CompCor | COMPLIANCE SOLUTIONS

Datenschutz für Golfbetreiberanlagen und Golfclubs

Hilfestellung zur Umsetzung der Regelungen der Datenschutz-Grundverordnung (DSGVO)

Hinweis:

Auf die Informationsunterlagen des Deutschen Golfverbandes wird ausdrücklich verwiesen:

- Rundschreiben 27/08 „Regelungen zum Datenschutz auf Golfanlagen“
- Datenschutz im Golfsport, August 2014
- EU-Datenschutz-Grundverordnung (DS-GVO) - Praxisnaher Überblick wichtigster Neuerungen, November 2017

Stand: 20. März 2018

Ausgangslage:

Am 25. Mai 2018 tritt die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft. Diese neue DSGVO wird als unmittelbar geltendes Recht in allen EU-Staaten die bisherigen nationalen Regelungen verdrängen.

Die DSGVO erlaubt an einigen (wenigen) Stellen, dass der jeweilige nationale Gesetzgeber ergänzende Regelungen treffen kann. Hierzu hat Deutschland das bisherige BDSG vollständig überarbeitet und ein neues BDSG erlassen (BDSG 2018), das künftig nur noch die ergänzenden Regelungen enthält.

Für Online-Marketingmaßnahmen von Bedeutung ist ferner auch die Änderung der bisherigen „E-Privacy-Verordnung“ der EU, die ebenfalls als unmittelbar geltendes Recht voraussichtlich 2019 in Kraft treten wird.

Die wesentlichen Regelungen des neuen Datenschutzrechts

Anwendungsbereich der Datenschutzregelungen

Gem. Art. 2 DSGVO gelten die Regelungen für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Die Regelungen gelten für alle Unternehmen und Vereine, unabhängig von Ihrer Größe.

Dies umfasst also die Mitglieder- und Turnierverwaltung, die über Software abgewickelt wird, ebenso die personenbezogenen Daten, die in anderen Dateien (Emails, Word- oder Excel-Dokumente) enthalten sind und auf dem Dateisystem der Golfanlage gespeichert werden.

Darüber hinaus gelten die Neuregelungen für den Umgang mit Beschäftigtendaten nach BDSG (2018) auch für Verarbeitung in Akten.

Deutlich erhöhte Bußgelder und Strafen, Versicherungen

Mit diesen Neuregelungen werden die bisherigen Strafen und Bußgelder für Datenschutz-Verstöße drakonisch verschärft. Ab Mai 2018 sind Bußgelder von bis zu 20 Millionen Euro oder bis zu 4% des gesamten Jahresumsatzes des vorangegangenen Geschäftsjahrs möglich, je nachdem, welcher der Beträge höher ist.

Verschiedene Versicherungen bieten hier sogenannte D&O-Versicherungen oder Strafrechtsschutzversicherungen an. Bitte beachten Sie dabei, dass bei diesen Versicherungen in der Regel nur fahrlässiges Handeln versichert ist, in Ausnahmefällen auch bedingter Vorsatz. Absichtlich begangene Verstöße gegen rechtliche Anforderungen sind jedoch grundsätzlich nicht versicherbar.

Die beste „Versicherung" ist aus unserer Sicht deshalb ein angemessenes und aktuelles Datenschutz Management System (DMS), das durch eine fachkundige Person erstellt wurde und aktuell gehalten wird. Ein solches DMS kann sie im Einzelfall natürlich nicht vor Anzeigen oder Angriffen schützen, wird jedoch bei der Bewertung der strafrechtlichen und haftungsrechtlichen Verantwortung in einem Verfahren eine wesentliche Rolle spielen. [1]

Rechenschaftspflicht, Dokumentation des Datenschutz Management Systems

Für Unternehmen und Vereine hält die DSGVO einige Neuerungen bereit, die einen nicht unerheblichen Aufwand erzeugen können. Dies gilt vor allem für die in Artikel 5 Abs. 2 und Art. 24 geregelte Rechenschaftspflicht. Der Verantwortliche der Golfanlage ist für die „Einhaltung der Regelungen der DSGVO" verantwortlich und **muss dessen Einhaltung nachweisen können („Rechenschaftspflicht"**). Ein solcher Nachweis ist bei Kontrollen von Aufsichtsbehörden oder im Falle von Verfahren zwingend vorzulegen.

Darüber hinaus müssen je nach Art der Daten „geeignete technische und organisatorische Maßnahmen" ergriffen werden, um **sicherzustellen** und den **Nachweis** dafür erbringen zu können, dass personenbezogene Daten in Übereinstimmung mit den neuen Regelungen verarbeitet werden.

Diese neuen **Rechenschaftspflichten** bringen auch **haftungsrechtliche Konsequenzen** mit sich: Bislang musste ein Betroffener vor Gericht selbst den Nachweis dafür erbringen, dass ein Unternehmen oder ein Verein als verantwortliche Stelle für eine fehlerhafte Verarbeitung von Daten zu haften hat. Diese Pflicht obliegt nun nach dem neuen Artikel 5 Abs. 2 dem Verantwortlichen für die Datenverarbeitung. Und diese Pflicht muss durch Dokumente belegt werden können. Hier kommt es also de facto zu einer Beweislastumkehr.

Damit ist eine Dokumentation der wesentlichen Maßnahmen und Prozesse zur Umsetzung des Datenschutzes in der Golfanlage zwingend.

Die wesentlichen Bestandteile einer Dokumentation des Datenschutzes in der Golfanlage sollten enthalten:

- ✓ Dokument mit allen wesentlichen Inhalten der Dokumentation des „Datenschutz-Management Systems DMS" zur Erfüllung der Rechenschaftspflicht nach Art. 5 und 24 DSGVO
- ✓ Bestellung eines fachlich geeigneten Datenschutzbeauftragten bei Bedarf
- ✓ Erstellung einer kundenspezifischen „Datenschutz-Richtlinie" mit den internen Prozess-Regeln für alle Mitarbeiter und Ehrenamtliche
- ✓ Erstellung der erforderlichen Verzeichnisse über Verarbeitungstätigkeiten
- ✓ Abschluss bzw. Anpassung der Verträge zur Auftragsverarbeitung
- ✓ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ✓ Regelmäßige Schulung und Beratung der Mitarbeiter
- ✓ Anpassung der Datenschutzerklärungen für Ihre Webseiten
- ✓ Prozessregeln zur Auskunft an Betroffene
- ✓ Prozessregeln zur Durchführung der Meldung eines Datenschutz-Verstoßes
- ✓ Jährliche Überprüfung des DMS mit Dokumentation, Jahresbericht

[1] BGH 1StR 265/16: Für die Bemessung der Geldbuße ist … von Bedeutung, inwieweit die Nebenbeteiligte ihrer Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein effizientes Compliance-Management installiert hat, das auf die Vermeidung von Rechtsverstößen ausgelegt sein muss….

