Informationsblatt des Ortsengel e.V.
zu einer „Datenpanne“

DSGVO - Wie geht man mit Datenpannen um?

Jeder Verein tut gut daran, bis zum 23. Mai 2018 seine Datenschutzpraktiken zu überprüfen und anzupassen. Hierzu gehört insbesondere auch zu überprüfen, ob die technisch- und organisatorischen Maßnahmen ausreichen, um die erhobenen und verarbeiten Daten ausreichend zu schützen. Jedoch lässt sich in der Praxis auch bei großen Anstrengungen nie völlig verhindern, dass es einmal zu einer Datenpanne kommt. Sei es, dass man gehackt wurde, oder es zu einem Verlust von Daten durch einen Softwarefehler kam.
Was dann zu tun ist, erklärt Ihnen der folgende Beitrag.

Was ist eine Datenpanne?

Eine Datenpanne, ein Datenvorfall bzw. eine Verletzung des Schutzes personenbezogener Daten ist ein Vorgang (oder mehrere zusammenhängende Vorgänge), durch welchen Daten

- Vernichtet werden

(Daten wurden gelöscht oder zerstört und können nicht wiederhergestellt werden)
Beispiel: Versehentliche Formatierung einer Festplatte mit Daten

- Verloren wurden

(Daten sind noch vorhanden, dem Verein stehen diese Daten jedoch nicht mehr zur Verfügung)
Beispiel: USB-Stick oder Laptop verloren

- Verändert werden

Korruptes Dateisystem, so dass auf vorhandene Daten nicht mehr zugegriffen werden kann.
Daten sind verschlüsselt und Schlüssel nicht zugänglich (Etwa der Fall bei Ransomware, ein spezieller Virus, welcher Daten verschlüsselt und den Schlüssel vorgeblich gegen Zahlung freigibt).
Nicht als Verlust gilt, falls aufgrund von planmäßigen Maßnahmen ein Zugriff auf Daten temporär nicht möglich ist (Etwa bei Wartung an einer Datenbank).

- diese unbefugt offengelegt werden

Daten können durch Dritte zur Kenntnis genommen werden, ohne dass es dafür eine Rechtsgrundlage gibt. Ob ein Abruf von Daten tatsächlich stattfand bzw. feststellbar ist, spielt grundsätzlich keine Rolle
Beispiel: Daten werden unbeabsichtigt auf einer Internetseite veröffentlicht
Eigentlich interne Datenbank kann von außen eingesehen werden

- oder Unbefugte Zugang erhalten

(Personen erhalten Zugang bzw. Zugriff zu Daten für welche sie nicht autorisiert sind)
Beispiel: Hacker erhalten Zugriff zu Datenbanken
Mitarbeiter des Vereins o. Ä. erhalten Zugriff zu Daten, zu welchen sie nicht befugt sind.
Ob dies unbeabsichtigt oder unrechtmäßig passiert, spielt hierbei keine Rolle. Hier geht es also sowohl um Versäumnisse und Versehen von Mitarbeitern des Vereins, wie vorsätzliches Handeln durch diese Mitarbeiter oder Dritte, also etwa durch einen Hackerangriff. Auf ein Verschulden des Vereins bzw. des Datenverarbeiters kommt es nicht an.

Worin liegen die Gefahren einer Datenpanne?

Es steht außer Frage, dass insbesondere bei sensiblen Daten die vorgenannten Vorfälle für die betroffenen Personen zu materiellen wie immateriellen Schäden und Beeinträchtigungen führen können. So können unbefugt erlangte Daten zu Diskriminierung oder Rufschädigungen führen oder zu Identitätsdiebstahl genutzt werden. Besonders offensichtlich ist das Missbrauchspotential natürlich bei Kreditkartendaten, aber auch andere Daten können ausgenutzt werden.

Wann ist bei einer Datenpanne die Aufsichtsbehörde zu informieren?

