Wichtige Hinweise:

Die vorliegende Darstellung soll der Tineon AG eine Arbeitshilfe zum Umgang mit dem Thema Datenschutz geben. Sie beantwortet im Sinne eines Nachschlagewerkes häufig gestellte Fragen und gibt einen Überblick über wichtige Themenfelder, in denen ein Tätigwerden der Tineon AG aus datenschutzrechtlicher Sicht erforderlich ist. Es kann als Muster für ein Handbuch zum Datenschutz im Unternehmen dienen.

Dieses Handbuch wurde mit größtmöglicher Sorgfalt erstellt. Die Tineon AG ist stets bemüht, dieses Handbuch an die aktuelle Rechtslage anzupassen. Eine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität kann jedoch nicht übernommen werden. Das Handbuch kann zudem eine Rechtsberatung im Einzelfall nicht ersetzen.

Tineon AG

Stand: Mai 2018

Datenschutz-Handbuch

Tineon AG

1 Geltungsbereich

Dieses Handbuch gilt für die Geschäftsleitung, die leitenden Angestellten (im Sinne des BetrVerfG), sowie alle Beschäftigten der Tineon AG.

2 Vorwort

Die Verarbeitung personenbezogener Daten beinhaltet stets einen Eingriff in die verfassungsrechtlich geschützte Sphäre. Die Achtung der deutschen und europäischen Grundrechte und die Bindung an Recht und Gesetz verpflichten uns, den Schutz personenbezogener Daten als wichtige Aufgabe zu verstehen. Jeder Umgang mit personenbezogenen Daten bedarf einer gesetzlichen Grundlage als Rechtfertigung für den damit verbundenen Eingriff. Dieses Datenschutzhandbuch regelt die clubinternen Verantwortlichkeiten beim Umgang mit personenbezogenen Daten.

3 Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten obliegen folgende Aufgaben:

- Unterrichtung und Beratung des Vorstandes und der Beschäftigten, die Verarbeitungen personenbezogener Daten durchführen, hinsichtlich ihrer Pflichten nach der EU Datenschutz-Grundverordnung (DSGVO), dem Bundesdatenschutzgesetz (BDSG) sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Bundesrepublik Deutschland;
- Überwachung der Einhaltung der DSGVO und des BDSG, anderer Datenschutzvorschriften der Union bzw. der Bundesrepublik Deutschland sowie der Strategien des Golfclubs für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation und gegebenenfalls Beratung zu allen sonstigen Fragen.

Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Für alle Fragen "rund um das Thema Datenschutz" wenden Sie sich bitte an unseren Datenschutzbeauftragten:

Andreas Winnes
c/o OmniPC GmbH, Mollenbachstrasse 14, 71229 Leonberg
Turmstraße 9, 78467 Konstanz
Tel. 07531 – 89282-0, Fax 07531 – 89283-77
E-Mail awinnes@omnipc.de

4 Einleitung

Die in der Tineon AG zu verarbeitenden personenbezogenen Daten und die eingesetzte Technologie der Datenverarbeitung sind unentbehrliche Arbeitsmittel und stellen wichtige Instrumente zur Erfüllung der Zwecke der Tineon AG dar. Sie müssen schon aus diesen Gründen heraus vor Verlust, unbefugter Veränderung, unbefugter Nutzung und zufälliger Zerstörung geschützt werden.

Die Themen "Datenschutz & Datensicherheit" sind somit ein wesentlicher Bestandteil unseres allgemeinen Qualitätsmanagements.

Dieses Datenschutzhandbuch gilt für alle Beschäftigten der Tineon AG. Die Gesamtheit der Regelungen hat verbindlichen Charakter, so dass Verstöße gegen die Inhalte dieses Datenschutzhandbuchs zu arbeitsrechtlichen Konsequenzen führen können.

Die DSGVO und das BDSG sind die allgemeine gesetzliche Grundlage für die Verarbeitung von personenbezogenen Daten. Es kommt darauf an, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Die in den Grundsätzen zum Datenschutz geforderten Maßnahmen dienen auch der Wahrung von Geschäftsgeheimnissen.

Bei allen unseren Aktivitäten müssen wir uns immer Eines vor Augen führen:

Datenschutz legt den Fokus auf **personenbezogene Daten**. Dies sind persönliche oder sachliche Informationen über bestimmte oder bestimmbare natürliche Personen (Betroffene), wie z.B. Angaben über Name, Adresse, Beruf, Geburtsdatum oder Vermögensverhältnisse, usw. Betroffene sind neben den Mitarbeitern und „Kunden“ auch Geschäftspartner oder auch Bewerber.

Als besonders sensibel gelten personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

4.1 Verantwortlichkeiten und Zuständigkeiten

Die Verpflichtung zur Einhaltung der Datenschutzgesetze obliegt jeweils dem "Verantwortlichen" im Sinne der DSGVO (unserer Geschäftsleitung). "Verantwortlicher" ist jede Person oder Stelle, die personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt.

Somit ist nicht nur die Tineon AG, sondern vielmehr auch jeder Beschäftigte oder vertraglich verbundene Dienstleister zur Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet, unabhängig seiner Funktion bzw. Stellung in der Tineon AG. Führungskräften kommt insofern eine Vorbildfunktion zu.

4.1.1 Die Verantwortung *der Geschäftsführung/des Vorstands*

Der Vorstand hat die Verantwortung für die Rechtmäßigkeit des Umgangs mit personenbezogenen Daten innerhalb der Tineon AG und bei ihrer Übermittlung. Er ist beispielsweise Adressat, wenn

- die betroffene Person ihre Rechte wahrnimmt,
- eine Kontrollinstitution in der Tineon AG die Beachtung datenschutzrechtlicher Bestimmungen überprüft, es wegen der Verletzung datenschutzrechtlicher Regelungen zu einem Bußgeldbescheid kommt.

Ihm steht das Recht zu,

- innerhalb der Tineon AG Einzelheiten für den Umgang mit personenbezogenen Daten verbindlich festzulegen,

- Strafantrag für den Fall eines datenschutzrechtlichen Verstoßes innerhalb der Tineon AG zu stellen.

Der Vorstand

- setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt.

- trifft geeignete technische und organisatorische Maßnahmen, 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.

- trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. 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.

- meldet im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, diese der zuständigen Datenschutz-Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

- benachrichtigt im Falle einer Verletzung des Schutzes personenbezogener Daten die betroffene Person unverzüglich von der Verletzung, es sei denn, die Verletzung des Schutzes personenbezogener Daten hat voraussichtlich kein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge.