Rechtsgrundlagen der Datenverarbeitung in der Golfanlage

Neben der Einhaltung von Dokumentationspflichten ist insbesondere zu prüfen, ob die bisherige Erhebung und Verarbeitung personenbezogener Daten im Golfclub nunmehr den Anforderungen der DSGVO genügt.

Auch mit Inkrafttreten der DSGVO gilt weiterhin der Grundsatz, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, es sei denn, es existiert eine Rechtsgrundlage, die eine Verarbeitung gestattet.

Als Rechtsgrundlagen zur Verarbeitung von personenbezogener Daten kommen nach der DSGVO in Betracht:

- Verarbeitung von Daten der Mitglieder auf der Grundlage eines Vertrages (Vereinsatzung bzw. Spielvertrag)
- Einwilligung des Betroffenen
- Interessensabwägung (Datenverarbeitung im Interesse der Golfanlage und kein entgegenstehendes Interesse des Betroffenen

Rechtlicher Ausgangspunkt für die Verarbeitung der durch den Golfclub an das DGV-Intranet übermittelten personenbezogenen Daten, u. a. etwa der Namen der bei Ihnen organisierten Golfspieler für die Bestellung des DGV-Ausweises, sind die Aufnahme- und Mitgliedschaftsrichtlinien (AMR) des DGV. Diese müssen jedoch wirksam in den Regelwerken der Golfanlage verankert werden, siehe hierzu auch das DGV-Rundschreiben Nr. 27/08.

Überprüfen Sie deshalb Ihre Vereinssatzung bzw. die Spielverträge, ob diese Regelungen aktuell sind bzw. passen Sie diese rechtzeitig an!

Einwilligungen

Wenn Sie personenbezogene Daten von Gästen und Interessenten speichern möchten, um diesen Personen später weitere Angebote und Einladungen zu übermitteln, dann ist dies nur im Rahmen einer Einwilligung gesetzlich zulässig.

Durch den Grundsatz der Datensparsamkeit dürfen nur solche personenbezogenen Daten erhoben und verarbeitet werden, die auch für spätere Einladungen und Werbung tatsächlich benötigt werden.

Wenn Sie neben der Emailadresse der Person zusätzlich weitere Kontaktdaten, z. B. eine Telefonnummer, erfassen und nutzen möchten, muss nach den Vorgaben des Gesetzgebers hierfür eine gesonderte Einwilligungserklärung abgegeben werden. Bitte passen Sie in diesem Falle den beigefügten Mustertext in Abstimmung mit Ihrem Datenschutzbeauftragten entsprechend an.

Um sicherzustellen, dass der Inhaber der angegebenen Emailadresse auch tatsächlich der Einwilligende ist, muss das Einverständnis in die Nutzung der Emailadresse nochmals durch den Inhaber der Emailadresse per E-Mail bestätigt werden. Dieses Vorgehen wird als sogenanntes „Double-Opt-In Verfahren“ bezeichnet und von den Aufsichtsbehörden als zwingend erforderlich angesehen.

Für die Praxis bedeutet das „Double-Opt-In Verfahren“, dass der Interessent im Rahmen der nachfolgenden Einwilligungserklärung zunächst seine Emailadresse angibt und in einem zweiten Schritt von Ihrem Club per Email mit der Bitte angeschrieben werden muss, die Nutzung der Emailadresse für die Übersendung von Werbung zu bestätigen.

Erst nach Eingang dieser Bestätigung, die beispielsweise durch das Klicken auf einen voreingestellten Link oder aber auch einfach durch den Rückversand einer Email erfolgen kann, ist eine Übersendung von Informationsmaterialien und Werbung zulässig.

Muster Einwilligungserklärung „Interessent, Gast“:

Ich bin damit einverstanden, dass der GC XXX meine unten angegebene E-Mailadresse für die Zusendung von Informationen zu Kurs- und Spielangeboten (ggf. ergänzen) des GC XXX nutzt.

Ich kann diese Erklärung jederzeit gegenüber dem GC XXX, Anschrift, Emailadresse, widerrufen und damit einer künftigen Nutzung meiner Daten widersprechen.

Name

Vorname

Email-Adresse

Ort, Datum

Unterschrift

Um sicherzustellen, dass die von Ihnen angegebenen Emailadresse auch die richtige Adresse ist, bedarf dies einer Bestätigung durch den Inhaber der Emailadresse (sogenanntes „Double-Opt-In Verfahren“).

Sie erhalten zunächst durch den Golfclub XXX eine Email mit der Bitte, die Nutzung Ihrer Emailadresse für die Übersendung von Informationen und Werbung durch den GC XXX zu bestätigen.

Fortgeltung bisheriger Einwilligungen

Nach Erwägungsgrund 171 der DSGVO ist es nicht erforderlich, dass die betroffene Person zu einer gleichartigen fortgesetzten Datenverarbeitung, zu der sie gemäß den bisherigen Regelungen eingewilligt hat, erneut einwilligt, wenn die Art der bereits erteilten Einwilligung den Bedingungen der DSGVO entspricht.

Die bisher in großer Zahl vorhandenen Einwilligungen sollen also wirksam bleiben und eine große „Einwilligungsbürokratie“ auf Seiten der betroffenen Personen und der Verantwortlichen vermieden werden.

Allerdings enthalten die bisherigen Einwilligungen nach dem bisherigen BDSG oftmals nicht alle Informationen, die nun nach Art. 13 DSGVO vorgesehen sind.

