

Datenlecks bei Schwimmbädern – undichte Stellen im Bereich Datenschutz erkennen

Datenlecks, Hackerangriffe, Datenschutz. Diese Themen sind allgegenwärtig. Der Schutz der Persönlichkeit der Badegäste wird daher immer wichtiger. Dieser Schutz soll durch die Datenschutzgesetze, welche die Personendaten der Badegäste schützen, gesichert werden. Personendaten sind Daten, mit der eine Person identifiziert werden kann (Beispiele: Name, Vorname, Bild). Was ist beim Datenschutz im Besonderen zu beachten?

TEXT: MANUELA ROGGER ■ FOTO: ZVG

Datenlecks sind Vorfälle, bei denen Personendaten eines Betriebs ungeschützt sind und von Drittpersonen eingesehen und gebraucht werden können. Datenlecks entstehen meist, wenn in den technischen Anwendungen Probleme bestehen. Dass die technischen Anwendungen sicher sind, ist Sache einer genügenden Datensicherheit (IT-Sicherheit). Es ist daher wichtig, dass die IT-Systeme dem aktuellen Stand der Technik entsprechen und regelmässig aktualisiert und überprüft werden. Damit kann ein Datenleck verhindert werden.

Sobald ein Datenleck festgestellt wurde, ist Folgendes vorzunehmen:

- **Fehlerbehebung:** Das technische Problem hinter dem Datenleck muss möglichst schnell behoben werden.
- **Meldung an Behörde:** Gleichzeitig muss sich der Betrieb überlegen, ob er eine Meldung des Datenlecks an die Behörden (behördliche Datenschutzbeauftragte) machen muss. Verletzungen der Datensicherheit müssen nur gemeldet werden, wenn deswegen ein hohes Risiko für negative Folgen für die betroffene Person besteht. Im Zweifelsfall ist eine solche Meldung an die Behörden vorzunehmen. Im Anwendungsbereich des Bundesgesetzes über den Datenschutz ist diese Meldung beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vorzunehmen unter dem Link: <https://databreach.edoeb.admin.ch/report>.
- **Meldung an betroffene Personen:** Ausserdem muss der Betrieb prüfen, ob er eine Meldung an die betroffenen Personen, d. h. an die Badegäste selbst, machen muss.

Die obigen Punkte sind so schnell wie möglich vorzunehmen, und ein Vorfall ist mit oberster Priorität zu behandeln.

Wie kann die Datensicherheit verbessert werden?

Datenschutz und Datensicherheit (IT-Sicherheit) hängen eng zusammen. Um Datenschutzverletzungen zu vermeiden, ist die IT-Sicherheit der Computersysteme zu gewährleisten. Nachfolgend sind exemplarisch einige Massnahmen aufgelistet, die im Bereich der Datensicherheit getroffen werden können:

Manuela Rogger ist Rechtsanwältin bei der Tschümperlin Lötcher Schwarz AG in Luzern und Kennerin der Bäderbranche.



- **Regelungen mit IT-Dienstleistern überprüfen:** Was ist mit den diversen IT-Dienstleistern vereinbart? Wie gewährleisten die IT-Dienstleister die IT-Sicherheit? Was ist im Bereich des Datenschutzes mit den IT-Dienstleistern geregelt?
- **Überprüfen der IT-Dienstleister:** Ergreifen die IT-Dienstleister die Massnahmen im Bereich der IT-Sicherheit?
- **Organisatorische Massnahmen treffen, wie beispielsweise:**
 - Erhöhter technischer Schutz von Kassensystemen und insbesondere doppelter Passwortschutz beim Zugriff auf Kassensysteme.
 - Bildschirme an Kassen so aufstellen, dass Badegäste keine Sicht auf den Bildschirm haben.
 - Bei Drehkreuzkontrollen keine Personendaten auf dem Display anzeigen. Ansonsten könnte die dahinter eintretende Person alle Personendaten der Person davor einsehen.
 - Keine WLAN mit universellem Passwort betreiben.
 - Vergangene Videoaufzeichnungen der Schwimmbäder nur zu zweit und nach einem vorgesehenen Ablauf sichten (nicht notwendig bei Echtzeitüberwachungen).
 - Individuelle Konten bei den IT-Systemen für die Mitarbeitenden erstellen und sinnvolle Berechtigungen erteilen.

Wie können Mitarbeitende helfen, Datenlecks zu verhindern?

Nicht nur Hackerangriffe führen zu Datenlecks, sondern auch ein unsorgfältiger Umgang mit Personendaten durch Mitarbeitende. Es ist deshalb wichtig, die Mitarbeitenden regelmässig im Thema Datenschutz und IT-Sicherheit zu schulen. Im Übrigen sollten die Mitarbeitenden bereits bei der Anstellung informiert werden, welche Punkte sie in ihrer täglichen Arbeit in Sachen Datenschutz beachten müssen. Natürlich muss der Betrieb den eigenen Mitarbeitenden auch mitteilen, wie mit ihren eigenen Personendaten, d. h. den Personendaten der Mitarbeitenden, umgegangen wird.