- stellt die Rechte der betroffenen Person sicher, insbesondere die Informationspflicht, das Auskunftsrecht, das Recht auf Berichtigung, das Recht auf Löschung das Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit und das Widerspruchsrecht (Art. 13 -23 DSGVO).

4.1.2 Der Datenschutzbeauftragte der Tineon AG

- nimmt die Aufgaben gem. 3 wahr,

- berät den Vorstand der Tineon AG und die übrigen Mitarbeiter oder Dienstleister in allen Angelegenheiten des Datenschutzes und koordiniert die Datenschutzmaßnahmen innerhalb der Tineon AG,

- prüft die Zulässigkeit der rechtmäßigen Verarbeitung personenbezogener Daten in Akten und automatisierten Verarbeitungen,

- schult die Mitarbeiter und ggf. auch die Dienstleister der Tineon AG in datenschutzrechtlichen Aspekten sowie zur Umsetzung datenschutzrechtlicher Bestimmungen,

- ist befugt Prüfungen sowie Kontrollen zur Einhaltung des Datenschutzes innerhalb der Tineon AG durchzuführen,

- überwacht die Übersicht über alle Verfahren, in denen personenbezogene Daten gespeichert sind oder verarbeitet werden,

- überwacht ggf. gesetzliche Meldepflichten und ist Ansprechpartner der Geschäftsleitung, der Mitarbeiter, von Kunden und von Dritten in allen Angelegenheiten, die den Datenschutz in der Tineon AG betreffen,

4.1.3 Mitarbeiter und vertraglich verbundene Unternehmen oder Dienstleister der Tineon AG

sind beim Umgang mit personenbezogenen Daten für die Beachtung der gesetzlichen Vorgaben sowie des Datenschutzhandbuchs des Golfclubs verantwortlich.

4.2 Verpflichtung der Mitarbeiter

Die Verpflichtung der Mitarbeiter oder vertraglich mit ihr verbundene Unternehmen und Dienstleister zur Vertraulichkeit ist Basis des Datenschutzes. Deshalb ist jeder Beschäftigte oder vertraglich mit ihr verbundene Unternehmen und Dienstleister, der mit der Verarbeitung und/oder Nutzung personenbezogener Daten betraut ist, auf die Einhaltung des geltenden Datenschutzrechts zu verpflichten.

Insbesondere gilt:

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

5 Grundlagen des Datenschutzes

5.1 Informationelles Selbstbestimmungsrecht

Der Begriff des "*informationellen Selbstbestimmungsrechts"* geht zurück auf ein Gutachten von Wilhelm Steinmüller und Bernd Lutterbeck aus dem Jahre 1971. Das informationelle Selbstbestimmungsrecht ist eine Ausprägung des allgemeinen Persönlichkeitsrechts und wurde vom Bundesverfas-

sungsgericht im so genannten Volkszählungsurteil 1983 als Grundrecht anerkannt. Ausgangspunkt für das Bundesverfassungsgericht ist das Allgemeine Persönlichkeitsrecht, also Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG.

Die freie Selbstbestimmung bei der Entfaltung der Persönlichkeit werde gefährdet durch die Bedingungen der modernen Datenverarbeitung. Wer nicht wisse oder beeinflussen könne, welche Informationen bezüglich seines Verhaltens gespeichert und vorrätig gehalten werden, werde aus Vorsicht sein Verhalten anpassen. Dies beeinträchtige nicht nur die individuelle Handlungsfreiheit, sondern auch das Gemeinwohl, da ein freiheitlich demokratisches Gemeinwesen der selbstbestimmten Mitwirkung seiner Bürger bedürfe. „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."

Das Recht auf informationelle Selbstbestimmung leitet sich zudem aus Art. 8 der Charta der Grundrechte der EU (Schutz personenbezogener Daten) ab: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten."

5.2 Keine Datenverarbeitung ohne Rechtsgrundlage!

Im Datenschutzrecht gilt: Eine Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, es existiert eine Rechtsgrundlage, die eine Verarbeitung erlaubt.

Mit Relevanz für die Tineon AG kommen als Rechtsgrundlage zur Nutzung personenbezogener Daten insbesondere die folgenden Tatbestände in Betracht:

5.2.1 Rechtsgrundlage: Einwilligung

Nach Art. 6 Abs. 1 Satz 1 lit. a. DSGVO sind Datenverarbeitungen erlaubt, sofern die hiervon betroffene Person ihre Einwilligung mit der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat. Beispielhaft kann die erforderliche Einwilligung in die Zusendung von Informationen mittels Newsletter genannt werden. Einzelheiten zur Einwilligung, insbesondere zu Form und Aufbewahrung, werden unter Ziff. 6.5.2 ff. behandelt.

5.2.2 Rechtsgrundlage: Datenverarbeitung zur Erfüllung des Auftragsverhältnisses

Die Verarbeitung personenbezogener Daten ist weiterhin dann zulässig, wenn die Verarbeitung zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen (Art. 6 Abs. 1 Satz 1 lit. b. DSGVO).

5.3 Verzeichnis der Verarbeitungstätigkeiten

Art. 30 DSGVO verpflichtet grundsätzlich zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten. Da die Verarbeitung personenbezogener Daten in unserem cloudbasierten Software im Sinne des Art. 30 Abs. 5 DSGVO erfolgt, ist ein solches Verzeichnis zu erstellen. Das Verzeichnis ist schriftlich (auch in einem elektronischen Format) zu führen.

Auch Auftragsverarbeiter haben ein Verzeichnis der im Auftrag der Tineon AG durchgeführten Verarbeitungstätigkeiten zu führen. Das jeweilige Verzeichnis ist Anlage der gesondert mit dem Auftragsverarbeiter geschlossenen Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag der Tineon AG (siehe Anlage AVV und TOM der Domain Factory GmbH, Ismaning).

5.4 Auftragsverarbeitung

5.4.1 Definition

Softwareanbieter wie die Tineon AG können im Umgang mit personenbezogenen Daten von Mitgliedern und Mitarbeitern eines Vereins im Rahmen einer Auftragsverarbeitung oder einer Funktionsübertragung (siehe Anlage 1 – Auftragsdatenverarbeitungs-Vereinbarung der Tineon mit ihren Kunden) tätig sein.

