

Daten schützen

Weshalb?

Daten sind für Ihre Feuerwehr, aber auch für die betroffenen Personen, ein sehr wertvolles Gut. Schon allein deshalb lohnt es sich, diese Daten zu schützen. Aber auch der Gesetzgeber erwartet von Ihnen, dass Sie geeignete technisch-organisatorische Maßnahmen ergreifen, um personenbezogene Daten adäquat vor Missbrauch, Diebstahl, Verlust und unautorisiertem Zugriff zu schützen.

(Rechtsgrundlage: u.a. Art. 32 DSGVO und Art. 5 DSGVO)

Zugriff autorisieren

Weshalb?

Das E-PROFVS ist ein wichtiges und sehr zentrales System, das es vor unbefugtem Zugriff zu schützen gilt. Sie müssen deshalb dafür sorgen, dass nur autorisierte Personen Zugriff darauf haben.

(Rechtsgrundlage: u.a. Art. 32 DSGVO und Art. 5 DSGVO)

Lösung im E-PROFVS:

Unsere Software schützt auf verschiedenen Wegen vor unbefugtem Zugriff. Besonders wichtig ist natürlich, dass Sie sicherstellen, dass für jeden Benutzer in der Software ein sicheres Kennwort vergeben wurde. Ab der Version 2.18.5-1 wird ein noch sichereres Verfahren angewendet um die Passwörter zu speichern. Alle Benutzer die ein altes Passwort verwenden werden nach dem Login aufgefordert ein neues Passwort zu vergeben.

Außerdem ist es empfohlen die Google 2 Wege Authentifizierung für die Benutzer zu aktivieren. siehe [Google 2 Wege Authentifizierung](#)

Daten einschränken

Weshalb?

Um das Risiko für einen Datenmissbrauch zu reduzieren, fordert das Datenschutzgesetz, dass der Zugriff auf personenbezogene Daten nur dem Mitarbeiterkreis zugänglich gemacht werden darf, für die der Zugriff darauf für ihre Arbeit unbedingt erforderlich ist.

(Rechtsgrundlage: u.a. Art. 32 DSGVO und Art. 25 DSGVO)

Lösung im E-PROFVS:

Das E-PROFVS hat eine sehr granulare Benutzerverwaltung. Sie haben hier die Möglichkeit, für einzelne Benutzer oder ganze Gruppen u. a. das Folgende freizugeben oder ganz zu sperren:

- Zentrale Funktionen der Software (lesen, ändern, löschen und exportieren von Daten)
- Individuell die Sichtbarkeit, Bearbeitbarkeit und Löschbarkeit bestimmter Datensätze (z. B. Einschränkung auf bestimmte Abteilungen)

Schränken Sie also, wo sinnvoll, den Zugriff auf Ansichten, Datensätze auf bestimmte Gruppen oder gar Einzelpersonen ein. Die Benutzerverwaltung ist nicht nur ein unverzichtbares Instrument für den Datenschutz, sondern ermöglicht auch, dass jeder Benutzer seinen eigenen Funktionsumfang nutzt, welcher perfekt auf seine individuellen Bedürfnisse abgestimmt ist. Jeder Benutzer sieht nur die für

die eigene Arbeit wichtigen Bereiche und Datensätze. Dies verringert die Komplexität der Software, schafft Klarheit, reduziert den Schulungsaufwand und sorgt für Akzeptanz, weil das Arbeiten mit der Software Freude macht.

From:

<https://fvsweb.com/wiki/> -

Permanent link:

https://fvsweb.com/wiki/doku.php?id=dsgvo:daten_schuetzen



Last update: **29.03.2019 01:00**