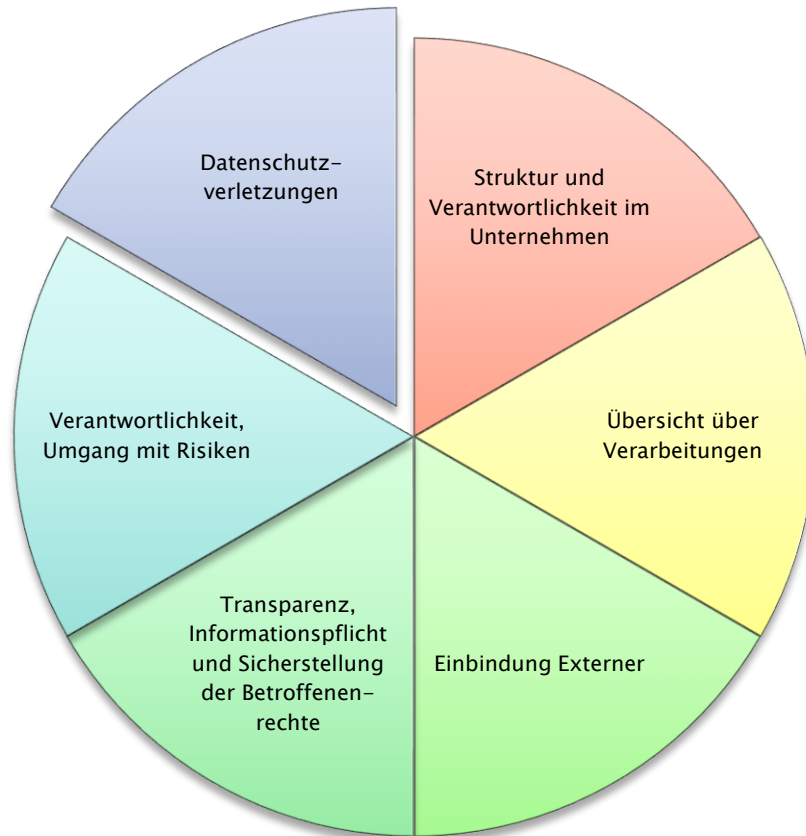
Allgemeine Fragen



► Fragestellungen

- Rechtmäßigkeit der Verarbeitung und Nachweis
- Einwilligungen und Nachweis
- Sicherheit der Verarbeitung
- risikoorientierte Betrachtungsweise auf Basis von Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der Betroffenen
- Datenschutz-Folgenabschätzung

Allgemeine Fragen



► Meldung von Datenschutzverletzungen

- Können Datenschutzverletzungen in Ihrem Verein erkannt werden?
- interner Prozess für den Umgang mit potentiellen Verletzungen vorhanden?
- Haben Sie gem. Art. 33 DS-GVO sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist?
- Festlegung, wer, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert

Umsetzung für Vereine

- ▶ **Datenschutzbeauftragter notwendig?**
 - Mind. 10 Mitarbeiter sind ständig mit der Verarbeitung personenbezogener Daten beschäftigt.
 - Hauptaufgabe der Mitarbeiter ist Datenverarbeitung
- ▶ **Entwickeln einer Datenschutzordnung**
 - Festlegung der Verantwortlichkeiten
 - Umgang Verein mit personenbezogenen Daten
- ▶ **Datenschutz-Informationsblatt**
 - Für Mitgliedsantrag, sonstige Formulare

Umsetzung für Vereine

- ▶ Verzeichnis Verarbeitungstätigkeiten
 - Mitgliederverwaltung
 - Lohnabrechnung, falls bezahlte MA
 - Betrieb der Webseite, falls pers.bez.Daten
 - Beitragsverwaltung
- ▶ Vertraulichkeitsverpflichtung „Mitarbeiter“
 - Alle mit Zugang zu personenbezogenen Daten
- ▶ Umgang mit Anfragen Betroffener

Umsetzung für Vereine

- ▶ Vereinbarung mit Auftragsverarbeitern
 - Dienstleister, die Daten im Auftrag des Vereins verarbeiten
 - Webhoster
 - Lohnabrechnungsbüro (außer Steuerberater)
- ▶ Meldung von Datenschutzverletzungen
 - Aufsichtsbehörde
 - Betroffene