Von Auftragsverarbeitung spricht man, wenn sich der Verantwortliche (z.B. Vorstand eines Vereins) einer Stelle bedient, die für ihn im Auftrag und weisungsabhängig personenbezogene Daten verarbeitet wie (z. B. externe IT-Dienstleister oder Anbieter von Clubverwaltungssystemen wie die Tineon AG). Das entscheidende Kriterium und Wesensmerkmal der Auftragsverarbeitung ist: Der Verantwortliche (Verein) bestimmt die Zwecke der Datenverarbeitung allein, während der Auftragsverarbeiter die Verarbeitung gemäß den Weisungen des Verantwortlichen durchführt. (Bertermann in: Ehmann/Selmayr, DSGVO, 2017, Art. 28 Rn. 3).

Die Verarbeitung von Daten im Auftrag bedarf einer vertraglichen Regelung zwischen Verantwortlichem und Auftragsverarbeiter. Die Inhalte dieses Vertrags zur Auftragsverarbeitung müssen mindestens den Vorgaben des Art. 28 DSGVO entsprechen (siehe auch Anlage der Auftragsdatenverarbeitungs-Vereinbarung der Tineon AG für deren Vereine und Nutzer von S-Verein).

Überwiegend nicht als Auftragsverarbeitung wird die Abwicklung von Bankgeschäften (z. B. der Einzug von Mitgliedsbeiträgen u. ä.) durch das beauftragte Kreditinstitut angesehen, weil das Kreditinstitut eine eigene Aufgabe erfüllt. Insofern liegt eine von der Auftragsverarbeitung abzugrenzende sog. Funktionsübertragung vor. Entsprechendes gilt für die Beauftragung von Rechtsanwälten und Steuerberatern, die keine genau definierte, unselbstständig weil nach genauen Weisungen erbrachte Dienstleistung zum Gegenstand haben. Vielmehr bestehen im Hinblick auf die Art und Weise der Durchführung des Auftrags regelmäßig gewisse Entscheidungsspielräume (anders wiederum bei der Lohnbuchhaltung, aber str.). Die Datenweitergabe an den Dritten bedarf allerdings auch in diesen Fällen einer Rechtsgrundlage, die – am Beispiel des Bankeinzugs – wenn nicht schon in einer Einwilligung durch Hingabe der Bankdaten regelmäßig darin zu sehen ist, dass eine Verarbeitung der personenbezogenen Daten zur Erfüllung des Spielrechtsvertrages bzw. des Mitgliedschaftsverhältnisses und damit von Art. 6 Abs. 1 Satz 1 lit. b. DSGVO legitimiert erfolgt.

5.4.2 Anforderungen an die Auswahl des Dritten

Der Auftragsverarbeiter muss durch geeignete technische und organisatorische Maßnahmen (bei IT-Dienstleister bspw. der passwortgeschützte Zugang zu Daten) der hinreichende Garantien dafür bieten, dass die Verarbeitung im Einklang mit dem Datenschutzrecht erfolgt. Als geeignete Garantien zum Nachweis der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters kommen insbesondere Zertifizierungen und genehmigte Verhaltensregeln in Frage. Darüber hinaus kommen Vor-Ort-Audits und Selbstauskünfte durch den Auftragsverarbeiter in Betracht. Genehmigte Verhaltensregeln werden durch die für den Sitz des Auftragsverarbeiters zuständige Datenschutzaufsichtsbehörde genehmigt. Zertifikate müssen hierbei durch akkreditierte Zertifizierungsstellen erbracht werden.

Die Durchführung von Vor-Ort-Audits und die Prüfung von Selbstauskünften müssen hierbei von fachkundigen Personen – in der Regel der Datenschutzbeauftragte – oder durch eine fachkundige externe Stelle erfolgen.

Die Beauftragung weiterer Auftragsverarbeiter durch die Tineon AG darf nur mit schriftlicher (oder elektronischer) Zustimmung erfolgen. Bei Abschluss eines Vertrags zur Auftragsverarbeitung sind die beauftragten weiteren Auftragsverarbeiter zu benennen. Hat ein Verein dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, so hat der Auftrags-

verarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung eines weiteren Auftragsverarbeiters zu informieren. Die Tineon AG kann hierbei die Hinzuziehung untersagen. Zur Durchsetzung dieses Anspruchs hat sich die Tineon ein Sonderkündigungsrecht (siehe die gültigen AGB) einräumen lassen.

5.5 Datenschutzrisiken für die betroffene Person

Die DSGVO fordert, dass der Verantwortliche (Tineon AG) unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzt. Für alle Verfahren ist daher eine Risikobewertung als Produkt aus Eintrittswahrscheinlichkeit und Schwere des Schadens für den Betroffenen zu erstellen. Hierbei kann eine Zusammenfassung der einzelnen Prozesse in Kategorien erfolgen.

Verbleibt ein hohes Risiko trotz Nachbesserung der technisch-organisatorischen Maßnahmen, so ist eine Datenschutz-Folgenabschätzung durchzuführen. Um diese Notwendigkeit beurteilen zu können, gilt es zunächst die Schwere des Schadens und die Eintrittswahrscheinlichkeit einzuschätzen und anschließend im Rahmen einer sog. Schwellwertanalyse zu entscheiden, ob eine Datenschutz-Folgenabschätzung erforderlich ist. Nach Auffassung des Bayerischen Landesamtes für Datenschutzaufsicht ist eine solche Datenschutzfolgeabschätzung im Verein in der Regel nicht erforderlich, da ein erhöhtes Risiko bei der Datenverarbeitung nicht anzunehmen ist.

5.6 Maßnahmen zur Gewährleistung sicherer Datenverarbeitung

Beim Umgang mit personenbezogenen Daten sind diese durch technisch-organisatorische Maßnahmen (sog. TOM, siehe auch Anlage 2) angemessen zu schützen (Art. 32 DSGVO). Dabei ist jede Art der Verarbeitung personenbezogener Daten zu berücksichtigen. Daten in Akten sind ebenso zu schützen wie Daten auf anderen Speichermedien (z.B. Festplatte, Server, USB-Stick, Chip-Karte, CD-ROM)

Zu ergreifende Maßnahmen sind insbesondere unter Berücksichtigung des Stands der Technik, der zu erwartenden Kosten sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte der Betroffenen festzulegen Im Einzelnen ist Folgendes zu gewährleisten:

5.6.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

durch

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit;

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

5.6.2 Integrität

im Sinne von Art. 32 Abs. 1 lit. b DSGVO durch

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

5.6.3 Verfügbarkeit und Belastbarkeit

im Sinne von Art. 32 Abs. 1 lit. b DSGVO durch

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

5.6.4 Verfahren zur regelmäßigen Überprüfung

nach Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management;

- Incident-Response-Management;

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

5.7 Vernichtung, Löschung vertraulicher Unterlagen / Datenträger

In der Tineon AG fallen viele nicht mehr benötigte Unterlagen an. Dazu zählen alte Akten, überzählige Kopien von Formularen oder Briefen, erledigte und nicht aufbewahrungspflichtige Vorgänge, fehlerhafte Unterlagen, Notizen und Vermerke usw.. Soweit diese Unterlagen personenbezogene Daten enthalten, sind sie durch das Datenschutzgesetz besonders geschützt.