Die zuständige Aufsichtsbehörde, im Normalfall diejenige seines Bundeslandes ist im Normalfall unverzüglich, d.h. ohne schuldhaftes Zögern innerhalb von 72 Stunden ab dem Zeitpunkt, in dem die Verletzung des Datenschutzes bekannt ist zu informieren.
Von der 72-Stunden-Frist kann abgewichen werden, sofern eine vorherige Meldung nicht möglich ist, diese Überschreitung der Frist muss aber gegenüber der Aufsichtsbehörde begründet werden.
Meldepflichtig ist dabei stets der "Verantwortliche", also der Vereinsvorstand gemäß BGB selbst.
Sofern ein Auftragsdatenverarbeiter genutzt wird und es bei diesem zu einem Datenleck führt, so hat dieser den "Verantwortlichen" zu informieren, welcher die Meldung vorzunehmen hat.
Zu informieren ist, sobald genügend Wissen über den Vorfall bekannt ist um den Aufsichtsbehörden eine sinnvolle Meldung zu machen. Die DSGVO erlaubt ausdrücklich eine schrittweise Meldung. Ein Verein mit Datenleck sollte also nicht abwarten, bis alle Details eines Vorfalls vorliegen, sondern den Vorfall sobald dieser im Verein auffällt zügig melden und Details sofern notwendig nachliefern.

Wann muss die Aufsichtsbehörde nicht informiert werden?

Eine Datenschutzverletzung gegenüber der Aufsichtsbehörde besteht nicht, wenn durch diese voraussichtlich kein Risiko für Rechte und Freiheiten natürlicher Personen besteht.
Bezüglich des Risikos sind die oben genannten Gefahren einer Datenpanne zu berücksichtigen.Voraussichtlich kein Risiko bestände beispielsweise, wenn ein USB-Stick mit Daten verloren gingen würde, dieser jedoch nach Stand der Technik verschlüsselt ist.
Auch bei einer E-Mail, welche aus Versehen an einen falschen Adressaten gerichtet wurde, welche jedoch keine sensiblen Daten enthielt, kann ein Risiko für Rechte und Freiheiten von betroffenen Personen nicht angenommen werden.
Aufgrund der hohen Bußgelder, welche die DSGVO bei Datenschutzverstößen vorsieht, ist jedoch zu empfehlen, die Aufsichtsbehörden im Zweifelsfall lieber zu informieren.

Wie muss die Aufsichtsbehörde informiert werden?

Es gibt keine vorgeschriebene Form. Meldungen können per Telefon, Fax, Mail oder Brief erbracht werden. Allein aus Dokumentationsgründen ist eine schriftliche Form jedoch angeraten. Denn der meldepflichtige Verein hat auch die Nachweispflicht. Manche Aufsichtsbehörden bieten eigens elektronische Formulare an (z.B.)

Bayrisches Landesamt für Datenschutzaufsichticht
https://www.Ida.bayern.de/de/datenpanne.html

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz
https://www.datenschutz.r1p.de/de/themenfelder-themen/meldung-datenpanne-42a-bdsg/

Welche Informationen müssen an die Aufsichtsbehörde gemeldet werden?

Die Meldung muss mindestens vier Angaben enthalten

- Beschreibung der Art der Datenpanne (Verlust, Vernichtung, Veränderung, Unbefugte Offenlegung von Daten, s.o.)

Soweit möglich:

- Betroffene Mitgliederkategorien (z.B. „Ehrenmitglieder") und ungefähre Anzahl der betroffenen Personen
- Betroffene Datenkategorien (z.B. Bestelldaten, Passwortdaten, Kreditkartendaten) und ungefähre Anzahl an betroffenen Datensätzen
- Name & Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden) bzw. andere Kontaktdaten für weitere Informationen
- Beschreibung der wahrscheinlichen Folgen der Datenpanne
- Bereits erfolgte oder geplante Maßnahmen zur Behebung der Datenpanne bzw. ggfs. zur Abmilderung der Folgen

Wie bereits erwähnt ist es zulässig, Informationen schrittweise zu liefern, sofern diese zum Zeitpunkt der ersten Meldung noch nicht oder nicht vollständig vorhanden sind.
Die Angaben sollen die Behörde ermöglichen, den Ausmaß der Datenpanne zu beurteilen und festzustellen, ob die getroffenen bzw. geplanten Maßnahmen ausreichen um das Risiko für betroffene Personen auszuschließen bzw. zumindest abzumindern.
Kommt die Aufsichtsbehörde zu dem Schluss, dass die getroffenen Maßnahmen nicht ausreichen, so kann diese geeignete Maßnahmen anordnen.

