web updates kmu Checkliste - Datenschutzgesetz DSG Schweiz

Offen/erledigt	Aufgaben	Bemerkungen
	Bearbeitungsverzeichnis (Art. 12 DSG)	
	Systemlandschaft definieren	
	Wie sieht ihre Systemlandschaft aus:	
	Welche Daten speichern Sie und warum?	
	Welche Geräte nutzen Sie, welche auf die Daten zugreifen können?	
	Werden die gespeicherten Daten an externe Dienste synchronisiert oder gespeichert?	
	Wie werden Backups erstellt und wo gespeichert?	
	Wer hat darauf Zugriff (Verarbeiter)?	
	Welche Personen können auf die Daten zugreifen?	
	Gibt es ein IT-Partner der Zugriff hat?	
	Wer ist der Webhoster / Supporter?	
	Verantwortlichen bestimmen	
	Hat ihre Firma mehr als 1 Person, dann ist die Frage, wer hat die Verantwortung über die Daten?	

Offen/erledigt	Aufgaben	Bemerkungen
	Datensicherheit (Art. 8 DSG)	
	Übersicht aller Massnahmen	
	Zu jedem einzelnen Punkt der Systemlandschaft sollte man sich folgende Punkte notieren:	
	Werden die Daten verschlüsselt?	
	Wie werden die Logins gesichert (z.B. 2nd Pass)?	
	Gibt es Backups?	
	Systemlandschaft und Administration	
	Die Fragen wiederholen sich zum Teil, aber die Fragen sollten unterdessen beantwortet sein:	
	Wo werden die Daten gespeichert?	
	Wie werden die Backups gemacht und wo abgelegt?	
	Wer hat Zugriff auf die Daten + Backups?	
	Welche Firmen haben alles Zugriff auf die Daten (verschlüsselt oder unverschlüsselt)?	

Offen/erledigt	Aufgaben	Bemerkungen
	Backup Disaster Recovery	
	Was passiert, wenn alle Stricke reissen und alle Systeme gleichzeitig ausfallen?	
	Beispiel: Es gibt ein Erdbeben, alle Server / Systeme und PCs fallen aus. Wie lange dauert es, ein komplettes System wieder lauffähig zu bekommen und Arbeitsplätze für die Mitarbeiter zu organisieren (in dem Fall kann die Neubesorgung von PCs/Servern auch massiv erschwert sein).	

	Arbeitsanweisung, Mitarbeiterschulung und Audits	
	Wer schreibt die Arbeitsanweisungen?	
	Werden die Mitarbeiter darauf hingewiesen, wie mit Daten umgegangen werden muss?	
	Wird dies regelmässig geprüft, in welchen Abständen?	
	Wer führt die Schulungen / Audits durch (verantwortliche Person)?	

	Vertraulichkeitserklärung	
	Hat jeder Mitarbeiter die Vertraulichkeitserklärung unterzeichnet?	
	Hat diese auch Bestand, wenn der Mitarbeiter die Firma verlässt?	

Offen/erledigt	Aufgaben	Bemerkungen
	Löschstrategie	
	Wann werden welche Daten vom Kunden gelöscht?	
	Wie ist der Prozess für Anfragen zur Datenlöschung von Personen?	
	Wer ist verantwortlich für die Datenlöschung / Datenauskunft?	

	Bekanntgabe von Daten im Ausland (Kapitel 2 DSG)	
	Liste aller Firmen erstellen	
	Liste von allen Unternehmen erstellen, inkl. Angaben, welche Daten die Firmen zur Verarbeitung erhalten.	
	Dies kann alles Mögliche betreffen, wie:	

	Newsletter Tool, wo die Mailadresse und Namen stehen	
	Online-Speicher, wo Dateien abgespeichert werden können	
	Buchhaltung / Treuhand Unternehmen, welches die Kunden und die Kontoführung sehen können	
	etc.	