Die Tineon darf Mitgliederdaten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftragsgebers berichtigen, löschen oder deren verarbeitung einschränken. Soweit vom Leistungsumfang erfasst, sind Löschkonzept, Recht auf „Vergessenwerden“, Berichtigung, Datenporabilität und Auskunft nach dokumentierter Weisung des Auftragsgebers unmittelbar durch die Tineon sicherzustellen.

Nicht mehr benötigte Unterlagen der Tineon AG mit personenbezogenen Daten, die keinen Dokumentationscharakter haben, sind durch jeden Beschäftigten der Tineon AG in eigener Zuständigkeit zu sammeln und bis zur Vernichtung sicher aufzubewahren. Für die Vernichtung steht in der Tineon AG ein Aktenvernichter zur Verfügung.

Entsprechendes gilt für Datenträger (USB-Sticks, Festplatten u. ä.). Insbesondere bei Leasinggeräten (Fax, PC u. ä.) ist darauf zu achten, dass Speicher und Festplatten vor einer Rückgabe irreversibel gelöscht werden. Gegebenenfalls ist mit dieser Löschung ein externes Unternehmen zu beauftragen, da die Löschung ohne spezielle Kenntnisse häufig nicht ohne weiteres möglich ist.

5.8 Meldepflichten bei Schutzverletzungen (Datenpannen)

An die Melde- und Dokumentationspflichten werden formell und inhaltlich unterschiedlich hohe Anforderungen gestellt. Zu unterscheiden ist die Meldepflicht einer Datenschutzverletzung gegenüber der Aufsichtsbehörde von der Meldepflicht gegenüber den betroffenen Personen.

Eine Meldepflicht gegenüber der Aufsichtsbehörde entsteht mit Eintritt einer Datenschutzverletzung. Darunter wird allgemein die Vernichtung, der Verlust, die Veränderung oder die unbefugte Offenlegung personenbezogener Daten verstanden, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (z. B. die Übermittlung eines Telefaxes an eine versehentlich falsch eingegebene Rufnummer).

Eine Meldepflicht besteht jedoch nicht, sofern sie voraussichtlich nur ein geringfügiges Risiko für die Rechte des Betroffenen darstellt, also die Datenpanne voraussichtlich nicht zu physischen, materiellen oder immateriellen Schäden des Mitglieds führt.

Diese Abwägung wird jedoch stets durch den Vorstand nach Rücksprache mit dem Datenschutzbeauftragten getroffen!

Diese Meldung hat unverzüglich und möglichst binnen 72 Stunden zu erfolgen.

Über die Datenschutzverletzung sind auch die betroffenen Personen zu unterrichten, sofern die Datenschutzpanne voraussichtlich ein hohes Risiko für seine Rechte und Freiheiten zur Folge hat.

Auch diese Abwägung wird stets durch die Geschäftsleitung nach Rücksprache mit dem Datenschutzbeauftragten (und ggf. der Datenschutz-Aufsichtsbehörde, dem IT-Sicherheitsbeauf-tragten, dem Leiter EDV sowie weiteren handelnden Personen) getroffen!

Um der Aufsichtsbehörde eine Kontrolle über die Einhaltung der Meldepflicht zu ermöglichen, ist jede Verletzung des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentationspflicht besteht im Gegensatz zur Meldepflicht nicht erst dann, wenn ein Risiko für die Rechte und Freiheiten der betroffenen Person zu erwarten sind, sondern bei jeder Datenschutzverletzung. Von der Dokumentationspflicht umfasst sind die mit der Verletzung in Zusammenhang stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen. Hierüber ist eine Aktennotiz zu verfassen und der Geschäftsleitung vorzulegen.

Inhalt der Aktennotiz:

- Art, Zeitpunkt u. Ursache der Datenpanne,
- Art der Daten,
- Anzahl der Betroffenen,
- unrechtmäßiger Empfänger der Daten,
- mögliche Beeinträchtigung der Betroffenen.

Entsprechende Meldevordrucke finden sich auf dem Internetauftritt der zuständigen Datenschutz-Aufsichtsbehörde.

Einen Reaktionsplan für den Fall einer Datenpanne in der Tineon AG ist im Anhang, dort Anlage 6, beigefügt.

6 Arbeitshilfen und häufig gestellte Fragen

Die nachfolgende Darstellung gibt Arbeitshilfen zur Gewährleistung des Datenschutzes in der täglichen Arbeit im Golfclub und beantwortet häufig gestellte Fragen zum Datenschutz auf Golfanlagen.

6.1 Verhalten am Telefon

Eine wichtige Rolle in der Tineon AG spielt das datenschutzrechtlich korrekte Verhalten am Telefon. Durch die Einhaltung der folgenden Sicherheitshinweise kann dem Risiko der "unerlaubten Informationssammlung“ durch unberechtigte Dritte entgegengetreten werden.

Grundsätzlich gilt:
Auskünfte zur Erfüllung des Geschäftszweckes sind zulässig. Kennen Sie jedoch Ihren "Gegenüber" nicht, gilt es zu prüfen, ob dieser ein Recht auf die gewünschten Informationen hat und ob Sie die gewünschten Informationen preisgeben dürfen!

Zudem sollten Sie folgende Punkte beachten:
Ein Telefonat ist – rechtlich gesehen – eine "1 zu 1 Beziehung" und damit unterliegt das gesprochene Wort dem Persönlichkeitsrecht (Grundgesetz). Ohne das ausdrückliche Einverständnis des Gesprächspartners ist ein "Mithören via Lautsprecher" grundsätzlich unzulässig.
Geben Sie keine Auskünfte zu eingesetzter Soft- und Hardware oder zu eingesetzter Technik, Bürogeräten oder Firmenfahrzeugen etc. Anfragen seitens Behörden (auch Kriminalpolizei und/oder der Staatsanwaltschaft) sollten nur auf schriftlichem Wege – unter Angabe der Rechtsgrundlagen – erfolgen. Verweisen Sie Interessenten im Zweifelsfall grundsätzlich an *die Geschäftsleitung/den Vorstand*.

