Round Tables IG Sport Luzern
–
Datenschutz & -sicherheit

Luzern & Oberkirch, 3. & 4. September 2018

Praktische Beispiele

Gruppe 1	Gruppe 2
• OK regionaler Sportanlass. • Schwierigkeiten, weil zu wenig Sponsoren.	• Neuer Sekretär Veloclub. • Mitgliederliste völlig veraltet.
• Krankenkasse meldet sich beim OK. • Sie sponsort den gesamten Anlass. • Im Gegenzug will sie per Email Vorname, Name, Klassierung, Adresse & Geburtsdatum sämtlicher Teilnehmer erhalten, um diesen per Post personalisierte Angebote zukommen zu lassen.	• Der Sekretär entschliesst sich, eine neue Liste in einer *Cloud* zu erstellen. • Er kontaktiert sämtliche ihm bekannten Mitglieder per Email und bittet sie um Vorname, Name, Adresse, Geburtsdatum, Zivilstand, Konfession, Arbeitgeber, Parteimitgliedschaften & Mitgliedschaften in anderen Vereinen oder Verbänden.

- Was halten Sie von diesen Vorgehensweisen, insb. mit Bezug auf Datenschutz & -sicherheit?
- Was empfehlen Sie dem OK, resp. dem Sekretär?

Stefan Pfister

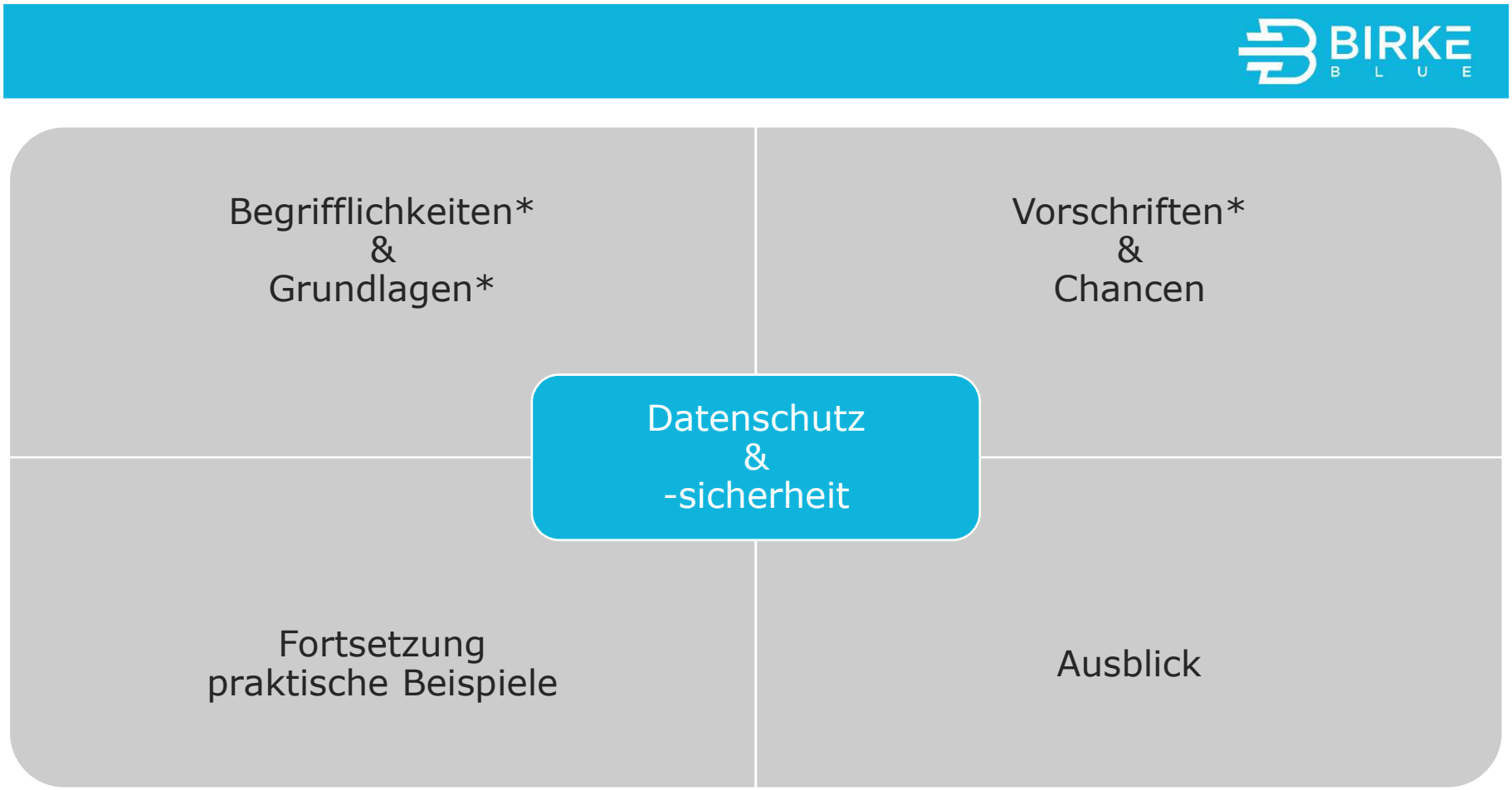
- Rechtsanwalt
- Mitgründer und Partner von birkeblue.ch AG
- Sportwesen
- IT-, Vertrags- & Arbeitsrecht
- Mergers & Acquisitions
- Compliance & Datenschutz

