1 Jahr DSGVO
Datenschutz im sozialen Bereich richtig umsetzen

Am 26. Mai 2018 - also vor fast genau einem Jahr - wurde die EU-Datenschutzgrundverordnung (DSGVO) wirksam. Sie werden sich vermutlich erinnern: allerorts wurden Schreckgespenster wie Abmahnwellen oder Bußgelder in aberwitziger Millionenhöhe in den schrillsten Farben illustriert. Die Branche der Datenschutz-Dienstleister wurde regelrecht überrannt von einem Heer schlecht qualifizierter Neulinge, die im DSGVO-Rausch verunsicherten Kunden überteuerte und oft unsinnige Leistungen verkauften. Für Verantwortliche in Organisationen aller Größen und Ausrichtungen war erhebliche Rechtsunsicherheit entstanden, da sie sich von der Politik nicht im Mindesten auf die neuen Anforderungen vorbereitet fühlten.

Bei dsXprt haben wir uns seit langem auf die Datenschutz-Beratung im sozialen Bereich und Gesundheitswesen spezialisiert.

Unsere Kunden vertrauen uns nicht nur bei der Klärung verrückt klingender Pressemeldungen wie der Forderung, Gesichter auf Fotos in Kindertagesstätten zu schwärzen oder angeblichen Verboten, Namen von Heimbewohnern an der Tür anzubringen. Auch bei ganz alltäglichen Themen wie Auskunftsrechten von Betroffenen oder Aufbewahrungspflichten von Daten stehen Ihnen unsere zertifizierten Datenschutzbeauftragten und -Auditoren mit langjähriger Expertise zur Seite.

Doch was ist von der Verunsicherung geblieben, die im Rahmen der DSGVO entstanden ist?

Die befürchtete Abmahnwelle ist tatsächlich ausgeblieben. Die deutschen Aufsichtsbehörden haben im ersten Jahr der DSGVO Bußgelder von 500.000 EUR ausgesprochen, gehen dabei aber mit erfreulichem Augenmaß vor. So wurde berücksichtigt, dass gerade kleine Organisationen nicht ausreichend auf die neuen Anforderungen vorbereitet waren. Allerdings ist auch klar: Die Schonzeit ist jetzt vorbei. Jeder Verantwortliche hatte mittlerweile hinreichend Zeit, die Anforderungen kennenzulernen und umzusetzen.

Die Schonzeit ist jetzt vorbei.

Bußgelder von bis zu 4% des weltweiten Jahresumsatzes oder 20 Millionen EUR (der höhere Wert ist relevant) sind im Gesetz klar verankert. Art. 83 regelt außerdem, dass Geldbußen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein müssen.

In diesem Kontext haben die deutschen Aufsichtsbehörden angekündigt, Beratungen zukünftig auf ein Minimum zu beschränken und stattdessen die Einhaltung der gesetzlichen Anforderungen konsequenter zu überwachen und dem entsprechend auch vermehrt Bußgelder auszusprechen. Beispielsweise können gegen Unternehmen, die zur Bestellung eines Datenschutzbeauftragen verpflichtet sind und diesen nicht bestellt haben, gem. Art. 83 DSGVO Geldbußen von bis zu 10 Mio. EUR bzw. 2% des Jahresumsatzes verhängt werden.

Nicht jeder muss einen Datenschutzbeauftragten benennen. Aber jede Organisation muss sich zwingend mit der DSGVO auseinandersetzen und die gesetzlichen Anforderungen umsetzen. Wer das Thema ignoriert befindet sich im Bußgeldrisiko.

Doch die Umsetzung der Datenschutz-Anforderungen in der Organisation hat oft viele weitere positive Effekte. In unserer Beratungspraxis gerade im sozialen Bereich und im Gesundheitswesen stellen wir fest, dass viele Kunden zwar zunächst die Aufwände scheuen, die mit dem Datenschutz verbunden sein können. Diese Einstellung ändert sich in der Regel recht schnell, wenn klar wird, wie leicht mit einer strukturierten Anleitung das Thema Datenschutz gehandhabt werden kann und welche **Einsparungen** sich tatsächlich ergeben können.

Die Arbeit am Datenschutzkonzept einer Organisation birgt durch Klärung von Fehlinformationen oder Missverständnissen oft enorme Verbesserungsmöglichkeiten.

Beispielsweise besteht ein offenbar weit verbreiteter Irrglaube, dass Gesundheitsdaten 30 Jahre aufbewahrt werden müssen. Hierdurch entstehen teilweise immense Kosten für Lagerung und Archivierung. Bei der Umsetzung der DSGVO-Anforderungen wird dann festgestellt, dass oft das exakte Gegenteil der Fall ist und Daten oft gar nicht so lange aufbewahrt werden dürfen. Somit können Aufwände für Langzeitarchivierung und Lagerung usw. eingespart werden.

10 Punkte, um in der Organisation datenschutzkonform zu arbeiten

1. Sie müssen sich mit der DSGVO beschäftigen. Daran führt kein Weg vorbei.
2. Prüfen Sie, ob Sie zur Benennung eines Datenschutzbeauftragten verpflichtet sind. Wenn Sie einen Datenschutzbeauftragten benennen, stellen Sie sicher, dass dieser über die Qualifikation und das Fachwissen verfügt, um der Aufgabe gerecht zu werden (Art. 37 DSGVO) und keine Interessenskonflikte vorliegen (Personen mit gleichzeitiger Verantwortung in Geschäftsleitung, Personal oder IT sind als DSB grundsätzlich ungeeignet).
3. Erstellen Sie die grundlegenden Pflichtdokumentationen: Verzeichnis von Verarbeitungstätigkeiten, Technische und organisatorische Maßnahmen, usw.
4. Definieren Sie Datenschutz-Prozesse: Auskunftsprozess, Notfallprozess bei Datenschutzvorfällen, ...
5. Machen Sie sich mit den Grundsätzen der Verarbeitung vertraut (Art. 5 DSGVO).
6. Prüfen Sie die Rechtsgrundlagen, bspw. Einwilligungen von Kunden, Partnern, Mitarbeitern zu bestimmten Verarbeitungstätigkeiten (Art. 6 DSGVO).
7. Erstellen Sie ein Aufbewahrungskonzept und ein Löschkonzept auf der Basis von Datenarten und -Kategorien
8. Erstellen Sie ein Berechtigungskonzept: Wer hat Zugriff auf welche Daten? Wer darf wem worüber Auskunft erteilen?
9. Erarbeiten Sie Kommunikations-Richtlinien zur Nutzung von E-Mail, Internet und Social Media, Telefon, Messenger-Diensten. (Ein Hinweis am Rande: WhatsApp ist in der betrieblichen Kommunikation grundsätzlich kritisch zu betrachten – bitte erwägen Sie die Nutzung sicherer Alternativen.)
10. Führen Sie die jährliche Datenschutzunterweisung für Mitarbeiter durch.

Datenschutzkonformes Arbeiten ist mit dem richtigen Konzept kein Problem. Allerdings darf nicht verschwiegen werden, dass die Umsetzung eines Datenschutzkonzeptes durchaus einigen Aufwand verursacht. Mit langjähriger Expertise und Branchenkenntnis unterstützen die **dsXprt**-Datenschutzbeauftragten Sie bei der schnellen, umfassenden und kostenbewussten Umsetzung der datenschutzrechtlichen Anforderungen.