Besondere Vorsicht bei Auskunftsersuchen!
Telefonische Anfragen sind riskant! Die Problematik dabei ist die Schweigepflicht. Das Datengeheimnis lässt eine Weitergabe von Informationen nur an Personen zu, die zum Erhalt der Information befugt sind. Am Telefon kann aber in der Regel nicht festgestellt werden, ob die anrufende Person wirklich diejenige ist, welche sie zu sein vorgibt. Damit sind Verletzungen des Datengeheimnisses leicht möglich. Vorgespielte Identitäten wie Polizei oder Versicherungen werden gerne genutzt, um Informationen über „Kunden“ oder Mitarbeiter in die Hand zu bekommen. Die Identität einer Person, an die ich Informationen, z.B. über „Kunden“ oder aus Personendaten weitergebe, muss zweifelsfrei feststehen. Um das Risiko von Schweigepflichtverletzungen zu minimieren, sollten folgende Schritte eingehalten werden:

Kontrollfragen
Durch Rückfragen an die anrufende Person feststellen, ob sie aufgrund ihres Wissens die Person sein kann, die sie vorgibt. Zum Beispiel: Fragen zur Kunden-/Mitgliedsnummer, zum letzten Rechnungsdatum, zur Adresse des Anrufers, zum Grund des Anrufs usw.

Rückruf
Sofern jemand mit einer nachprüfbaren Identität anruft (Firma, Ehepartner/in, Behörde, Versicherung, Polizei, usw.) bestehen Sie grundsätzlich auf einem Rückruf. Lassen Sie sich die Telefonnummer geben und überprüfen Sie die Nummer (z.B. im öffentlichen Telefonbuch). Rufen Sie dann zurück. Lassen Sie sich bei Anrufern von Organisationen über deren Zentrale mit dieser Person verbinden. Damit können Sie sicher sein, dass diese Person zu dieser Organisation gehört.

Bitte merken: Auskünfte an die Polizei und an die Staatsanwaltschaft immer nur durch die Geschäftsleitung!

Schriftliche Anfrage
Wenn grundsätzliche Zweifel bestehen und die Angelegenheit nicht eilbedürftig ist, bitten Sie um eine schriftliche Anfrage. Ggf. kann auch das Fax an dieser Stelle (bei Dringlichkeit) verwendet werden. Schriftliche Anfragen per E-Mail sind mit Vorsicht zu behandeln.

6.2 Datenübermittlung an Dritte

Es gehört zum operativen Tagesgeschäft der Tineon AG, dass im Rahmen der Kommunikation, z.B. mit unseren Geschäftspartnern, Auskünfte erbeten und auch erteilt werden. Nicht immer ist einfach zu beurteilen, ob eine Auskunftserteilung oder Datenübermittlung auch erfolgen darf. Bitte beachten Sie folgende Grundregeln:

- Auskunftsersuchen "Betroffener" sind entsprechend der im Anhang zu diesem Handbuch unter der beigefügten Arbeitsanweisung „Umgang mit Auskunftsersuchen“ zu bearbeiten.
- Bei Auskunftsersuchen durch einen Geschäftspartner (Kunde, Lieferant, Dienstleister, Subunternehmer, etc.) entscheiden Sie im Rahmen Ihrer Zuständigkeit, ob die um Auskunft ersuchende Stelle die gewünschte Auskunft erhält oder nicht. Im Zweifelsfall wenden Sie sich an *die Geschäftsleitung/den Vorstand*.

6.3 Umgang mit Besuchern

Sollten Sie Gäste allein in Räumlichkeiten der Tineon AG antreffen, so sprechen Sie diese bitte höflich an und fragen Sie nach dem Grund des Aufenthaltes und dem evtl. Gastgeber in unserem Haus.

Lassen Sie Servicetechniker oder sonstige "Gäste" in Ihrem Büro oder in anderen Räumlichkeiten niemals unbeaufsichtigt. Sollten Sie von einem "Service" (z.B. EDV) nichts wissen, kontaktieren Sie bitte umgehend den Vorstand.

Lassen Sie sich nicht durch evtl. "amtliche Dienstausweise" täuschen. Bitte fragen Sie auch in diesen Fällen unbedingt bei dem Vorstand nach.

6.4 Öffnen von Briefen u. ä.

Alle Briefe und Postsendungen, die an die Tineon adressiert sind, können ohne weiteres von der Poststelle oder Verwaltung geöffnet werden. Wenn jedoch die Ergänzung „Persönlich“ oder „Vertraulich“ mit der Angabe einer bestimmten Person erfolgt, ist sicher zu stellen, dass nur der namentlich genannte Empfänger den Brief öffnet.

Das Landesarbeitsgericht Hamm hat mit Urteil vom 19.02.2003 (Az. 14 Sa 1972/02) geurteilt, wie mit Posteingängen zu verfahren ist. Soweit die Adresse keinen Vermerk „Persönlich“ oder „Vertraulich“ enthält, darf auch an Mitarbeiter adressierte Post geöffnet werden. Diese übliche Gepflogenheit in Behörden und Betrieben, die dazu dient, eingehende Post mit einem Eingangsstempel zu versehen, können Mitarbeiter nicht über den Erlass einer einstweiligen Verfügung verbieten lassen und auch nicht mit der schlagwortartigen Begründung der Verletzung ihrer Persönlichkeitsrechte.

Aus diesem Urteil ergibt sich folgende Konsequenz: Wenn eine im Betrieb eingehende Postsendung als Empfänger sowohl den Betrieb als auch einen bestimmten Mitarbeiter ausweist, ist auf besondere Vertraulichkeitsvermerke zu achten. Fehlen solche, darf die Post geöffnet werden. Ist der Brief als „Vertraulich“ oder „Persönlich“ gekennzeichnet, wäre eine Öffnung der Post ein Verstoß gegen das Briefgeheimnis mit der Folge, dass sogar Strafbarkeit (§ 202 StGB) gegeben sein kann.

6.5 Informationspflichten bei Datenerhebung

Grundsätzlich ist der von einer Datenerhebung Betroffene **bei, d. h. im Zeitpunkt** der Datenerhebung auf Art und Zweck der Datenverarbeitung hinzuweisen und umfassend über die Zwecke zu denen die Daten erhoben werden sowie seine Rechte zu informieren (Art 13 DSGVO). Wenn bereits personenbezogene Daten ohne die Kenntnis der Betroffenen gespeichert sind, müssen die Informationspflichten nach Art. 14 DSGVO **nach** der Datenerhebung, d. h. nachträglich erfüllt werden.

Diese Informationspflichten sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung zu stellen. Die Übermittlung der Informationen kann schriftlich oder in anderer Form; gegebenenfalls auch elektronisch erfolgen. Erfassung von Interessentendaten zur Ansprache auf PE-Angebote u. ä.