In Erwägungsgrund 42 der DSGVO werden folgende Kernpunkte für Einwilligungen genannt:

- Einwilligungserklärung in verständlicher, klarer und einfacher Sprache und in leicht zugänglicher Form
- keine missverständlichen Klauseln
- Information, wer der Verantwortliche für die Datenverarbeitung ist und zu welchen Zwecken die Verarbeitung der personenbezogenen Daten erfolgt
- Hinweis auf die Widerrufsmöglichkeit

Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO)

Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der auf ihrer Grundlage bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Der Widerruf der Einwilligung muss für die betroffene Person so einfach wie die Erteilung der Einwilligung sein.

Sonderfall „Kinder und Jugendliche“

Bislang kannte das BDSG keine Altersgrenze, deshalb kam es bisher auf die Einsichtsfähigkeit des Kindes an. Die Einwilligung eines Kindes in die Verarbeitung seiner Daten war dann wirksam, wenn es die Tragweite seiner Entscheidung vernünftigerweise absehen konnte.

Nunmehr enthält Art. 8 DSGVO eine ausdrückliche gesetzliche Regelung in Bezug auf die Einwilligung von Kindern und Jugendlichen für Personen mit einer Altersgrenze von 16 Jahren. Für Kinder und Jugendliche unter 16 Jahren ist eine Einwilligung nur dann wirksam, wenn sie entweder von den Erziehungsberechtigten selbst erteilt wurde oder deren Zustimmung vorliegt. Die Einwilligung des Kindes allein genügt dann nicht.

Dies ist eine der Stellen, an denen die Mitgliedsstaaten ergänzende Regelungen treffen und ggf. eine niedrigere Altersgrenze festlegen können. Die Grenze darf allerdings nicht unter 13 Jahren liegen.

Deutschland hat keine eigenständige Regelung getroffen, deshalb gilt die Grenze von 16 Jahren auch in Deutschland. Andere Mitgliedsstaaten haben teilweise niedrige Grenzen festgelegt.

Die besondere Einwilligung von Erziehungsberechtigten ist gem. Art. 8 DSGVO erforderlich, wenn in Golfanlagen ein sogenannter „Dienst der Informationsgesellschaft“ angeboten wird. Dieser Begriff wird in der DSGVO leider nicht definiert, sondern nur auf die EU-Richtlinie 2015/1535 verwiesen:

Ein „Dienst der Informationsgesellschaft“ liegt insbesondere bei Verwendung des Internets oder Social-Media-Plattformen (z.B. Facebook) vor.

Dies bedeutet, dass für die Veröffentlichung von Bildern von Kindern und Jugendlichen (z.B. Turnier-, Mannschaftsbilder) im Internet oder Social-Media-Plattformen die Einwilligung aller Erziehungsberechtigten **ZWINGEND** vorliegen muss!

Bestellung eines Datenschutzbeauftragten (DSB)

Zu den Anforderungen an den betrieblichen Datenschutzbeauftragten hat die Art. 29 Gruppe aktuelle Leitlinien veröffentlicht.

Hier sind auch Ausführungen zu der erforderlichen Fachkunde, den möglichen Interessenskonflikten und den Haftungsfragen enthalten.

Die Funktion des DSB kann sowohl intern besetzt als auch durch eine externe fachlich geeignete Person wahrgenommen werden. Sie finden Verzeichnisse über qualifizierte Berater über verschiedene Verbände (BvD, GDD). Bitte prüfen Sie im Einzelfall, ob das externe Consulting-Unternehmen über ausreichende Fachkunde als auch Branchenkenntnisse verfügt, möglichst auch über entsprechende Referenzen.

Deutschland hat für diesen Bereich die DSGVO durch Regelungen im BDSG (2018) ergänzt, die im Wesentlichen der bisherigen Rechtslage entsprechen.

Ein betrieblicher Datenschutzbeauftragter für Golfanlagen ist gem. Art. 37 DSGVO bzw. § 38 BDSG (2018) zu bestellen, wenn eine der folgenden Bedingungen vorliegt:

- eine „Kerntätigkeit“ gegeben ist, die eine umfangreiche und systematische Überwachung von Personen umfasst;
- die „Kerntätigkeit“ in der umfangreichen Verarbeitung besonders sensibler Daten besteht;
- Verfahren zum Umgang mit Personendaten vorliegen, die einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) unterliegen (z.B. bei der Verarbeitung sensibler Daten, Einsatz von Videokameras) oder
- mindestens zehn (10) Personen sich ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Bei einer Golfanlage können also verschiedene Gründe vorliegen, die eine Bestellung eines Datenschutzbeauftragten erfordern.

Wesentlich bei der Beurteilung der Anzahl der Personen (zehn) sind folgende Punkte:

Wer fällt alles darunter:

Es sind alle „Beschäftigte“ zu berücksichtigen, unabhängig von ihrem arbeitsrechtlichen Status (Geschäftsinhaber, Vorstände, Partner, Angestellte, Auszubildende, Praktikanten, freie Mitarbeiter, Leiharbeitnehmer etc.). Ob die Personen einen vollen oder Teilzeitvertrag besitzen, ist nicht wesentlich. Die Aufsichtsbehörden rechnen hier auch ehrenamtlich tätige Personen mit, wenn diese die Daten von Mitgliedern in Dateien automatisiert verwalten (z.B. in Excel-Tabellen).[2]

Was bedeutet „ständig“:

Für die Beurteilung der Formulierung „ständig“ ist wesentlich, ob der Umgang mit personenbezogenen Daten zum Aufgabenfeld der Mitarbeiter gehören. Hier spielt es keine Rolle, wie oft die Aufgabe anfällt (es genügt auch nur gelegentlich). Es umfasst also alle Personen, die mit Personendaten von Mitarbeiter, Kunden, Lieferanten befasst sind, auch wenn dies nur gelegentlich erfolgt (auch IT-Mitarbeiter mit Zugriffsmöglichkeiten auf Personendaten). Nicht umfasst werden dagegen Personen, zu deren Tätigkeitsfeld der Umgang mit Personendaten gerade nicht gehört (z.B. Greenkeeper).