Marco Steiner

- Dr. iur.
- Mitgründer und Partner von birkeblue.ch AG
- Sportwesen
- Allgemeines Vertrags- & Arbeitsrecht
- Personalführung & Qualitätssicherung
- Behördenkontakte

Lebensläufe

- www.birkeblue.ch



*stark vereinfacht, kein Anspruch auf Vollständigkeit

Begrifflichkeiten*

Datenschutz

Datenschutz regelt den Umgang mit Personendaten.

Personendaten

Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, etwa Name, Adresse, Email, Foto, Online-Daten, Kontodaten, Autonummer.

Besonders schützenswerte Personendaten

Bspw. Daten über religiöse oder politische Ansichten, Gesundheit, Ethnie, Sozialhilfe, strafrechtliche Sanktionen.

Datensicherheit

Eigenschaften von IT-Systemen, welche die Vertraulichkeit, Verfügbarkeit und Integrität von Daten sicherstellen.

Gesellschaftliche Grundlagen

Daten sind ein wertvolles Gut, insb. Personendaten.

Diese Aussage kann man sowohl materiell, als auch ideell verstehen.

Mit Hilfe möglichst vieler möglichst detaillierter Daten können bspw. Unternehmen das Konsumverhalten einzelner Personen genau nachzeichnen, um etwa ihre Werbestrategien gezielt auszugestalten und umzusetzen («Profiling»).

Das Ganze oft unbemerkt.

Es geht jedoch in einer demokratischen und rechtsstaatlichen Gesellschaft nicht an, dass der Mensch nicht über eine minimale Kontrolle über die Verwendung «seiner» Daten verfügt.

Umgesetzt wird dieser Grundsatz durch das informationelle Selbstbestimmungsrecht.

Erstes Ziel des Datenschutzes ist es, das informationelle Selbstbestimmungsrecht zu verteidigen.

Diese Aufgabe ist nicht immer einfach, weil es legitime Interessen geben kann, dieses Recht einzuschränken.

Rechtliche Grundlagen*

Art. 13 der Bundesverfassung legt fest: Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Um diesen Schutz gesetzlich zu verankern, wurde das DSG verabschiedet, das seit dem 1. Juli 1993 in Kraft ist (gilt für private Personen und Bundesorgane).

Für kantonale Behörden gelten die jeweiligen, kantonalen Datenschutzgesetze.

Es existieren zahlreiche weitere Bestimmungen zum Schutz der Persönlichkeit.

In Art. 28-28l ZGB bspw. wird festgelegt, wie im Fall von Persönlichkeitsverletzungen vorzugehen ist.

Die EU-DSGVO gilt unmittelbar in jedem Mitgliedstaat der EU.

Ebenso bei Verarbeitung von Daten von Personen aus der EU durch einen Dritten ausserhalb der EU (etwa Schweiz). Falls ja: Datenschutzvertreter in der EU erforderlich.

Vorschriften* & Chancen

Grundsätze der Datenbearbeitung

Rechtmässigkeit
Transparenz
Zweckbindung
Verhältnismässigkeit
Datensicherheit

Anwendungsbereich

Art. 2 DSG

Art. 2 & 3 EU-DSGVO

Zuwiderhandlungen

Art. 15 & 34 DSG

Art. 77 - 84 EU-DSGVO

Chancen

Ein datenschutz-konformer Webauftritt ist die erste extern wahrnehmbare Visitenkarte einer Organisation.