6.5.1 Allgemeines

Zu beachten ist der Grundsatz der Datensparsamkeit: D. h. es dürfen nur personenbezogene Daten erhoben und verarbeitet werden, die zur Erfüllung der konkreten Aufgabe erforderlich sind. Sofern eine Ansprache aus Kostengründen nachvollziehbar ausschließlich per E-Mail erfolgen soll, besteht grundsätzlich kein Bedürfnis zur Abfrage der postalischen Anschrift, es sei denn, diese ist aus anderen Gründen (z. B: zur eindeutigen Identifizierung) erforderlich.

6.5.2 Regelmäßig Einwilligung erforderlich

Die Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage in Form eines Erlaubnistatbestandes.

6.5.3 Anforderungen an die Einwilligung

Der Gesetzgeber verlangt zwar nicht mehr, dass die Einwilligung schriftlich erfolgt (inklusive Datum und Unterschrift), dennoch ist es anzuraten Einwilligungen immer schriftlich einzuholen, damit der Verpflichtung zum Nachweis nachgekommen werden kann.

Die Einwilligung ist so zu formulieren, dass klar ist, wer welche Daten zu welchem Zweck verwenden möchte, das heißt, die einwilligende Person muss konkret erkennen können, wem gegenüber in die Nutzung welcher Daten zu welchen Zwecken eingewilligt wird.

Wirksamkeitsvoraussetzung der Einwilligungserklärung ist zudem deren freiwillige Abgabe. Wichtig ist der Hinweis darauf, wem gegenüber die Einwilligungserklärung auf welche Art und Weise, widerrufen werden kann.

Eine Kopplung der Einwilligungserklärung an eine andere Leistung, z.B. die Teilnahme an einem Gewinnspiel, darf nicht erfolgen. Außerdem ist von der Ergänzung der Einwilligungserklärung um weitere Erklärungen oder Hinweise abzuraten.

6.5.4 Das Double-Opt-In-Verfahren bei der Nutzung vom E-Mail-Adressen

Das Risiko der Angabe und Nutzung einer falschen E-Mail-Adresse trägt der Datenverarbeiter, d. h. die Tineon AG. Um – soweit möglich - sicherzustellen, dass der Inhaber der angegebenen E-Mail-Adresse auch tatsächlich der Einwilligende ist, muss das Einverständnis in die Nutzung der E-Mail-Adresse nochmals durch den Inhaber der E-Mail-Adresse per E-Mail bestätigt werden. Dieses Vorgehen wird als sogenanntes „Double-Opt-In Verfahren“ bezeichnet.

Erst nach Eingang dieser Bestätigung, die beispielsweise durch das Klicken auf einen voreingestellten Link oder aber auch einfach durch den Rückversand einer E-Mail erfolgen kann, ist die Nutzung der E-Mail-Adresse datenschutzrechtlich zulässig.

6.5.5 Verfallfrist von Einwilligungen

Vorsicht ist geboten, wenn E-Mail-Adressen über einen längeren Zeitraum ungenutzt bleiben. Die Rechtsprechung ist hinsichtlich einer Verwendungsdauer zwar uneinheitlich, eindeutige Tendenz ist aber: Einwilligungen sind nicht unbegrenzt gültig!

Bisher sind – soweit ersichtlich – vier relevante Entscheidungen zur Gültigkeit von Einwilligungen in die Zusendung von Werbung ergangen: Das Landgericht Hamburg (Urteil vom 17.02.2004, Az.: 312 O 645/02) hat 2004 entschieden, dass eine vor zehn Jahren erhobene, zwischenzeitlich nicht genutzte Einwilligungserklärung ihre Gültigkeit verliert. Ebenfalls im Jahre 2004 hat das Landgericht Berlin (Urteil vom 02.07.2004, Az.: 15 O 653/03) entschieden, dass die Gültigkeit der Einwilligung bei Inaktivität über einen Zeitraum von zwei Jahren nicht hinausgeht. Bei Werbung per Telefax definierte das Oberlandesgericht Stuttgart sogar eine Maximalverwendungsfrist von vier Wochen. Entsprechend dem Urteil vom 08.04.2010 des Landgerichts München I (Az. 17 HK O 138/10) stuften die Richter die Versendung einer Werbeemail nach 17 Monaten als unzulässig ein.

Vor dem Hintergrund dieser uneinheitlichen Rechtsprechung besteht erhebliche Unsicherheit im Hinblick auf die Länge der Verfallfrist. In der praktischen Konsequenz sollten Sie daher vor jeder Werbung per E-Mail zumindest prüfen, wann zuletzt eine entsprechende Werbung versandt wurde.

6.5.6 Aufbewahrung von Einwilligungen

Im Zweifel muss die Tineon AG nachweisen können, dass eine Person eine Einwilligung in die Nutzung der personenbezogenen Daten auch tatsächlich erteilt hat. Bitte bewahren Sie deshalb die abgegebenen Einwilligungserklärungen auf und zwar jedenfalls so lange, bis die Daten nicht mehr genutzt werden!

Unabhängig davon sollten die Tineon AG außerdem in der Lage sein, jedem, dessen Daten Sie speichern, Auskunft über die Verwendung und Herkunft seiner Daten geben zu können. Schon deshalb sollte jede Verwendung und Herkunft der personenbezogenen Daten dokumentiert sein.

6.6 Arbeitnehmerdatenschutz

Auch in Bezug auf die personenbezogenen Daten von Arbeitnehmern der Tineon AG sind die Regelungen des Datenschutzes zu beachten.

Beispielhaft wird an dieser Stelle darauf hingewiesen, dass Personalakten der Mitarbeiter verschlossen aufzubewahren sind, so dass ein Zugriff unbefugter Personen ausgeschlossen ist. Im Übrigen sind auch im Personalwesen personenbezogene Daten zu löschen, sobald keine Notwendigkeit zur weiteren Aufbewahrung gegeben ist. Dies gilt etwa für Arbeitsunfähigkeitsbescheinigungen, die in der Regel nach fünf Jahren zu vernichten sind.

Für die Nutzung von Bildern der Mitarbeiter auf der Unternehmenshomepage muss eine eigenständige Einwilligung eingeholt werden.

Denken Sie bitte auch an eine regelmäßig stattfindende datenschutzrechtliche Schulung Ihrer Mitarbeiter, da die Einhaltung der gesetzlichen Vorgaben andernfalls nicht gewährleistet werden kann.