Somit dürften also alle Personen, die im Sekretariat einer Golfanlage tätig sind; alle Personen im Vorstand, die über einen Mitgliedsantrag entscheiden und alle ehrenamtliche Abteilungsverantwortliche, die Zugang zu den Kontaktdaten von Mitgliedern haben, hier zu berücksichtigen sein. Damit dürfte die überwiegende Mehrzahl von Golfanlagen und Golfclubs zur Bestellung eines Datenschutzbeauftragten verpflichtet sein.

Bitte beachten Sie:

Wenn Sie die Kriterien für die Bestellung eines Datenschutzbeauftragten nicht erfüllen, entbindet Sie dies allerdings nicht von der Verantwortung für den Umgang mit Personendaten. Ohne Datenschutzbeauftragten ist die Geschäftsleitung selbst weiterhin verantwortlich (=der Verantwortliche für die Datenverarbeitung).

Gemeinsame Verantwortliche (Art. 26 DSGVO)

In vielen Fällen wird der Spielbetrieb auf einer Golfanlage von oftmals zwei verschiedenen Rechtsformen organisiert, z.B. eine GmbH und ein eingetragener Verein. In diesen Fällen werden die personenbezogenen Daten von Mitgliedern und auch Gästen in vielen Fällen von beiden Rechtsformen verarbeitet.

Grundsätzlich sind diese beiden „Rechtsformen“ eigenständige Verantwortliche, so dass jede Rechtsform selbst für die Verarbeitung der Daten verantwortlich ist und der „Datenfluss“ zwischen diesen Rechtsformen entsprechend geregelt werden muss.

[2] Thomas Kranig, BayLDA, „Erste Hilfe zur Datenschutz-Grundverordnung“, C.H.Beck, München 2017, S. 34

Die DSGVO sieht in solchen Fällen nun die Möglichkeit vor, dass bei mehreren Verantwortlichen ein sogenannter „Gemeinsamer Verantwortlicher“ eingeführt wird. Diese Möglichkeit ist neu, deshalb sind zu der konkreten Umsetzung bislang wenige Erläuterungen vorhanden.

Generell ist dazu festzuhalten, dass sowohl Art. 26 Abs. 1 Satz 2 DSGVO als auch § 63 BDSG (2018) in einem solchen Fall eine transparente Vereinbarung zwischen den gemeinsam Verantwortlichen fordern. Dabei muss zwingend festgelegt sein, wer welche datenschutzrechtlichen Verpflichtungen erfüllt. In diesem Zusammenhang wird ausdrücklich die Wahrnehmung der Rechte der Betroffenen und die Erfüllung der Informationspflichten genannt. Inhaltlich ist allerdings sicherzustellen, dass eine klare Zuteilung der Verantwortlichkeiten sichergestellt sein muss.

Siehe hierzu auch den Gesetzestext:

Art. 26 DSGVO Gemeinsam für die Verarbeitung Verantwortliche

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Siehe dazu auch „Erwägungsgrund 79“: Zuteilung der Verantwortlichkeit

Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung, einschließlich der Fälle, in denen ein Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines Verantwortlichen durchgeführt wird.

Empfehlung: Sind auf einer Golfanlage zwei (oder mehr) Rechtsformen vorhanden (z.B. Betreibergesellschaft und Verein), dann kann das „Zusammenwirken“ dieser Gebilde in einer transparenten Vereinbarung nach Art. 26 DSGVO geregelt werden. Damit werden verschiedene interne Vorgaben deutlich vereinfacht. Die betroffenen Mitglieder sind darüber entsprechend zu informieren.

Auftragsverarbeitung

In vielen Firmen wie auch in Golfclubs und Golfanlagen erfolgt die Verarbeitung personenbezogener Daten selten ohne fremde Hilfe oder externe Dienstleister.

Eine Auftragsverarbeitung ist durchaus zulässig, sofern die gesetzlichen Bedingungen eingehalten werden und dies vertraglich geregelt wird.

GOLFCLUB oder -ANLAGE	DIENSTLEISTER
▪ Verantwortlich für die Verarbeitung der Daten der Mitglieder und Gäste ▪ Auswahl des Dienstleisters ▪ Kontrolle der Einhaltung der Sicherheitsmaßnahmen ▪ ggf. Bestellung eines Datenschutzbeauftragten ▪ schriftlicher Vertrag erforderlich	▪ verarbeitet die Daten auf Weisung des Golfclubs oder -anlage ▪ ggf. Bestellung eines Datenschutzbeauftragten ▪ Datenverarbeitung innerhalb der EU ▪ verantwortlich für die Sicherheitsmaßnahmen ▪ schriftlicher Vertrag erforderlich

Vertrag über Auftragsverarbeitung gesetzlich vorgeschrieben!

- ➢ Unterschrift oder digitale Bestätigung des Vertrages erforderlich!
- ➢ ohne Vertrag Auftragsverarbeitung NICHT zulässig!

ACHTUNG: Hohe Bußgelder!

Beispiele:

- Software für Mitglieder- und Turnierverwaltung
- Betreiber von Web-Seiten
- externe Lohnabrechnung, Buchhaltung
- IT-Dienstleister zur Betreuung der Hardware
- externe Rechenzentren, in denen Daten gespeichert werden

Künftig haften bei Verstößen nicht nur der Auftraggeber der Datenverarbeitung, sondern auch der Auftragnehmer (also der eigentliche Datenverarbeiter). Damit müssen die Vertragsregelungen zur Auftragsverarbeitung mit den bisherigen Vertragspartnern überarbeitet und an die neue Rechtslage angepasst werden.

Verstärkung der Rechte der Betroffenen

Eine deutliche Erweiterung erfahren mit dem Inkrafttreten der DSGVO die Pflichten, betroffene Personen bereits bei Erhebung personenbezogener Daten u. a. über den Zweck der Verarbeitung zu informieren. Soweit die Daten – wie auf Golfanlagen üblich – unmittelbar selbst erhoben werden, sind zu diesem Zeitpunkt, z. B. im Antrag auf Aufnahme in den Golfclub, und sofern für die Datenverarbeitung bedeutsam, folgende Informationen zu geben:

- Name bzw. Firma sowie Kontaktdaten des Golfclubs,
- Kontaktdaten des ggfs. vorhandenen Datenschutzbeauftragten,
- Zwecke und Rechtsgrundlage der Datenverarbeitung,
- Empfänger der personenbezogenen Daten (d. h. derjenige, demgegenüber die Daten offengelegt werden),
- die geplante Speicherdauer oder falls unmöglich die Kriterien für die Festlegung der Speicherdauer,
- 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,
- gegebenenfalls das Recht zum jederzeitigen Widerruf einer Einwilligung mit Wirkung für die Zukunft,
- das Beschwerderecht bei der Aufsichtsbehörde.