Müssen Vorfälle dokumentiert werden?

la, der Vereinsvorstand gemäß BGB hat eine Dokumentationspflicht alle Datenpannen betreffend. Hier müssen die Umstände einer Datenpanne, die Auswirkungen und die ergriffenen Gegenmaßnahmen niedergeschrieben werden.
Hier sind auch Datenpannen zu dokumentieren, bei welchen der Verein die Aufsichtsbehörde nicht informiert, da voraussichtlich kein Risiko für die Rechte und Freiheiten von Personen besteht. Die Argumentation dieser Abwägung sollte ebenfalls zu Papier gebracht werden.
Da es hier keine Trivialgrenze gibt, sind selbst kleinste Datenpannen zu dokumentieren.
So wäre die vorher erwähnte falsch adressierte E-Mail auch zu dokumentieren.
Diese Dokumentation soll es den Aufsichtsbehörden ermöglichen, sowohl gemeldete wie nicht gemeldete Datenpannen nachvollziehen zu können. Die Dokumentation muss also detailliert genug sein, um eine solche Prüfung vornehmen zu können.
Diese Dokumentation muss nicht aktiv an die Aufsichtsbehörde kommuniziert werden, diese können diese jedoch anfragen.

Wann sind betroffene Personen zu informieren?

Unter Umständen müssen auch die Personen informiert werden, deren Daten vom Datenleck betroffen sind. Die Hürden dafür sind jedoch deutlich höher als für die Meldepflicht gegenüber der Aufsichtsbehörde.
Denn nur wenn für die betroffenen Personen voraussichtlich ein hohes Risiko für deren Rechte und Freiheiten besteht, sind diese unverzüglich zu informieren.
Während für die Aufsichtsbehörde die Meldepflicht bei dem voraussichtlichen Vorliegen eines grundsätzlichen Risikos zu informieren sind, gilt dies gegenüber den betroffenen Personen nur, wenn dieses Risiko hoch ist. Zur Ermittlung des Risikos muss die Eintrittswahrscheinlichkeit des Schadens mit dem potentiell entstehenden Schaden verglichen werden.

Ein hohes Risiko kann bei einer hohen Eintrittswahrscheinlichkeit bereits bei einem mittleren anzunehmenden Schaden angenommen werden. Ist der potentielle Schaden hoch, so reicht bereits eine geringe Eintrittswahrscheinlichkeit.
Auch spricht für ein hohes Risiko, wenn besonders sensible Daten von der Datenpanne betroffen sind (z.B. Gesundheitsdaten, Daten zu religiöser Überzeugung, Daten zum Sexualleben oder zur sexuellen Orientierung).

Wann müssen betroffene Personen nicht informiert werden?

Für die Informationspflicht bei Vorliegen eines hohen Risikos gibt es Ausnahmen.
So muss nicht informiert werden, wenn die Daten mit technisch und organisatorischen Maßnahmen nach Stand der Technik vor Missbrauch geschützt wurden.
Dies wäre etwa der Fall, falls beispielsweise zwar ein USB-Stick von einem Mitarbeiter versehentlich im Zug vergessen worden war und dieser personenbezogene Daten von Kunden enthielt, dieser jedoch nach Stand der Technik ausreichend verschlüsselt wurde.
Ein verlorener USB-Stick kann im Normalfall an jeden handelsüblichen Rechner angeschlossen werden, die Eintrittswahrscheinlichkeit wäre also hoch. Sofern die dort vorhanden Daten ein gewisses Missbrauchspotential haben, könnte also eigentlich ein hohes Risiko angenommen werden.
Wenn die Daten jedoch auf dem USB-Stick so verschlüsselt wurden, dass diese für einen Dritten nicht lesbar sind, entfällt die Informationspflicht.
Darüber hinaus entfällt die Pflicht, wenn es dem Verein gelang, nach erfolgter Datenpanne durch getroffene Maßnahmen das hohe Risiko zu beseitigen. Die im Anschluss an den Vorfall getroffenen Maßnahmen müssen einen Missbrauch also unterbinden oder mindestens sehr unwahrscheinlich machen.
Schließlich kann eine Benachrichtigung der einzelnen betroffenen Person entfallen, wenn diese mit unverhältnismäßigen Aufwand verbunden wäre.
Diese Ausnahme befreit jedoch nur von der individuellen Information, stattdessen muss ein Verein in diesem Fall eine öffentliche Bekanntmachung (amtliches Verkündungsblatt, Tageszeitung) oder eine Veröffentlichung im Internet durchführen. Eine solche Internetveröffentlichung muss so präsent sein, dass davon ausgegangen werden kann, dass die betroffenen Personen davon Notiz nehmen können.