Konkret können Mitarbeitende beispielsweise mit den folgenden Massnahmen helfen, Datenlecks und Datenschutzverletzungen zu verhindern:

- **Auskunftserteilung an Drittpersonen:** Es werden keine Auskünfte über eine bestimmte Person an eine Drittperson erteilt. Das heisst, eine anfragende Person darf nur über sich selbst Auskunft erhalten. Auch an Freunde oder Verwandte sollte demnach keine Auskunft über eine Person erteilt werden.
- **Auskunft über sich selbst:** Nur die anfragende Person darf über sich selbst Auskunft erhalten. Wie oben beschrieben, werden keine Auskünfte über eine Person an eine Drittperson gegeben. Wenn jedoch die anfragende Person über sich selbst Auskunft erhalten möchte, dann hat sie Anrecht auf eine umfassende Auskunft. Das heisst, sie darf alle Bearbeitungen erfahren, die mit ihren Personendaten vorgenommen werden. Bei jeder Auskunftsanfrage sollte die Identität überprüft werden, beispielsweise mit einer ID oder einem Abo.
- **Auskunft an Behörden:** In gewissen Fällen, wie beispielsweise bei einem Strafverfahren, werden Behörden Auskunft über Personendaten verlangen und darüber eine Verfügung erlassen. Dieser Verfügung ist in der Regel nachzukommen und der Behörde Auskunft zu erteilen. Auch vor dieser Datenbekanntgabe ist jedoch eine Abklärung und eine Einschätzung zu treffen.
- **Sensibilisierung und Schulung:** Wichtig ist, dass sich Mitarbeitende bewusst sind, dass sie im Arbeitsalltag mit Personendaten zu tun haben und dass es im Umgang damit gewisse Risiken gibt. Ein Beispiel wäre, dass sich Mitarbeitende der Gefahr von Phishing-E-Mails (betrügerische E-Mails) bewusst sind und wissen, wie sie damit umgehen sollen.

Neues Datenschutzgesetz – Checkliste

Das neue Datenschutzgesetz ist am 1. September 2023 in Kraft getreten. Mit dem neuen Gesetz soll der Datenschutz gestärkt und den veränderten technologischen und gesellschaftlichen Verhältnissen besser gerecht werden.

Die **einzelne betroffene Person**, d.h. beispielsweise ein Kunde des Schwimmbads, dessen Daten bearbeitet werden, erhält mit dem neuen Datenschutzgesetz mehr Rechte. Die Kunden müssen daher beispielsweise informiert werden, welche Daten das Schwimmbad über sie bearbeitet. Dies geschieht mittels Datenschutzerklärungen. Datenschutzerklärungen werden auf der Website publiziert und auch physisch abgegeben. Ausserdem kann jede betroffene Person (z. B. die Kundin/der Kunde) Auskunft über die Bearbeitung ihrer/seiner Daten und auch die Löschung ihrer/seiner Daten verlangen.

Die **einzelnen Unternehmen** erhalten mit dem neuen Datenschutzgesetz neue Pflichten. Sie müssen beispielsweise beim Sammeln von Personendaten mehr Informationen angeben als bisher. Die Unternehmen müssen die betroffenen Personen genau informieren, für was sie welche Personendaten gebrauchen. Dies kann beispielsweise in einer Datenschutzerklärung erfolgen. Weiter haben Unternehmen mit mehr als 250 Mitarbeitenden ein Verzeichnis aller Datenbearbeitungen zu führen. Auch für Unternehmen mit weniger als 250

Für eilige Leser

Beim Datenschutz geht es um den Schutz von Daten, mit denen eine Person identifiziert werden kann (Beispiele: Name, Vorname, Bild). Im Bereich der Schwimmbäder handelt es sich beispielsweise bei den Listen von Abonentinnen und Abonenten um Personendaten.

Die Personendaten, die ein Unternehmen bearbeitet, müssen angemessen geschützt sein (Datensicherheit/IT-Sicherheit). Das heisst, es dürfen keine «Datenlecke» entstehen, bei denen unbefugte Dritte Personendaten eines Betriebs ungeschützt einsehen können. Diesbezüglich können beispielsweise die beigezogenen IT-Dienstleister und die Regelungen mit den IT-Dienstleistern in Sachen Datensicherheit und Datenschutz überprüft werden.

Weiter ist es wichtig, dass die Mitarbeitenden, die mit Personendaten zu tun haben, zum Thema Datenschutz sensibilisiert sind. Es dürfen beispielsweise keine Auskünfte über eine bestimmte Person an Drittpersonen (auch angebliche Freunde oder Verwandte) erteilt werden. Für Unternehmen gilt es sodann, Datenschutzaspekte bei sämtlichen unternehmerischen Tätigkeiten zu beachten und einen Überblick über die Bearbeitung von Personendaten zu haben.

Mitarbeitenden ist es empfehlenswert und sinnvoll, ein solches Verzeichnis zu führen, um überhaupt einen Überblick zu erlangen, wo welche Personendaten bearbeitet werden.

Wichtige Punkte, die ein Unternehmen in Sachen Datenschutz zu beachten und umzusetzen hat, sind in der folgenden **Checkliste** dargestellt:

- Überblick erhalten, wo welche Personendaten bearbeitet werden.
- Definieren, wer innerhalb des Unternehmens für den Datenschutz verantwortlich ist.
- Datenschutzerklärungen erstellen und überarbeiten.
- Risiken bei einzelnen Datenbearbeitungen evaluieren.
- Angemessene Datensicherheit durch IT-Massnahmen herstellen.
- Datenschutzklauseln in Verträge mit Dienstleistern integrieren.
- Abläufe für Verletzungen der Datensicherheit und für Auskunfts- und Löschbegehren festlegen.

Fazit

Datenschutz ist bei der täglichen Arbeit und in allen Bereichen einzuhalten. Schwimmbäder bearbeiten Personendaten beispielsweise von den Abonentinnen und Abonenten, von den Besuchenden und von den Mitarbeitenden. Darunter befinden sich unter Umständen auch heikle Bearbeitungen von Personendaten, wie beispielsweise Videoüberwachungsaufnahmen. Damit der Datenschutz eingehalten werden kann, ist insbesondere wichtig, dass Massnahmen im Bereich IT-Sicherheit getroffen werden und die Mitarbeitenden in Datenschutz geschult und sensibilisiert sind. Dadurch können Datenlecks verhindert werden. ■