Nachdem diese Informationspflichten über das bislang erforderliche Maß hinausgehen und damit bisher kaum erfüllt worden sein dürften, empfiehlt sich die Erstellung eines Informationsblatts für die jeweils betroffene Personengruppe (Mitglieder, Gäste, Mitarbeiter).

Hierzu hat der DGV mit seiner Broschüre im November 2017 eine Mustervorlage übersandt, in der die erforderlichen Informationen für die Verarbeitung der Daten durch den DGV über das DGV-Intranet enthalten sind. Diese Mustervorlage muss nun allerdings noch um die Informationen zu den Datenverarbeitungsvorgängen der jeweiligen Golfanlage ergänzt werde.

Soweit Gastspieler betroffen sind, empfiehlt sich ein entsprechender Aushang im Sekretariat, bei Buchungen über das Internet ein Hinweis dort.

Bitte beachten Sie, dass die Regelungen der DSGVO und damit die Informationspflichten auch gegenüber den Mitarbeiterinnen und Mitarbeitern des Golfclubs gelten!

Meldepflicht bei Datenschutzverstößen (künftig innerhalb von 72 Stunden)

Was ist eine „Datenpanne“?

Gehackt, gestohlen oder verloren. Die Möglichkeiten, dass personenbezogene Daten in unbefugte Hände gelangen, sind vielseitig, z.B.

- eine Webanwendung, die eine Sicherheitslücke aufweist,
- ein Bug im Webserver, der einen Vollzugriff auf Systemebene ermöglicht,
- ein verlorener USB-Stick mit Personendaten,
- ein Einbruch in den schlecht gesicherten Serverraum, der mit einem Verlust der Backup-Platten einhergeht,
- Diebstahl eines mobilen Endgerätes (Laptop, Smartphone), auf dem Zugangsdaten zum IT-System der Golfanlage gespeichert sind,
- Angriff von außen durch Schadsoftware wie Virus oder Trojaner,
- Missbrauch von Personendaten durch Beschäftigte,
- Unzulässige Weitergabe von Daten an Dritte.

Die Meldung von Datenpannen ist grundsätzlich nichts Neues. Bislang war dies in § 42a BDSG enthalten, allerdings nur wenn besonders sensible Daten betroffen waren und durch die Datenpanne ein hohes Risiko für den Betroffenen entstand. Deshalb waren die Meldungen auf dieser Grundlage bislang in Deutschland nur gering.

Nunmehr werden durch die Neuregelungen der DSGVO die Schwellen für eine Meldung deutlich gesenkt.

Im Unterschied zu § 42a BDSG (alt) gilt die Meldepflicht nach Art. 33 DSGVO nicht nur bei Datenpannen bzgl. bestimmter „sensibler" personenbezogener Daten (wie etwa Gesundheitsdaten), sondern bei jeglicher „Gefahr" für personenbezogene Daten. Einzige Einschränkung ist, dass eine Meldung an die Aufsichtsbehörde nicht erfolgen muss, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt." Dies ist eine Prognoseentscheidung, die entsprechend begründet werden muss. Im Zweifel raten wir deshalb zu einer Meldung.

Ein weiterer großer Unterschied zur bisherigen Rechtslage ist der Umstand, dass nach der Definition des Art. 4 Nr. 12 DSGVO für eine Meldepflicht bereits ein reiner Datenverlust ausreicht, ohne dass bereits ein Missbrauch vorliegen muss.

Bedeutet die Datenpanne „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten" des Betroffenen, so ist neben der zuständigen Aufsichtsbehörde zusätzlich auch der Betroffene unverzüglich gem. Art. 34 DSGVO von der Datenschutzverletzung „in klarer und einfacher Sprache" zu unterrichten.

Der bayrische Datenschutzbeauftragte bietet für die Meldung bereits ein „Online-Meldeformular" an: https://www.lda.bayern.de/de/datenpanne.html.

Welche Maßnahmen eine Aufsichtsbehörde nach Eingang einer solchen Meldung trifft, ist nicht konkret festgelegt, aber sicherlich abhängig von Art und Ausmaß der Datenpanne. Auf jeden Fall sollte sich eine Golfanlage darauf einstellen, dass die zuständige Aufsichtsbehörde im Falle einer „Datenpanne" die entsprechenden Datenschutzregelungen überprüfen wird (siehe Rechenschaftspflicht).

Verzeichnisse über Verarbeitungstätigkeiten

Das Verfahrens- bzw. Verarbeitungsverzeichnis gewinnt – und hierin liegt eine ganz wesentliche Änderung gegenüber der aktuellen Rechtslage – zukünftig erheblich an Bedeutung, denn wie oben dargestellt ist der Golfclub für eine rechtskonforme Verarbeitung personenbezogener Daten „verantwortlich und muss deren Einhaltung nachweisen können."

Der Kern dieser Dokumentation sind die „Verzeichnisse über Verarbeitungstätigkeiten". Hierzu haben die deutschen Aufsichtsbehörden entsprechende Muster bereitgestellt, die von CompCor zur erleichterten Nutzung entsprechend erweitert wurden. Die CompCor-Muster können auf Wunsch interessierten Golfanlagen zur Verfügung gestellt werden.

Der DGV hat in seinen Informationen vom November 2017 Muster für ein Verarbeitungsverzeichnis für die Nutzung in Zusammenhang mit dem DGV-Intranet für die Golfclubs bereitgestellt.

Sofern die Golfanlage der vom DGV mit Rundschreiben vom 11. Dezember 2008 (Rundschreiben Nr. 27/08) gegebenen Empfehlung gefolgt und personenbezogene Datenverarbeitungen in einer Vereinsordnung zum Datenschutz bzw. im Spielrechtsvertrag erfasst wurden, kann die Golfanlage damit auf ein aktuelles Verfahrensverzeichnis zu diesem Bereich zurückgreifen.