Offen/erledigt	Aufgaben	Bemerkungen
	Risikobeurteilung der Daten im Ausland	
	Es muss abgewogen werden, welche Risiken für die Kundendaten entstehen, wenn diese ins Ausland übermittelt werden. Nicht jede ausländische Firma bietet DSG konforme Verträge an.	
	Die Risiken muss jede Firma selbst abwägen. Es ist aber sicherlich weniger tragisch, wenn Name und Mailadresse an ein Newsletter Tool übertragen werden, als wenn Gesundheitsdaten mit Geburtsdatum im Ausland gespeichert werden.	

	Bearbeitung durch Auftragsbearbeiter (Art. 9 DSG)	
	Datenverarbeitungsvertrag	
	Es **muss** ein Datenverarbeitungsvertrag mit allen Firmen, sowohl Inland als Ausland abgeschlossen werden.	
	Gewisse Firmen bieten den Vertrag elektronisch an, andere auf Papier. So oder so sollten alle Verträge aufbewahrt werden und jederzeit einsichtig sein.	
	Sollte eine Datenschutzverletzung bei einer Subverarbeiter auftreten, ist dieser nur haftbar, wenn ein Datenverarbeitungsvertrag geschlossen wurde. Anderenfalls kann man haftbar gemacht werden, für Verletzungen anderer der eigenen Kundendaten!	

Offen/erledigt	Aufgaben	Bemerkungen
	Ausübung der Rechte (Kapitel 4 DSG)	
	Vorlage für die Ausübung der Rechte	
	Wenn eine Person oder Unternehmen die eigenen Daten gelöscht haben möchte, wie soll diese Anfrage eingehen und welche Angaben sind nötig zur Verifikation der Berechtigung?	
	Will man das per Formular oder schriftlichen Antrag? Das muss den Personen mitgeteilt werden, damit diese entsprechend ihre Rechte wahrnehmen können.	

	Bearbeitung der Anfragen	
	wenn eine Löschanfrage eingeht:	

	welche Daten müssen (gesetzlich verpflichtend) aufbewahrt werden?	
	Wie sichert man die Daten vor versehentlichem erneutem Zugriff?	
	welche Daten können und müssen gelöscht werden?	
	wenn eine Auskunft Anfrage eingeht:	
	Wer bearbeitet diese?	
	Wer stellt die Auskunft innert der gesetzlich vorgegebenen Frist zur Verfügung?	

Offen/erledigt	Aufgaben	Bemerkungen
	Informationsschreiben (Art. 19 DSG)	
	Datenschutzbestimmungen	
	Sind die Datenschutzbestimmungen auf der Website aktualisiert?	

	Datenverarbeitungsvertrag	
	Haben Sie mit allen Subunternehmern, mit welchen Sie Daten teilen, einen Datenverarbeitungsvertrag?	
	Bieten Sie Ihren Kunden einen Datenverarbeitungsvertrag an?	

	Kundeninformation	
	Informieren Sie Ihre Kunden darüber!	

	Cookie Banner & Website	
	Datenschutzerklärung Website	
	Ist bereits eine Datenschutzerklärung auf der Website vorhanden?	

	Nur CH-Kunden	
	Kein Cookie-Banner nötig.	

	Auch EU-Kunden	
	Cookie-Banner und Einwilligungen zum Tracking werden benötigt.	

Wir sind keine Rechtsanwälte und geben keine Gewähr auf die obengenannten Angaben.

Der gesamte Prozess ist zeitaufwändig und erfordert viel Zeit und Ressourcen. Dennoch ist dieser Aufwand unvermeidlich, um zukünftig die Sicherheit der Kundendaten zu erhöhen und zu gewährleisten.

Falls Sie Fragen haben oder Unterstützung benötigen, sind wir gerne bereit, Ihnen beizustehen. Auf Wunsch können wir auch einen Rechtsanwalt hinzuziehen, um sicherzustellen, dass Ihre Einhaltung der Datenschutzgrundverordnung (DSG) rechtlich abgesichert ist.

Stefan Murawski hat als ehemaliger IT in grossen und mittleren Unternehmen die Qualifikation und das (technische) Wissen, wie Systemlandschaften und Sicherheitskonzepte ausgearbeitet. Kontakt über fragen@wuk.ch