Unterstützung

- ▶ Informationen vom BayLDA
 - www.lida.bayern.de/de/kleine-unternehmen.html
- ▶ Informationen vom WLSB
 - www.wlsb.de/aktuelles/news/712-datenschutz-im-verein
- ▶ Startklar-Projekt „Datenschutz im Verein“
 - www.datenschutz-verein.de

Spezialfragen WBRS

▶ Frage:

- Ist die Datenerhebung zur Teilnahme am Rehasport rechtmäßig?

▶ Antwort:

- Kommt auf die Daten an, die der Verein erhebt und verarbeitet
 - Daten der Verordnung inkl. konkrete Teilnahmedaten für Abrechnung:
 - Rechtsgrundlage: DSGVO Artikel 6 Abs. 1 lit b) „Vertrag“
 - Bei Abrechnung über ein Abrechnungszentrum muss der Verein eine Vereinbarung zur Datenverarbeitung im Auftrag mit dem Abrechnungszentrum (Artikel 28 Abs. 3 DSGVO) abschließen
 - Bitte legen Sie diese Vereinbarung dem WBRS vor (Empfehlung DBS)
 - Daten für Kommunikation in der Gruppe
 - Rechtsgrundlage:
 - DSGVO Artikel 6 Abs. 1 lit f) „Interessenabwägung“
 - Formular benutzen
 - Werden weitere Daten erhoben?
 - Prüfen, ob Rechtsgrundlage gefunden werden kann.
 - Teilnehmer müssen auf jeden Fall darüber informiert werden, wie ihre Daten verarbeitet werden und welche Rechte sie haben
 - Vorlage von DBS



Teilnehmer
Kommunikation



Information
Datenerhebung

Spezialfragen WBRS

▶ Frage:

- Datenschutzkonforme Nutzung des Formulars „Teilnahme am Rehasport“



Teilnahme
Rehasport

▶ Antwort:

- Siehe meine Ausarbeitung vom Mai 2018



Bewertung

▶ Antwort von DBS:

- Verwendung der Teilnahmebestätigungslisten (Unterschriftenlisten):
 - Wie bisher auch, sollten die Verordnungsunterlagen in einem verschlossenen Schrank unzugänglich für Dritte aufbewahrt werden. Bei der Landesgeschäftsführer/innen-Tagung hat unser Datenschutzbeauftragter empfohlen, für jede Gruppe einen eigenen Ordner zu führen und die Teilnahmebestätigungslisten nur mit **Namen, Vornamen** und ggf. Angebotsnummer zu füllen.
 - Die Eintragung der restlichen personenbezogenen Daten (Geburtsdatum, Versicherungsnummer, Rehabilitationsträger) sollen erst **zum Zeitpunkt der Abrechnung** erfolgen.
 - Damit wird gewährleistet, dass nur die ohnehin bekannten Informationen (Name, Vorname) innerhalb der Gruppe verwendet werden und diese nicht an unbeteiligte andere Gruppen weitergegeben werden.

Spezialfragen WBRS

▶ Frage:

- Muss ein DSB benannt werden, weil x Ärzte auch Zugriff auf Daten der Rehasport-Teilnehmer haben?

▶ Antwort:

- Ärzte sind Empfänger von Daten
 - Sie zählen **nicht** zu den Vereins-Mitarbeitern, die mit der Datenverarbeitung beschäftigt sind

Spezialfragen WBRS

▶ Frage:

- Sind die Daten der Reha-Sport-Teilnehmer (Daten von der Verordnung) besonders sensible Daten (im Vergleich zu den Daten des "normalen" Vereinsmitglieds)? Wenn ja, inwieweit ist anders mit diesen Daten umzugehen?

▶ Antwort Teil 1:

- Daten der Verordnung sind sensiblere Daten als z.B. Adressdaten
- Schon die Teilnahme am Reha-Sport gilt als (besonders) schützenswerte Information
- Personenbezogene Daten müssen grundsätzlich entsprechend ihrer Sensibilität behandelt werden.
 - Fragestellung:
 - Wie hoch ist das Risiko für den Betroffenen?
 - Welcher Schaden könnte für den Betroffenen durch die Verarbeitung der Verordnung entstehen?