Datenschutz-Folgenabschätzung

Dies ist eine neue, wesentliche Formvorschrift der DSGVO, die allerdings Golfanlagen und Golfclubs nur im besonderen Fällen trifft.

Wann ist dies durchzuführen?

Hat eine Form der Verarbeitung …. ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen ….. durch.
(Art 35 (1) DSGVO).

Inhalte einer Datenschutz-Folgenabschätzung:

Die DSGVO bestimmt in Art. 35 Abs. 7 Mindestanforderungen bezüglich des Inhalts einer Datenschutz-Folgeabschätzung.

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen.
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.
- Eine Bewertung der Risiken der Rechte und Freiheiten der betroffenen Personen.
- Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden.

Anwendungsbeispiele für Golfanlagen:

Aus unserer Sicht wäre eine Datenschutz-Folgenabschätzung bei Golfanlagen zumindest in folgenden Fällen erforderlich:

- Einrichtung von Videoanlagen, bei denen personenbezogene Daten erkennbar sind.
- Verarbeitung besonders sensibler Daten in Zusammenhang mit Leistungsüberwachung bestimmter Trainingseinheiten (Gesundheitsdaten, Leistungsdaten).
- Bereitstellung selbst erstellter IT-Anwendungen (App), die auch Zugriff auf Ortungsdaten ermöglichen.

Datenschutz durch Technik und Voreinstellungen

Begriffe wie Datensicherheit, IT-Sicherheit und technischer Datenschutz werden im heutigen Datenschutzalltag zwar häufig verwendet, aber leider immer wieder miteinander vermischt oder auch verwechselt. Es besteht deshalb ein nicht unwesentlicher Interpretationsspielraum, welche technischen Sicherheitsmaßnahmen auch aus Datenschutzgesichtspunkten erforderlich sind.

Der bisherige § 9 BDSG (alt) zu den erforderlichen technischen und organisatorischen Maßnahmen wird nun durch die Regelungen der DSGVO ersetzt.

Besondere Bedeutung hat Art. 32 DSGVO, der den Titel „Sicherheit der Verarbeitung“ trägt. In diesem Artikel wird beschrieben, nach welchen Kriterien technische und organisatorische Maßnahmen zu wählen sind, um ein angemessenes Schutzniveau zu gewährleisten.

In Art. 25 und Art. 32 DSGVO werden einige Maßnahmen und Schutzziele in Bezug auf die Technik und Sicherheit der Datenverarbeitung aufgeführt. Diese beziehen sich teils unmittelbar auf die personenbezogenen Daten, teils aber auch auf die Systeme und Dienste, die im Zusammenhang mit der Datenverarbeitung eingesetzt werden (vgl. insbesondere Art. 32 Abs. 1 DSGVO).

Auch wenn hier teilweise neue Begrifflichkeiten und Systematiken verwendet werden, finden sich doch letztlich alle bisher schon erforderlichen Sicherheitsanforderungen auch in der Datenschutz-Grundverordnung wieder:

- Vertraulichkeit: Schutz vor unbefugter Kenntnisnahme der Daten.
- Integrität: Gewährleistung der Echtheit, Vollständigkeit, Zurechenbarkeit, Urheberschaft und (Rechts-)gültigkeit der Daten.
- Verfügbarkeit: zeitgerechte Bereitstellung von Daten, Möglichkeit zur ordnungsgemäßen Verarbeitung.
- Belastbarkeit („Resilience“): Dies ist ein neuer Begriff, der bisher im Datenschutzbereich nicht verwendet wurde. Im IT-Bereich ist mit „Resilience“ üblicherweise eine gewisse Stabilität gegenüber Ausfällen oder Angriffen – wie etwa „Denial of Service“-Angriffen – gemeint. Die Abgrenzung zur Verfügbarkeit ist jedoch nicht eindeutig.
- Wiederherstellbarkeit: Dieser Begriff wurde bisher ebenfalls nicht als eigenständiges Schutzziel verwendet, da auch er dem Begriff der Verfügbarkeit zugeordnet werden könnte. Hierunter fallen Notfallkonzepte für Rechenzentren, um nach einem Ausfall oder Angriff schnell wieder betriebsbereit zu sein.
- Data protection by design/Datenschutz durch Technikgestaltung: Fragen des Datenschutzes müssen zukünftig bereits bei der Konzipierung von Verfahren und Produkten betrachtet werden. Dies betrifft etwa die Punkte Datenminimierung (Pflichtfelder), Pseudonymisierung, Möglichkeiten zur Datenlöschung, sichere Verschlüsselung und Berechtigungskonzept.
- Data protection by default/datenschutzfreundliche Voreinstellungen: Die Voreinstellungen von Produkten und Verfahren sollen so gestaltet sein, dass sie die Grundprinzipien des Datenschutzes und der IT-Sicherheit von vornherein berücksichtigen (Beispiele: keine Standard-Passwörter, Verschlüsselung aktiviert, Beschränkung der Berechtigungen von Nutzenden, Ortungsdienste ausgeschaltet). Dieser Aspekt sollte zukünftig insbesondere bei der Beschaffung von Produkten berücksichtigt werden.
- Pseudonymisierung, Verschlüsselung: Diese beiden Maßnahmen dienen den Zielen der Vertraulichkeit und Integrität.

Bei der Auswahl der technischen und organisatorischen Maßnahmen ist gemäß Art. 25 DSGVO der „Stand der Technik“ zu beachten, der jedoch gesetzlich nicht näher definiert wird. Wie bisher auch, ist es daher sinnvoll, sich an öffentlich zugänglichen Standards zu orientieren (siehe BSI - Bundesamt für Sicherheit in der Informationstechnik).

Für die Prüfung, ob eine konkrete technische und organisatorische Maßnahme erforderlich ist, müssen (wie bisher) die Implementierungskosten mit den Ergebnissen der Risikoanalyse abgewogen werden. Zudem müssen der Schutzbedarf der Daten und die Ergebnisse der Risikoanalyse betrachtet werden. Je sensibler die Daten (siehe etwa besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO) und je höher die Risiken für die betroffenen Personen sind, desto umfassendere Maßnahmen sind erforderlich.