6.7 Rechte der „betroffenen Person“

Betroffene Personen von Vereinen, also Personen (Beschäftigte, Kunden, Lieferanten, Interessenten etc.), deren Daten in YouTrack verarbeitet werden, haben eine Reihe von Rechten, die unmittelbar gegenüber der Tineon AG geltend gemacht werden können und Handlungspflichten in der Tineon AG auslösen. Im Einzelnen ist dies das Recht auf

- Information: Information über alle Angaben die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln;
- Auskunft: Vollständige Auskunftserteilung durch die verantwortliche Stelle.
- Berichtigung: Unverzügliche Korrektur falscher Daten.
- Löschung: Sofortige Löschung nicht (mehr) erforderlicher Daten. Grundlage hierfür ist grundsätzlich die Speicherfrist im Verzeichnis der Verarbeitungstätigkeiten.
- Einschränkung der Verarbeitung: Sofortige Einschränkung der Verarbeitung (Sperrung) strittiger und/oder nicht (mehr) erforderlicher Daten.
- Mitteilung: Weitergabe von Berichtigung und Löschung an weitere Empfänger.
- Widerspruch: Keine Nutzung oder Übermittlung der Daten für Zwecke der Werbung. Recht auf Widerspruch gegen eine Verarbeitung oder eine erteilte Einwilligung.
- Datenübertragbarkeit: Aushändigung oder Übermittlung von Daten in einem strukturierten, gängigen und maschinenlesbaren Format .

Über sämtliche Anfragen, die durch betroffene Personen hinsichtlich der Wahrnehmung Ihrer Rechte an die Tineon AG gestellt werden, ist unverzüglich *der Vorstand* zu informieren.

Übt eine betroffene Person ein Betroffenenrecht aus, so muss die Tineon AG die Identität der betroffenen Person feststellen. Kann die Identität der betroffenen Person nicht festgestellt werden, so muss die Ausübung eines Betroffenenrechts aus den Artikeln 15 –20 DSGVO verweigert, die anfragende Person unterrichtet und der Vorgang dokumentiert werden. Die Prüfung der Plausibilität der Identität ist hierbei ausreichend. Verwendet die betroffene Person eine Adresse, mit der sie zuvor mit dem Verantwortlichen korrespondiert hat, darf eine Auskunft an diese Adresse versendet werden.

Die Tineon AG muss sicherstellen, dass ein Betroffenenrecht spätestens innerhalb eines Monats gewährt wird.

6.7.1 Auskunftspflichten (Art. 15 DSGVO)

Die Tineon AG muss der betroffenen Person Kopien über die folgenden personenbezogenen Daten zur Verfügung stellen, sofern sie Gegenstand der Anfrage sind (Artikel 15 Absatz 1 DSGVO):

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Golfclub oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen;
- über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Die Auskunft muss verweigert werden, wenn die Auskunft in Konflikt mit den Rechten und Freiheiten anderer Betroffener steht. Die Form der Auskunftserteilung richtet sich nach der Form der Anfrage. Wird die Auskunft elektronisch beantragt (z. B. per E-Mail), erfolgt die Bereitstellung in einem gängigen elektronischen Format (z. B. als PDF durch Übersendung oder Bereitstellung zum Download), sofern der Betroffene nicht ein anderes Format angibt. Wird die Anfrage in sonstiger Weise gestellt, erfolgt die Übersendung oder Bereitstellung einer lesbaren Kopie auf Papier.

6.7.1.1 Allgemeine Voraussetzungen der Auskunft

- Eine Auskunft kann in der Regel nur zu einem Einzelfall gegeben werden.
- Die Anfrage muss einen konkreten Sachverhalt beschreiben, über den um Auskunft gebeten wird.
    - Beschreibung von Fall und Problematik,
    - konkrete Fragen, die sich deutlich auf die Fallproblematik beziehen,
    - Nennung der Dokumente bzw. Informationen, die für die Beurteilung des Falles erforderlich sind und übersandt werden sollen.
- Die Auskunft muss für die Durchführung der Aufgaben des Anfragenden tatsächlich erforderlich sein. Bitte prüfen Sie ungewöhnliche Anfragen ggf. durch Nachfragen.
- Die Auskunft muss für die Durchführung der Aufgaben des Anfragenden tatsächlich erforderlich sein. Bitte prüfen Sie ungewöhnliche Anfragen ggf. durch Nachfragen.
- Ein Versand von Originalunterlagen ist nicht möglich. Nur Kopien dürfen versandt/überlassen werden. Im Zweifelsfall fragen Sie bei der Geschäftsleitung nach.
- Nur der tatsächlich geforderte und für die Aufgabenerfüllung erforderliche Informationsumfang darf offenbart bzw. in Dokumenten übersandt werden. Dies kann auch bedeuten, dass in Dokumenten (wie z.B. Anschreiben, Faxschreiben, E-Mails, Zeugnisse, Rechnungen, etc.) für bestimmte Fragestellungen irrelevante Stellen vor dem Kopieren abgedeckt werden. Unzulässig ist das:
    - Übersenden von nicht angeforderten Dokumenten,
    - Übersenden von Dokumenten, die nicht zur Fragestellung gehören.
- Die Anfrage mit Namen, Datum Uhrzeit, und den gegebenen Auskünften unbedingt kurz dokumentieren.

6.7.2 Informationsrecht bei Erhebung personenbezogener Daten

Die DSGVO fordert in Art. 13 und Art. 14 eine Information der betroffenen Person, in Abhängigkeit davon, ob die Daten bei der betroffenen Person erhoben wurden oder nicht. Hierfür sind im Rahmen des Internetauftritts und bei der Erhebung von Daten in Zusammenhangmit dem Abschluss von Verträgen (einschließlich Arbeitsverträgen) umfangreiche Informationen zur Verfügung zu stellen. Im Falle einer telefonischen Vertragsanbahnung kann in der Regel auf die im Internet bereitgestellten Informationen verwiesen werden.

6.7.3 Berichtigung unrichtiger Daten

Berichtigungen unrichtiger Daten (Art. 16 DSGVO) sind vor ihrer Umsetzung zu prüfen. Die Tineon AG muss auf Anfrage des Betroffenen unrichtige personenbezogene Daten unverzüglich berichtigen und unvollständige personenbezogene Daten müssen auf Anfrage des Betroffenen vervollständigt werden.

6.7.4 Löschen/Recht auf Vergessen werden

Die Aufbewahrungsfristen richten sich nach dem Zweck der Verarbeitung. Diese können sich u. a. aus den rechtlichen Aufbewahrungspflichten, den Einwilligungen der Betroffenen sowie aus der Erforderlichkeit zur Vertragsabwicklung (Anlage 3 AGB der Tineon AG) ergeben.