Mitarbeiter (Trainer und Übungsleiter) auf Vertraulichkeit / Verschwiegenheit verpflichtet!

Spezialfragen WBRS

▶ Frage:

- Sind die Daten der Reha-Sport-Teilnehmer (Daten von der Verordnung) besonders sensible Daten (im Vergleich zu den Daten des "normalen" Vereinsmitglieds)? Wenn ja, inwieweit ist anders mit diesen Daten umzugehen?

▶ Antwort Teil 2:

- Sind es auch besonders sensible Daten nach Artikel 9?
 - ✓ Gesundheitsdaten
- Wann dürfen diese Daten verarbeitet werden?
 - Rehasport: Die Grundlage für die gesetzlich definierte Leistung „Rehabilitationssport“ bildet das Sozialgesetzbuch IX §64.
 - Zulässigkeit der Datenerhebung (...) nach SGB X, §§ 67 a ff.
 - Daten dürfen für die Zwecke, für die sie erhoben worden sind, verarbeitet werden, wenn sie
 - zur **Erfüllung** der in der **Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben** nach diesem Gesetzbuch **erforderlich** sind,
 - Nur wenn sie zu **anderen Zwecken** verarbeitet werden, bedarf es der Einwilligung des Betroffenen.

Spezialfragen WBRS

▶ Frage:

- Falls die Reha-Sport-Daten sensible Daten sind, heißt das automatisch, dass ein Datenschutzbeauftragter bestellt werden muss, auch wenn der Reha Sport nicht Kernbereich des Vereins ist?

▶ Antwort:

- Ein DSB muss bestellt werden
 - die Kerntätigkeit ... in der **umfangreichen** Verarbeitung besonderer .. Daten (DSGVO)
 - ... mind. 10 „Mitarbeiter“ ... (BDSG)
 - ... Verarbeitungen ... Datenschutz-Folgenabschätzung ..
 - DSFA notwendig, wenn Verarbeitung vermutlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat

Spezialfragen WBRS

▶ Frage:

- Welche Vorgaben gelten für die Aufbewahrung der Daten? Wie/Wo müssen sie (z. B. die Verordnungen) aufbewahrt werden? Wie lange müssen die Daten aufbewahrt werden?

▶ Antwort:

- Aufbewahrungsort:
 - so, dass sie nicht an Unbefugte gehen
- Dauer:
 - Bis der Zweck erfüllt ist, für den sie erhoben wurden
 - Gesetzliche Aufbewahrungsfristen

Spezialfragen WBRS

▶ Frage:

- Können die Verordnungen weiterhin per Post an das Abrechnungszentrum geschickt werden?

▶ Antwort:

- Ja, die DSGVO hat hier nichts geändert

Spezialfragen WBRS

▶ Frage:

- Muss aufgrund der Sensibilität der Daten eine Risikofolgenabschätzung gemacht werden, auch wenn der Reha-Sport nur einen kleinen Bereich des Sportvereins (nicht Kernbereich) ausmacht?

▶ Antwort:

- Eine Risikobewertung muss bei **jeder** Verarbeitung gemacht werden
- Eine Datenschutz-Folgenabschätzung muss dann gemacht werden, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat
- Das ist unabhängig davon, wie groß der Anteil dieser Verarbeitung am „Bereich“ des Sportvereins ist.

Spezialfragen WBRS

▶ Frage:

- Wir benutzen für unsere Datenverarbeitung das Vereinsprogramm der KSK. Müssen wir eine Vereinbarung treffen?

▶ Antwort:

- Gegenfrage 1: Was ist „das Vereinsprogramm der KSK“?
- Gegenfrage 2: Welche Art von Vereinbarung ist gemeint?

Spezialfragen WBRS

- ▶ Frage:
 - Wer haftet für die evtl. Weitergabe von Daten, die wir für die halbj. Abrechnung mit den Krankenkassen an die Abrechnungsstellen geben?
- ▶ Antwort:
 - ??

Fragen

