TOM - Technische und organisatorische Maßnahmen

Work in progress

Alle TOMs gelten sowohl für alle vom Stamm genutzten Räume, für die Privaträume, für Stammescomputer, aber auch für private Smartphones, Laptops, Tablets und PCs. Sprich für alles auf dem Daten verarbeitet oder aufbewahrt werden.

Um Daten zu schützen, müssen wir auch einige so genannte **TOMs** treffen. Diese TOMs dienen zum einem dem Datenschutz zum anderen haben sie den Zweck, dass sie den BdP und Euren Stamm vor Schaden bewahren.
Nämlich vor Schäden, die durch ein Leck oder ähnlichem entstehen können. Dazu reicht es schon, dass die falsche Liste an alle Mitglieder des Stammes verschickt wurde.

Personenbezogene Daten sollen verschlüsselt und nach Möglichkeit pseudonymisiert werden. Außerdem sollen sei vertraulich und integer (also unversehrt) behandelt werden, sowie verfügbar sein; die Systeme (PCs, usw.) und Dienste (Email - Provider usw.) mit denen die Daten verarbeitet werden sollen zudem belastbar sein. Was das im Einzelnen heißt. wird unten erklärt.

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsdatenverarbeiter (Art. 30 Abs. 2 lit. d)

Folgende Punkte gibt es bei TOM zu beachten.

Pseudonymisierung	Davon spricht man, wenn personenbezogene Daten nach Möglichkeit pseudonymisiert werden sollen. Zum Beispiel durch einen falschen Namen die Identifikation einer Person unmöglich machen.	
Verschlüsselung	Davon spricht man, wenn personenbezogene Daten digital oder analog verschlüsselt werden sollen.	**Eine kleine Geschichte, wie es nicht laufen sollte.**
Gewährleistung der Vertraulichkeit	Davon spricht man, wenn Menschen, die bestimmte Daten nichts angehen, zu diesen auch keinen Zugang haben sollen.	*Die Sippenführerin Veronika Vergesslich hat die ausgefüllten Anmeldungen zum Sippenwochenende im Stammesheim liegen lassen. Die junge R/R - Runde amüsieren sich, dass ein Sippling keine Milchprodukte verträgt.*
Gewährleistung der Integrität	Davon spricht man, wenn die Daten davor geschützt werden sollen, von irgendwem verändert zu werden, der das nicht darf.	*Plötzlich kommt der Rundensprecher rein und sieht die Anmeldungen. Bevor die Anmeldungen eingesammelt werden, schreibt er bei einem Sippling dazu, dass er keine Schokolade verträgt, nur um diesen zu ärgern.*
Gewährleistung der Verfügbarkeit	Davon spricht man, wenn die Daten sofort genutzt werden können, wenn sie benötigt werden.	*Inzwischen sitzt Veronika Vergesslich zu Hause und stellt fest, dass das Sippenwochenende zu günstig kalkuliert wurde und sie die Eltern über schnell über die Mehrkosten informieren muss. Blöderweise findet sie die Anmeldungen nicht und weiß nicht, wie sie die Eltern erreichen soll.*
Gewährleistung der Belastbarkeit der Systeme	Davon spricht man, wenn die "Systeme und Dienste", z.B. PC oder hessenwiki, genug Leistung haben, dass auf ihnen Daten verarbeitet werden können ohne in die Knie zu gehen.	*Natürlich hat die Sippenführerin die Telefonnummern der Eltern auf ihrem Laptop gespeichert. Dachte sie zumindest. Sie kann sie nicht finden und noch während sie sucht, fällt ihr ein, dass sie die Datei neulich löschen musste, weil die Festplatte mal wieder voll war.*
Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall		

	Davon spricht man, wenn mal irgendwas passiert (Platzregen auf Fahrt (physisch) oder ein technischer Defekt). Dann solltet ihr Vorkehrungen getroffen haben, wie ihr die Daten wiedergewinnen könnt. Ziel muss sein, die Daten schnell wieder zur Verfügung zu haben ohne sie noch einmal neu zu erheben.	*Da fällt Veronika ein, dass sie die Anmeldungen im Stammesheim liegen gelassen hat und fährt sofort hin. Der Regenguss auf dem Heimweg hat alles durchweicht. Wirklich alles. Von den Anmeldungen lässt sich nur noch "verträgt keine Schokolade" entziffern, da es mit permanent Marker geschrieben war.*
Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen	Davon spricht man, wenn Ihr z.B. von eurem Virenschutz und Euren PC auf dem neusten Stand haltet und ihm ab und an mal ein Update gönnt. Die kommen, wie Ihr wisst immer automatisch, aber es schadet auch nicht, wenn Ihr selber mal schaut, ob noch alles auf dem neusten Stand ist. Überprüft auch, ob das WLAN Passwort nicht schon mehr Leute haben als Euch lieb ist. Da es ja auch nicht digitale Daten gibt (Mitgliederanträge usw.) solltet Ihr mal überlegen, wer inzwischen alles weiß wo der Schlüssel zum Schrank ist. Und wer immer wieder die Liste mit den Kontaktdaten ins Heim hängt.	*So läuft es besser.* *Wegen ihrer Vergesslichkeit hat Veronika angefangen sich die Anmeldungen der Eltern als PDF per Mail schicken zu lassen. Nun kann sie die Anmeldungen* ***verschlüsselt*** ⚠️ *in ihrer Dropbox speichern. So kann sie jeder Zeit drauf zugreifen.*

TOM Vorlage:

Informationen zu TOM:

https://it-service.network/blog/2018/04/03/tom-datenschutz-toms-dsgvo/

Wer muss was, wann, warum und wie verarbeiten? Diese Frage solltet ihr Euch stellen bevor Ihr anfangt wie wild TOM Listen zu erstellen.
Hier an einem kurzen Beispiel - Sommerlager - erklärt:

Wer muss auf dem Lager auf die Daten zugreifen? - Lagerleitung (gesamte TN); Gruppenleitung (auf die TN der Gruppe)
Wann muss der/die Schatzmeister*in die Zuschüsse beantragen und braucht deshalb die TN-Listen mit Adressen und Alter? usw.

Diese Angaben müssen immer wieder neu entschieden werden, auch wenn es Ähnlichkeiten gibt.

Bei Sachen die immer wieder kommen, wie Aufnahmeanträge, solltet ihr vorher klären, wo sie aufbewahrt werden und wer Zugang hat.

Am Besten macht ihr alles schriftlich, da viele der Antworten von oben in den **nächsten Jahre gebraucht werden!**

Die zweite Frage ist, welche **Risiken** können auf uns zukommen? Was passiert, wenn war verloren geht, Daten verändert, falsch vernichtet oder ausversehen offengelegt wurden. Kontodaten der Mitglieder, die plötzlich im Netz zu finden sind - dann habt Ihr ein sehr großes Problem. Weniger problematisch, aber auch nicht gut, ist das rumliegen lassen von Zuschusslisten (unbefugte Offenlegung) und in der dann jemand nachträglich was verändert. Sowas kann ganz schön Ärger mit den Leuten geben, die uns die Zuschüsse geben.

Bei der **Risikoabwägung** hilft Euch das Verzeichnis der Verarbeitungstätigkeiten. Denn darin steht, wer, wann, wie und warum Daten verarbeitet hat und wo es ein Leck gegeben haben könnte.