Datenschutzrechtliche Konformität bedeutet i.d.R. interne, sauber geführte Systeme, Abläufe & Prozesse.

Ausblick

Das zu revidierende DSG wird voraussichtlich ab Mitte 2019 in Kraft treten und die (strengere) EU-DSGVO zu guten Teilen übernehmen, mit analogen Sanktionen.

Es wird für Schweizer Akteure kein Weg an einer Diskussion über die Umsetzung des revidierten DSG vorbeiführen.

Insbesondere wird man sich nicht (mehr) darauf verlassen können, keine Priorität für «die Datenschützer» zu haben.

Im Auftrag des Gesundheitsdepartements des Kantons führt die IG Sport Luzern die Qualitätskontrolle bei den Luzerner Vereinen & Verbänden mittels Zertifizierung durch.

Die Zertifizierung soll mittelfristig durch die Säule «Datenschutz und -sicherheit» ergänzt werden.

In Zusammenarbeit mit birkeblue.ch bietet die IG Sport Luzern ihren Vereinen & Verbänden bereits heute an, in vereinfachter Form die Konformität des Datenhandlings in ihrem Webauftritt einem Fitness-Check zu unterziehen.

Rechtmässigkeit

- Der Grundsatz der Rechtmässigkeit verlangt,
  - dass jede Bearbeitung von Personendaten die durch eine rechtliche Grundlage gestattet ist,
  - eine ausdrückliche, rechtsgültige Einwilligung des Betroffenen oder
  - überwiegende Interessen vorliegen.

Transparenz

- Der Grundsatz der Transparenz (auch: von Treu & Glaube) verlangt unter anderem, dass die betroffene Person weiss oder erkennen kann, welche Daten beschafft werden & zu welchem Zweck.

- Das heimliche Beschaffen und Bearbeiten von Daten verstösst gegen diesen Grundsatz.

Zweckbindung

- Der Grundsatz der Zweckbindung schreibt vor, dass Daten nur zu dem Zweck bearbeitet werden dürfen,
  - der bei deren Beschaffung angegeben wird,
  - gesetzlich vorgesehen
  - oder aus den Umständen ersichtlich ist.

- Der Veranstalter eines Sportanlasses kann die erhaltenen Daten (etwa Name, Adresse, Jahrgang, Verein) zur Erstellung der Rangliste verwenden.
  - Es ist jedoch nicht erlaubt, die erhaltenen Daten ohne Zustimmung der Athleten einer Versicherung weiterzugeben, damit diese den Teilnehmern massgeschneiderte & günstige Angebote zukommen lassen kann.

Verhältnismässigkeit

- Der Grundsatz der Verhältnismässigkeit sieht vor, dass nur Daten beschafft & bearbeitet werden dürfen, die geeignet und objektiv gesehen erforderlich sind, um ein (legitimes) Ziel zu erreichen.
- Bei der Bearbeitung der Daten müssen das verfolgte Ziel & die verwendeten Mittel zudem in einem vernünftigen Verhältnis zueinander stehen & die Rechte der betroffenen Personen möglichst gewahrt werden.

- Ein Veloclub darf von seinen Mitgliedern nur Personendaten erheben, die einen direkten Zusammenhang mit dem Eintritt & der Vereinstätigkeit haben & deren Beschaffung die Privatsphäre der betroffenen Person nicht unnötig oder übermässig beeinträchtigt,
  - d.h., i.d.R. keine Erhebung von Zivilstand, Konfession, etc.

Quelle: www.edoeb.admin.ch

Datensicherheit

- Personendaten müssen in Übereinstimmung mit dem Grundsatz der Datensicherheit mittels geeigneter organisatorischer & technischer Massnahmen (TOM's) vor jeder rechtswidrigen Bearbeitung geschützt werden.
  - Ziel der TOM's: Vertraulichkeit, Integrität und Verfügbarkeit der Daten.

- Leistungstest von Sportlern sind nicht «ungeschützt» und/oder für alle Mitarbeiter des Team-Sekretariats zugänglich auf dem Server oder gar in einer ausländischen Cloud zu speichern.

https://www.igsportluzern.ch/

Verschlüsselung?
Datenschutzerklärung / AGB?
Impressum?
Social Media Plugins?
Analyse-Tools?
Kontaktformular?
Newsletter?