Nach Ablauf der gesetzlichen Aufbewahrungspflichten bzw. der intern festgelegten Aufbewahrungspflichten sind personenbezogene Daten zu löschen (Art. 17 DSGVO). Im Rahmen der internen Organisation wird die Dokumentation der Löschung sichergestellt.

Im Verarbeitungsverzeichnis müssen, soweit möglich, die vorgesehenen Löschfristen für die verschiedenen Datenkategorien festgehalten sein (Art. 30 Abs. 1 S. 2 Buchst. f) DSGVO). Aufgrund ihrer Rechenschaftspflicht muss die Tineon AG die geeigneten technischen und organisatorischen Maßnahmen zur Einhaltung des Grundsatzes zur zeitlichen „Speicherbegrenzung“ nachweisen können (Art. 5 Abs. 2 DSGVO). Aus diesem Grund wird die Einhaltung der Löschung einmal jährlich durch die Geschäftsleitung oder eine durch die Geschäftsleitung beauftragte Person überprüft. Das Ergebnis dieser Prüfung ist zu dokumentieren.

Sofern die Löschanfrage einer betroffenen Person berechtigt ist, müssen ebenfalls alle personenbezogenen Daten des Betroffenen aus den Datenbeständen gelöscht werden. Eine Löschung darf nicht vorgenommen werden, wenn die Löschung im Konflikt mit gesetzlichen Regelungen steht (z. B. Aufbewahrung steuerrelevanter Unterlagen). Alternativ kann eine Einschränkung erfolgen.

6.7.5 Einschränkung der Datenverarbeitung

Die Tineon AG muss prüfen, ob die gesetzlichen Voraussetzungen zur Einschränkung der Verarbeitung der personenbezogenen Daten des Betroffenen vorliegen (Artikel 18 Abs. 1 DSGVO). Bei positiver Prüfung muss die Tineon AG die Verarbeitung personenbezogener Daten der betroffenen Person aussetzen.

6.7.6 Datenübertragung

Die Tineon AG muss auf Antrag der betroffenen Person die sie betreffenden personenbezogenen Daten, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen (Art. 20 DSGVO). Verlangt die betroffene Person eine Übermittlung ihrer Daten an einen Dritten, so muss die Tineon AG dem nachkommen.

6.7.7 Widerspruchsrecht

Die Tineon AG muss die Verarbeitung der personenbezogenen Daten auf den Widerspruch des Betroffenen hin beenden, es sei denn, es gibt eine weitere Rechtsgrundlage für diese Verarbeitung z. B. gesetzliche Aufbewahrungspflichten(Art. 21 DSGVO).

7 Der Internetauftritt der Tineon AG

7.1.1 Veröffentlichung von Fotos im Internet (Homepage, social media u. a.)

Die Frage der Zulässigkeit einer Veröffentlichung von Fotoaufnahmen im Internet berührt verschiedene Rechtsgebiete: Betroffen sind das Urheberrecht des Fotografen sowie das allgemeine Persönlichkeitsrecht des Abgebildeten. Zugleich kann eine Bildaufnahme personenbezogene Informationen ent-

halten (etwa dann, wenn eine auf dem Bild erkennbare Person mit Bezug zu einem bestimmten Wettspiel identifizierbar ist) und damit in den Anwendungsbereich des Datenschutzrechts fallen.

Als Ausfluss seines Urheberrechts entscheidet zunächst der Fotograf, in welcher Art und Weise die von ihm gefertigte Aufnahme verwertet werden darf. Es bedarf hier als des Einverständnisses mit einer Veröffentlichung etwa auf der Unternehmens-Homepage.
In Abhängigkeit von der jeweiligen Bildaufnahme kann daneben die Einwilligung des Abgebildeten erforderlich sein (sog. Recht am eigenen Bild). § 22 Satz 1 des Kunsturhebergesetzes (KunstUhrG) regelt insofern den Grundsatz, dass Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen.

7.1.2 Die Datenschutzerklärung auf der Unternehmenshomepage

Augenmerk verdient unbedingt auch der Auftritt der Tineon AG sowie seiner Softwareangebote für Verein (S-Verein) im Internet, da bspw. beim Besuch der Homepage durchaus personenbezogene Daten verarbeitet werden. Bereits die IP-Adressen der Besucher der Clubhomepage gelten als personenbezogene Daten, deren Verarbeitung nach allgemein geltenden datenschutzrechtlichen Standards zu genügen hat, d. h. grundsätzlich einer Erlaubnis bedarf. Sofern Cookies genutzt werden, ist durchaus umstritten, ob eine Einwilligung in die Verwendung von Cookies bereits bei Aufruf der Webseite zu erfolgen hat. Ganz unabhängig davon gelten auch in diesem Bereich die oben beschriebenen Informationspflichten gegenüber den Nutzern, d. h. es ist bspw. über die Rechts der Betroffenen aufzuklären (siehe hierzu oben Ziff. 6.5).

8 Fernwartung der IT-Systeme

Eine Fernwartung erfolgt grundsätzlich aufgrund einer mit dem jeweiligen Dienstleister vertraglich geregelten Datenverarbeitung im Auftrag. Hierin wird der Dienstleister unter anderem verpflichtet, die von ihm mit der Fernwartung betrauten Mitarbeiter zur Einhaltung von Datenschutz und Geheimhaltung zu verpflichten und schriftlich über die Konsequenzen eines Daten- und Geheimnismissbrauchs zu belehren.

Das Unternehmen, welches die Fernwartung durchführt ist verpflichtet, personenbezogene Daten, die es bei der Wartungsmaßnahme erhalten hat, unverzüglich zu löschen, sobald diese Daten für die Wartungsmaßnahme nicht mehr benötigt werden. Ausgenommen ist die Protokollierung der Wartungsmaßnahme selbst. Das fernwartende Unternehmen bekommt zudem nur die Zugriffsrechte eingeräumt, die zur Durchführung der Fernwartungsarbeiten unerlässlich sind. Der die Fernwartung überwachende Mitarbeiter ist verpflichtet, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen und ggf. jederzeit abbrechen zu können. Zur Sicherung von Vertraulichkeit, Integrität und Authentizität der übertragenen Bildschirminhalte (Daten) darf die Datenübertragung mit dem Fernwartungsrechner grundsätzlich nur verschlüsselt erfolgen. Nach Abschluss der Fernwartungsarbeiten ist die Verbindung unverzüglich zu beenden.

- Ende des Datenschutzhandbuchs V1 -