<msg class="important">

Liebe IT-Leiter: DSGVO ist nicht Ihre Verantwortung, aber Ihre Aufgabe!

</msg>

Die Datenschutz-Grundverordnung (DSGVO) ist seit Mai in Kraft. Die erste Anlaufstelle, wenn es um technische Maßnahmen zur Erfüllung der Datenschutzvorgaben geht, ist die IT-Abteilung. Wie wird die Verarbeitung personenbezogener Daten systemtechnisch unterstützt? Sind die Daten ausreichend gesichert? Darauf müssen Sie Antworten haben. Wir haben Ihnen **5 Work-Hacks** aus technischer Sicht zusammengestellt, mit denen Sie starten können.

Art. 30 Abs. 1 Satz DSGVO

Verzeichnis von Verarbeitungstätigkeiten
Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.

Hack 1

Unterstützen Sie den Datenschutzbeauftragten

Erstellen Sie folgende Übersichten:

- über alle IT-Anwendungen – Nicht das Softwareinventar, sondern die Verfahren!
- über alle in Anwendungen erfasste Daten und die evtl. Übermittlung von Daten an Dritte
- über das aktuell genutzte Backupkonzept
- über allgemeine technische und organisatorische Sicherheitsmaßnahmen

Art. 17 DSGVO

Recht auf Löschung
»Recht auf Vergessenwerden«

Hack 2

Vergiss mich, vergiss mich nicht – Aufbau eines Löschkonzepts

Folgende Schritte sollten Sie bei der Erstellung eines Löschkonzepts durchführen:

1. Personenbezogene Daten im Unternehmen lokalisieren (siehe Verarbeitungsverzeichnis).
2. Aufbewahrungsfristen von Rechtsabteilung, Steuerberater oder notfalls Geschäftsführung festlegen lassen.
3. Daten in Kategorien einordnen, für die jeweils die gleiche Aufbewahrungsdauer gilt. Löschregeln je Kategorie definieren (Art. 25 Abs. 2 DSGVO i.V.m. Erw.-Grund 39). Hier empfiehlt es sich, die Anzahl der Löschregeln möglichst gering zu halten.
4. Nach handels- und steuerrechtlichen Vorschriften oder Vorgaben (GoBD) archivieren.
5. Nach Ablauf der Aufbewahrungsfrist Löschung nach sicheren Verfahren mit automatisierten Löschprotokoll. Bei Daten in Cloud-Anwendungen empfiehlt sich der Einsatz von Cloud Access Security Broker bzw. Cloud Data Protection Gateway, bei dem von vorneherein nur verschlüsselte Daten in der Cloud landen. Es genügt, den Schlüssel zu löschen, um die Daten dauerhaft unzugänglich zu machen.
6. Testen, testen, testen! Vor Inbetriebnahme der Löschverfahren umfassend testen, ob eine Löschung richtig und rechtzeitig durchgeführt wird und die Protokolle erzeugt werden. Vor allem, wenn Abhängigkeiten zwischen verschiedenen Systemen bestehen. Wie schnell wird in die angeschlossenen Systeme synchronisiert? Kommt es zu Fehlfunktionen?
7. Dokumentieren – et voilà, damit haben Sie ein Löschkonzept.

Art. 32 DSGVO

Sicherheit der Verarbeitung

Hack 3

Verschlüsselung DAU-kompatibel ermöglichen

In der DSGVO werden zwei konkrete Maßnahmen genannt, die Sie umsetzen sollten: die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten. Verschlüsselung ist für eine Vielzahl von E-Mails eigentlich die einzig regelkonforme Übermittlungsart. In der Praxis zeigt sich aber, dass viele User Verschlüsselungsverfahren aufgrund zu komplexer Abläufe umgehen.
Unsere Empfehlung: Etablieren Sie Schritt für Schritt Verschlüsselungsverfahren in Ihrem Unternehmen. Beginnen Sie bei der Kommunikation mit dem Steuerberater/Wirtschaftsprüfer und weiten Sie es dann auf Ihre Hauptkunden und Bewerbungen aus.

Als kryptographische Maßnahmen empfehlen sich aktuell:

- Bitlocker oder Veracrypt zur Datenträgerverschlüsselung
- HTTPS und TLS zur Transportverschlüsselung
- symmetrische (z.B. 7-Zip) und asymmetrische (S/MIME, PGP) Verfahren zur Ende-Zu-Ende-Verschlüsselung.

Art. 32 DSGVO

Sicherheit der Verarbeitung

Hack 4

Pseudonymisierung

Pseudonymisierung dient vor allem dazu, die Zuordnung von Daten und Personen zu erschweren. Gehen Sie am besten folgendermaßen vor:

- Versehen Sie Daten z.B. mit einem nicht personenbezogenen Namen oder einer Nummer – sofern Ihre Datenverarbeitung dies zulässt.
- Stellen Sie sicher, dass die pseudonymisierten Daten ohne weitere Informationen keine Zuordnung zu betroffenen Personen zulassen.
- Bewahren Sie das Pseudonym und die zur Identifizierung notwendigen Daten getrennt voneinander auf – räumlich und technisch.
- Für die Gewährleistung der Pseudonymisierung bei Google Analytics binden Sie folgendes Script ein:

```
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag () {dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'UA-4151676-2', { 'anonymize_ip':true});
</script>
```

Art. 32 DSGVO

Sicherheit der Verarbeitung

Hack 5

Überprüfen Sie Ihre technischen und organisatorischen Sicherheitsmaßnahmen (TOMs)

Im Grunde hat jedes Unternehmen mehr oder weniger umfangreiche technische und organisatorische Datensicherheitsmaßnahmen im Einsatz. Um den Ist-Stand Ihrer Unternehmens-IT zu erfassen, können ein IT-Sicherheitscheck oder eine IT-Infrastrukturanalyse nützlich sein. Auf Basis einer Risikobewertung können Sie die bestehenden technischen und organisatorischen Maßnahmen auf ihre Wirksamkeit überprüfen und analysieren, ob weitere Maßnahmen notwendig sind.
Unser Tipp: Greifen Sie dafür auf international anerkannte Normen und Standards in der Informationssicherheit zurück, wie beispielsweise die ISO 27002 oder BSI Grundschutz.

Weitere Infos, Consultingangebote & Trainings:
www.softed.de/dsgvo