Fortsetzung praktische Beispiele

Besprechung im Plenum

Fortsetzung Ausblick

Es gelten für die Personendatenbearbeitung weiterhin die bisherigen Prinzipien, so insb. bezüglich Rechtmässigkeit, Transparenz, Zweckbindung & Verhältnismässigkeit.

Daran hat sich auch mit Inkrafttreten der EU-DSGVO nichts geändert.

Allerdings wird der Umsetzung dieser Prinzipien mittlerweile erhöhtes Gewicht beigemessen.

Dies wird sich mit Inkrafttreten des revidierten DSG auch für CH-Unternehmen, Verbände etc. verstärken.

Die Übersicht der wichtigsten Prinzipien kann helfen, die erforderlichen Schritte bis zur Sicherstellung der Konformität der diversen Prozesse & Systeme mit datenschutzrechtlichen Vorgaben in ihren Gesamtkontext zu stellen.

Synthese Grundsätze*

Rechtfertigung	Jede Datenbearbeitung erfordert die ausdrückliche, aktive Einwilligung der Betroffenen oder einen anderen Rechtfertigungsgrund.
Information	Betroffene müssen umfassend informiert werden, direkt oder über eine Publikation (z.B. Webseite).
Rechte	Betroffene haben umfangreiche Rechte, so namentlich auf Auskunft, Rückgabe übergebener Daten, Korrektur, Löschung und Widerspruch gegen bestimme Bearbeitungen (z.B. Direktmarketing).
Pflichten	Der für eine Datenbearbeitung Verantwortliche muss belegen können, dass er den Datenschutz einhält, dies inkl. umfangreicher Dokumentationspflichten.
Beauftragter / Koordinator	Einen betrieblichen Datenschutzbeauftragten müssen nur "Risiko-Unternehmen" ernennen, viele werden jedoch faktisch nicht ohne einen solchen auskommen («Koordinator»).

*stark vereinfacht, kein Anspruch auf Vollständigkeit

Synthese Grundsätze (Fortsetzung)*

Massnahmen	Personendaten müssen durch angemessene technische und organisatorische Massnahmen gesichert sein.
Meldung	Datenschutzverstösse mit möglichen Folgen für Betroffene müssen der Behörde innert 72 Stunden und, bei drohenden schweren Folgen, zusätzlich den Betroffenen gemeldet werden.
Folgenabschätzung	Heikle Projekte erfordern vorab grundsätzlich eine Datenschutz-Folgenabschätzung inkl. Beizug des Datenschutzbeauftragten, ggf. auch der nationalen Datenschutzbehörde.
Verträge	Verträge mit beauftragten Datenbearbeitern (z.B. IT-Outsourcing) müssen bestimmten Anforderungen genügen (z.B. Vetorecht des Auftraggebers).
Transfers	Datentransfers in Länder ohne anerkannt angemessenen Datenschutz sind nur unter bestimmten Bedingungen zulässig.

Angebot Fitness-Check Datenschutz

<u>birkeblue.ch</u>

Geschätzter Aufwand
pro Verein / Verband
& Website:
zwei Stunden.

<u>Umfang Fitness-Check</u>

Verschlüsselung
Datenschutzerklärung / AGB
Impressum
Social Media Plugins
Analyse-Tools
Kontaktformular
Newsletter

<u>Kosten</u>

Verrechnung pro Verein / Verband.
Die Verrechnung erfolgt durch birkeblue.ch direkt an den jeweiligen Verein / Verband.

<u>Zeitplan</u>

Eingang der Anmeldungen bis am 12. Oktober 2018.
Weiterleitung der Anmeldungen durch die IG Sport Luzern an birkeblue.ch bis am 19. Oktober 2018.
Abschluss der Arbeiten bis am 30. November 2018.

Anmeldung

IG Sport Luzern

Anmeldung per Email bis am 12. Oktober 2018
beim Geschäftsführer René Baumann:
info@igsportluzern.ch.

Vereine & Verbände

Name des Vereins / Verbands
Name & Email zuständige Person

Informationen

Adresse Website
(Adresse Webshop)

Wir stellen höchste Ansprüche an unsere Integrität

Der langfristige Erfolg des Kunden ist entscheidend für uns

Wir entwickeln fortlaufend wegweisende Lösungen

birkeblue.ch AG

Schifflände 5
4800 Zofingen

062 552 05 77

contact@birkeblue.ch

www.birkeblue.ch

Stefan Pfister
stefan.pfister@birkeblue.ch

Marco Steiner
marco.steiner@birkeblue.ch