Wie sind betroffene Personen zu informieren?

Es ist keine Form vorgeschrieben, grundsätzlich kann die Information also mündlich, telefonisch, per Fax, Brief oder E-Mail erfolgen. Allerdings muss das Unternehmen im Zweifelsfall den Zugang der Information belegen können, weswegen auch hier die schriftliche Form zu empfehlen ist.

Welche Informationen müssen an betroffene Personen kommuniziert werden?

Es muss

- die Art der Verletzung beschrieben werden,
  hier sollte auch die betroffenen Daten genannt werden.
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle um weitere Informationen zu erhalten, genannt werden
- Eine Beschreibung der wahrscheinlichen Folgen gegeben werden
- sowie eine Beschreibung von bereits getroffenen oder noch geplanten Maßnahmen um Auswirkungen für die Betroffenen zu verhindern oder wenigstens abzumildern.

Die Informationen müssen in klarer und einfacher Sprache gehalten sein. Informationen müssen übersichtlich, eindeutig und hinreichend strukturiert und sollten sich nur auf den Vorfall beziehen, also nicht mit anderen Infonnationen verbunden werden. Ebenso sollte kein Fachvokabular verwendet werden.

Die Information hat unverzüglich zu erfolgen, d.h. ohne schuldhaftes Zögern. Hier gibt es jedoch keine feste 72- Stunden-Pflicht. Je nach Datenpanne kann eine sehr zeitnahe Information notwendig sein, insbesondere wenn betroffene Personen selbst etwas tun können, um das Risiko einzudämmen. Dies ist etwa denkbar, wenn Passwörter durch einen Hack entwendet wurden.
Da viele Nutzer die gleichen Passwörter für verschiedene Accounts nutzen, sollten diese zeitnah informiert werden, damit diese die Passwörter an anderer Stelle schnell ändern können.

Da bei jeglichem potentiellen Risiko die Aufsichtsbehörden zu informieren sind, können diese zu jeglichen Fragen, ob betroffene Personen zu informieren sind, zu Rate herangezogen werden. Die Aufsichtsbehörden können auch selbst Unternehmen anweisen, betroffene Personen zu informieren.

Fazit:

Jeder Verein sollte sein Bestes tun, zu verhindern, dass es zu Datenpannen kommt.
Ist dies jedoch doch einmal passiert, ist schnelles Handeln angesagt.

Insbesondere gegenüber der Aufsichtsbehörde ist mit der regulären Frist von 72 Stunden ein sehr enges Zeitfenster vorgegeben, einen Vorfall zu melden.

Jeder Verein sollte sich daher im Vorfall einen Reaktionsplan machen.
In diesem sollte geklärt und mit den eigenen "Mitarbeitern" kommuniziert werden:

- Wie erkennt man eine Datenpanne,

Wie geschrieben stellt bereits eine falsch adressierte Email eine Verletzung des Datenschutzes im Sinne der OSGVO dar.

- Wer ist im Verein zu informieren, wenn es zu einer Datenpanne kommt?

Es bedarf klarer Kommunikationsstrukturen, damit die Information nicht untergeht, und so die „72-Stunden-Frist“ nicht eingehalten wird

- Wer übernimmt die Prüfung einer Datenpanne?
- ► Besteht ein Risiko? Muss also die Aufsichtsbehörde informiert werden?
- ► Ist dieses Risiko hoch, müssen also auch betroffene Personen informiert werden?
- ► Welche Maßnahmen können getroffen werden, um das Risiko zu reduzieren / auszuschließen,
- Wer übenimmt sofern notwendig die Meldung an die Aufsichtsbehörde und ggfs. an die betroffenen Personen?
- Wer ist Ansprechpartner für die Aufsichtsbehörde und ggfs. für die betroffenen Personen?
- Wie werden Datenpannen im Unternehmen dokumentiert und wer ist dafür zuständig?

Je nach Tätigkeitsbereich eines Vereins ist es sinnvoll, genaue Reaktionspläne für mögliche Szenarien zu erstellen. Hier könnte etwa geklärt werden, wie bei einem Hackerangriff die Kommunikationswege und mögliche Schritte sind.