Checkliste
Datenschutz in KMU bis 250 Mitarbeiter

Führen Sie mit dieser Checkliste eine Schnelleinschätzung Ihres Datenschutzstandards durch. Die Liste umfasst die wichtigsten Praxispunkte aus dem Schweizerischen Datenschutzgesetz, aus der EU-Datenschutzgrundverordnung DSGVO und aus der kommenden Schweizerischen Datenschutz Totalrevision im 2019.

Kundendaten:

- ☐ Informieren Sie Ihre Kunden über die Erfassung personenbezogener Daten, wenn diese aus einem Vertragsverhältnis nicht klar hervorgehen.
- ☐ Holen Sie die Einwilligung Ihrer Kunden zu obenstehendem Punkt ein. Die Einwilligung müssen Sie belegen können.
- ☐ Prüfen Sie die Kundendaten darauf, dass dort nur Daten erfasst sind, welche Sie wirklich für die Vertrags- oder Auftragserfüllung benötigen
- ☐ Stellen Sie sicher, dass Sie keine Kundendaten an Dritte weitergeben oder verkaufen

Organisatorisches:

- ☐ Erstellen Sie einen Meldeprozess für Datenschutzbrüche und -Verstösse
- ☐ Nehmen Sie das Thema Datenschutz in Ihre obligatorische Risikobewertungsmatrix auf
- ☐ Informieren Sie Ihre Mitarbeitende mit Kundenkontakt, wie bei Anfragen zu Datenlöschung, Berichtigung oder Herausgabe zu reagieren ist (Prozessbeschrieb)

IT Systeme:

- ☐ Überprüfen Sie laufend Ihre Datensicherheit auf organisatorische und technische Mängel
- ☐ Überprüfen Sie, ob Sie dem Recht von Betroffenen auf Datenherausgabe, -Berichtigung und -Löschung mit Ihren IT Systemen nachkommen können
- ☐ Prüfen Sie, wohin Ihre Kundendaten überall hinfliessen, ob der Datenschutz hier vertraglich geregelt ist, und ob die Betroffenen über die Weitergabe Bescheid wissen
- ☐ Prüfen Sie, ob personenbezogene Daten im Ausland gespeichert werden (z.B. Dropbox usw.), und ob die Betroffenen hierfür ihre explizite Einwilligung gegeben haben
- ☐ Richten Sie in Ihrer Kundendatenbank sogenannte «Fangadressen» ein, damit Sie bei einem Datendiebstahl sofort informiert sind und reagieren können

Webseite:

- ☐ Erstellen einer Datenschutzrichtlinie auf der Webseite
- ☐ Erstellen eines Impressums mit Postadresse und Kontaktoptionen, Verlinkung am besten in der Fusszeile jeder Seite
- ☐ Überprüfen aller Anbieter von Plugins und Addons, ob sie den Datenschutz einhalten, und verlinken auf deren Datenschutzrichtlinie
- ☐ Keine Social-Media Buttons einsetzen, welche automatisch Daten übermitteln
- ☐ Keine Plugins einsetzen, welche automatisch Daten an Dritte weitergeben
- ☐ Hinweis in der Datenschutzrichtlinie über ihren Provider, und was dieser alles speichert. Kann beim Provider angefragt werden
- ☐ Sicherstellen, dass Sie mit Ihrem Web-CMS (Wordpress, TYPO3, usw.) Benutzerdaten auf Anfrage herausgeben oder löschen können
- ☐ Sicherstellen, dass aufgezeichnete IP-Adressen in Ihrem Web-CMS anonymisiert werden
- ☐ Sicherstellen, dass Datenübermittlungen verschlüsselt geschehen, z.B. mittels SSL-Zertifikats
- ☐ Sicherstellen, dass Sicherheitsupdates für die Webseite gemäss Wichtigkeit zeitgemäss ausgeführt werden, z.B. innert 24h, und dies vertraglich auch geregelt ist
- ☐ Meldung für Cookies: hier fehlen Praxiserfahrungen und die Meinungen gehen auch juristisch weit auseinander. Um auf der sicheren Seite zu sein, kann man das einbauen lassen.
- ☐ Privacy-by-Default: auf Kontaktformularen usw. nur die wirklich zwingenden Angaben als Pflicht-Eingabefelder definieren

Google Analytics:

- ☐ IP-Anonymisierung im Tracking-Code einschalten
- ☐ Aktivieren der Datenaufbewahrungsrichtlinie in Google Analytics
- ☐ Aktivieren der Option Personenbezogene Daten nach 14 Monaten automatisch löschen
- ☐ Erwähnung des Trackings in der Datenschutzerklärung auf der Webseite
- ☐ Option auf der Webseite zur Verfügung stellen für Opt-Out aus Google Analytics
- ☐ Auftragsverarbeitungsvertrag lösen, mit einem Klick in Google Analytics aktivierbar

Newsletter (für Personen ohne aktive Geschäftsbeziehung):

- ☐ Prüfen, ob der Anbieter einen angemessenen Datenschutz umsetzt
- ☐ Double-Opt-In Verfahren verwenden: damit erhält ein Anmelder eine Mail mit Bestätigungslink, den er anklicken muss
- ☐ Newsletter-erwünscht-Checkbox bei Kontaktformularen: auch hier Double-Check-In, und Häklein nicht standardmässig aktiviert
- ☐ Von bestehenden Newsletter-Empfängern rückwirkend Bestätigung einholen, falls bisher ohne Double-Opt-In Verfahren gearbeitet wurde
- ☐ Sicherstellen, dass man sich einfach von einem Newsletter wieder abmelden kann
- ☐ In der Datenschutzerklärung der Webseite auf den Newsletter aufmerksam machen
- ☐ Auftragsverarbeitungsvertrag lösen, bei vielen Newsletter Tools einfach aktivierbar

INSOR AG

Schwarzackerstrasse 11, Wallisellen
+41 44 585 2700
info@insor.ch
www.insor.ch

Wer sind wir?

Von der einfachen Homepage bis zum komplexen Anmeldesystem für Kurse: Als KMU realisieren wir webbasierte Projekte innovativ und kundenorientiert. Insbesondere in den Branchen Bildung und Betreuung haben wir uns in den vergangenen Jahren einen Namen gemacht, haben aber auch Kunden aus den unterschiedlichsten Wirtschaftszweigen.