Deshalb: Es wird nun ein Datenschutzkonzept erforderlich sein, das die Risikoanalyse, die ergriffenen Maßnahmen und die regelmäßigen Prüfungen umfasst.

Was Sie in einer Golfanlage deshalb umsetzen sollten (ToDo-Liste):

- ✓ Überprüfen Sie Ihre Rechtsgrundlagen zur Verarbeitung personenbezogener Daten von Mitgliedern, Gästen und Personal (Vertrag, Satzung, Arbeitsverträge).
  Passen Sie diese bei Bedarf an.
- ✓ Überprüfen sie die vorhandenen Einwilligungen und passen Sie diese bei Bedarf an.
  Beachten Sie insbesondere die Regelungen für Einwilligungen von Kindern und Jugendlichen!
- ✓ Erstellen Sie eine Dokumentation der Verfahren zur Verarbeitung der personenbezogenen Daten, von besonderer Bedeutung sind u.a.
  - interne Datenschutz-Richtlinien, Prozessanweisungen
  - Anpassung der Einwilligungserklärungen
  - Aktualisierung der Erklärungen für Webseiten
- ✓ Erstellen oder aktualisieren Sie Ihre Verzeichnisse über Verarbeitungstätigkeiten.
- ✓ Bestimmen Sie einen Ansprechpartner im Vorstand/in der Geschäftsleitung für Datenschutz.
  Bei mehreren Rechtsformen (GmbH, e.V.) sollten Sie das Zusammenwirken konkret regeln (gemeinsame Verantwortliche).
- ✓ Prüfen Sie, ob Sie einen Datenschutzbeauftragten bestellen müssen. Falls ja, bestellen Sie einen internen oder externen DSB und melden diesen an die zuständige Aufsichtsbehörde.
- ✓ Prüfen Sie folgende Gesichtspunkte:
  Wer kann in der Golfanlage auf welche personenbezogenen Daten zugreifen?
  Zugriff und Auswertung auf einzelne Daten (Mitgliedsbeiträge, Bankdaten, Mahnverfahren, Auswertungen einzelner Daten wie z.B. Zutrittsdaten, Veröffentlichungen im Internet oder Club-Magazin, Datenübermittlungen).
  Wer hat welche Auswertungsbefugnisse? Wie wird dies kontrolliert?
  Regeln Sie die entsprechenden Rechte.
- ✓ Überprüfen Sie Ihre vorhandenen techn. und organisatorischen Sicherungsmaßnahmen.
- ✓ Überprüfen Sie, welche personenbezogenen Daten Sie bei Marketing-Maßnahmen, Newslettern, Social-Media-Plattformen verarbeiten. Passen Sie bei Bedarf die Regelungen an.
- ✓ Überprüfen Sie die Speicherdauer der Daten. Führen Sie ein Löschkonzept ein.
- ✓ Prüfen Sie, welche Auftragsverarbeitungs-Verhältnisse vorliegen (Club-Software, Internet-Provider, Personaldaten, Buchhaltung u.a.). Passen Sie bei Bedarf die Verträge an.
- ✓ Informieren Sie die Betroffenen über die Verarbeitung Ihrer Daten.
- ✓ Richten Sie einen internen Meldeprozess für die Entgegennahme von Auskunftsersuchen oder Anfragen von Betroffenen ein.
- ✓ Richten Sie einen internen Meldeprozess für Datenpannen ein.
- ✓ Schulen Sie regelmäßig alle beteiligten Personen in der Golfanlage zum Datenschutz.
- ✓ Überprüfen Sie regelmäßig Ihre Verfahren. Erstellen Sie einen internen Jahresbericht.

Einzelfragen:

Wie gehe ich zukünftig mit dem Aushang von Start- und Ergebnislisten bei Golfturnieren korrekt um?

Startlisten:

Wegen der mit dem Internet verbundenen Risiken ist sicherzustellen, dass der Zugriff auf eine Startliste über das Internet nicht für jedermann möglich ist. Eine Startliste enthält sensible Daten, nämlich die Startzeiten einzelner Personen, die gleichzeitig deren Abwesenheit von zu Hause dokumentieren.

Die Veröffentlichung einer Startliste im Internet ist deshalb nur über einen passwortgeschützten Zugang möglich. Der Aushang einer Startliste am Schwarzen Brett im Golfclub ist zulässig. Über die Verfahrensweise sollte der Betroffene vorab informiert werden (z. B. durch Hinweis in einer Rahmenausschreibung oder auf der Meldeliste).

Ergebnislisten:

Dem Aushang von Ergebnislisten stehen keine überwiegenden schutzwürdigen Interessen der Mitglieder regelmäßig entgegen. Dies dient unmittelbar der Verwirklichung des Vereinszwecks (Sportausübung durch die Mitglieder) und ist daher zulässig, auch die Veröffentlichung der Ergebnisliste im Internet. Es sollte jedoch auch hier bereits bei der Datenerhebung (Meldung zum Wettspiel) oder gar schon in der (Rahmen-) Ausschreibung deutlich darauf hingewiesen werden, dass eine Veröffentlichung der Ergebnisliste im Internet erfolgt. Widerspricht ein Betroffener der Veröffentlichung seiner Daten im Rahmen der Ergebnisliste, so wäre sein Name im Internet „zu schwärzen“.

Dürfen Daten von Turnierteilnehmern an Sponsoren übermittelt werden?

Eine Weitergabe von personenbezogenen Daten von Turnierteilnehmern an Sponsoren ist nur mit Einwilligung des Betroffenen zulässig. Diese Einwilligung kann im Rahmen der Turnieranmeldung erhoben werden.

Widerspricht ein Turnierteilnehmer im Rahmen der Turnieranmeldung der Weitergabe seiner Daten an den Sponsor, dann ist ein Ausschluss aus dem Turnier gesetzlich nicht zulässig.

Startzeiten-Buchungen: Wie behandle ich Buchungen von Startzeiten für weitere Mitspieler?

Zur Abwicklung eines effizienten Startzeiten-Buchungsmoduls ist es erforderlich, dass bei Buchung einer Startzeit für den Interessenten ersichtlich ist, welche weiteren Mitspieler bereits diese mögliche Startzeit gebucht haben.

Eine Einsicht in die Übersicht der gebuchten Personen sollte aber nicht für jedermann möglich sein, sondern erst nach einer passwortgeschützten Anmeldung am Buchungssystem.

Ferner sollten die Betroffenen bei Einführung des Buchungsmoduls bzw. über entsprechende Informationen auf der Webseite über diese Veröffentlichung informiert werden und entsprechend bei der Erst-Registrierung im Buchungsmodul den jeweiligen Datenschutzregeln der Golfanlage zustimmen.

Dürfen Messenger-Dienste wie WhatsApp für das Jugendtraining genutzt werden?

Dies bedarf der Regelung im Einzelfall, so dass hier eine sorgfältige Prüfung und Regelung zwingend erforderlich ist!

Grundsätzlich ist die Nutzung von Messenger-Diensten für eine Gruppe Jugendlicher möglich, muss jedoch entsprechend geregelt werden. Hierbei sind folgende Punkte zu bedenken bzw. zu regeln:

- Auswahl des Messenger-Dienstes (US-Anbieter WhatsApp oder europäische Anbieter wie „Telegram“).
- Vereinbarung über Auftragsverarbeitung mit dem Software-Anbieter.
- Festlegung der konkreten Funktionen der Messenger-Gruppe (nur Termine, Kommunikation, Ortungsdienste?).
- Zustimmung der Betroffenen vor Nutzung der Gruppe (bei Kinder und Jugendlichen unter 16 Jahren durch alle Erziehungsberechtigte).

Wie ist mit Dateien zu verfahren, die personenbezogene Daten enthalten, aber nicht in der Clubverwaltungs-Software integriert sind?

Wie bei allen personenbezogenen Daten, die durch einen Golfclub oder Betreibergesellschaft erhoben und verarbeitet werden, sind auch hier folgende Punkte zu klären bzw. zu regeln:

- Rechtsgrundlage der Verarbeitung
- Wer hat Zugriff auf die Daten
- An wen werden die Daten übermittelt (Funktionsträger, externe Dienstleister)
- Nutzungsregelungen, Zweckbegrenzung
- Anweisungen zur technischen Sicherung der Daten
- Regeln zur Datensicherung und Löschung

Dürfen Kontaktdaten von Mitgliedern an Mannschafts-Captains übermittelt werden?

Die Weitergabe von Personendaten einzelner Mitglieder mit Anschrift, Kontaktdaten (Email) und ggf. Geburtsdatum an einen Mannschafts-Captain ist zur Durchführung des Vereinszwecks zulässig. In der internen Datenschutz-Richtlinie der Golfanlage ist allerdings entsprechend zu regeln, dass die Daten nur zum Vereinszweck verwendet werden dürfen, eine Übermittlung an Dritte (z.B. Versicherungen) nicht zulässig ist, die Daten entsprechend sicher aufzubewahren sind und nach Ende der Funktion zu löschen sind.

Was ist bei Fotoveröffentlichungen und Videoüberwachungen zu beachten?

Fotoveröffentlichungen:

Golfvereine dürfen aus Gründen des Persönlichkeitsschutzes grundsätzlich keine Angaben über Mitglieder an die Presse oder an andere Medien übermitteln, soweit schutzwürdige Interessen der Mitglieder entgegenstehen. Schutzwürdige Interessen werden nicht entgegenstehen, wenn nur der Name und ein Spiel- bzw. Wettspielergebnis im Rahmen einer Berichterstattung über ein Vereinswettspiel weitergegeben wird. Mit einer solchen üblichen Berichterstattung muss das Mitglied rechnen und willigt darin von vornherein ein.
Eine Veröffentlichung von Bildern ist nur mit Einwilligung der Betroffenen zulässig.

Videoüberwachung:

Dies ist gesetzlich geregelt und grundsätzlich nur in Ausnahmefällen möglich. Eine konkrete Beurteilung kann nur im Einzelfall erfolgen. Bitte beachten Sie, dass Sie hier ggf. eine Datenschutz-Folgenabschätzung benötigen.

Falls Sie zu einzelnen Punkten Rückfragen haben, können Sie sich gerne direkt an uns wenden (office@compcor.de).

CompCor Compliance Solutions GmbH & Co. KG

Frankfurt am Main, März 2018

Angebot der CompCor Compliance Solutions für Golfbetreiberanlagen und Golfclubs:

Die CompCor Compliance Solutions GmbH & Co. KG bündelt Kompetenzen und Erfahrungen im Beratungs- und Trainingsbereich zu Compliance-Themenstellungen.

Die Schwerpunkte dabei sind die Bereitstellung von Compliance-Tools zur Erleichterung der Compliance- und Datenschutz-Maßnahmen im Unternehmen (z.B. CompCor Compliance Process Tools, CompCor Hinweisgebersystem oder Compliance Trainingsprodukte) und eine verfahrens- bzw. produktorientierte Compliance-Beratung bis hin zur Übernahme der Funktion des externen Compliance Officers oder externen Datenschutzbeauftragten.

Das Angebot von CompCor umfasst auch die Umsetzung eines umfassenden Compliance Management Systems oder Datenschutz Management Systems.

Mehr als 20 interdisziplinär arbeitende Ingenieure, Naturwissenschaftler, Rechtsanwälte und Datenschutz-Experten stehen hinter ihren Kunden, um gemeinsam die Projekte perfekt umzusetzen.

Übernahme der Funktion des externen Datenschutzbeauftragten für Golfanlagen

Ein erfahrener Senior Consulter von CompCor übernimmt das Mandat als „externer Datenschutzbeauftragter“. Vertragspartner ist die CompCor Compliance Solutions GmbH & Co. KG.

Da mehrere Personen bei CompCor seit vielen Jahren auch aktiv Golf spielen, sind wir sowohl mit der eingesetzten Clubverwaltungs-Software als auch den Abläufen eines Golfclubs bestens vertraut.

Ansprechpartner bei der CompCor Compliance Solutions

Frau Jana Vogel (Senior Sales Consultant Compliance) steht Ihnen bei Fragen oder zur weiteren Kontaktaufnahme zur Verfügung.

CompCor Sales Office:	(0) 7232 - 809 14 – 0
E-Mail:	office@compcor.de