Datenschutzgesetz ab 01.09.2023 Eco-CHECKLISTE

Ab dem 01. September 2023 wird folgendes Datenschutzgesetz neu eingeführt.

Das Berufsgeheimnis erledigt: ☐ Ja ☐ Nein ☐ später

Personendaten die uns zu beruflichen Zwecken anvertraut werden, halten und bearbeiten wir vertraulich.

10 Grundregeln im Datenschutz: erledigt: ☐ Ja ☐ Nein ☐ später

1. Die Person ist im Vorhinein zu informieren, was mit Ihren Daten passieren wird.
2. Es werden nur die notwendigen Daten angefordert.
3. Die Daten werden nicht zweckwidrig eingesetzt.
4. Was nicht mehr gebraucht wird, wird gelöscht.
5. Man erledigt nur das, was man persönlich auch billigen würde.
6. Eine Person darf sich auch weigern, seine Daten bekannt zu geben.
7. Die Daten werden auf Fehler geprüft.
8. Die Daten werden ausschliesslich aus vertrauten Quellen beschaffen.
9. Sensible Daten werden nicht ohne Autorisierung an Drittpersonen weitergegeben.
10. Es werden Massnahmen getroffen, um die Daten im Betrieb abzusichern.

Verzeichnis der Bearbeitungstätigkeiten: erledigt: ☐ Ja ☐ Nein ☐ später

Unternehmen, die sensible Daten in grossem Umfang bearbeiten oder Hochrisiko-Profiling betreiben oder Unternehmen mit > 250 Mitarbeiter haben folgende Pflicht:

- Führen eines Verzeichnisses Ihrer Aktivitäten, bei denen Personendaten bearbeitet werden (zum Beispiel: Verwaltung der Kundendaten, Personalverwaltung, Buchhaltung, Onlineshop).

Das Verzeichnis muss gemäss Art. 12 revDSG folgendes mindestens beinhalten:

- die Identität des Verantwortlichen
- den Bearbeitungszweck
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten
- die Kategorien der Empfängerinnen und Empfänger
- wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer
- wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8
- falls die Daten ins Ausland weitergegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2.

Datenschutzerklärung erledigt: ☐ Ja ☐ Nein ☐ später

In der Datenschutzerklärung (DSE) muss jede planmässig, gesetzlich nicht erforderliche Beschaffung von Personendaten aufgeführt werden. Die Kunden müssen auf das DSE hingewiesen werden. Ebenfalls muss sie auf der Webseite ersichtlich sein.

Was die Datenschutzerklärung (DSE) alles beinhaltet:

- Von wem ist die DSE (mit Kontaktangaben)
- Wozu werden die Daten benötigt
- An wen werden die Daten weitergereicht (Namensnennung nicht nötig)
- In welche Länger, Kantone oder Regionen gehen die Daten
- Worauf ist das Unternehmen rechtlich gestützt

Auftragsbearbeiter erledigt: ☐ Ja ☐ Nein ☐ später

Falls Sie zur Bearbeitung Ihrer Daten ein IT-Unternehmen oder eine Privatperson Ihre Daten anvertrauen, ist im Voraus ein «ADV» (= Auftragsdatenverarbeitung) Vertrag abzuschliessen, der Ihnen erlaubt, ihn zu steuern und zu kontrollieren.

NEU können Sie den Beizug von Dritten vorab genehmigen oder ihm widersprechen.

Der Vertrag hält die Sicherheitsmassnahmen fest, welche von ihnen zu prüfen sind. Ein ADV nach Art. 28 DSGVO würde genügen, falls der ebenso auf das DSG verweist. Der Auftragsbearbeiter darf nur das tun, was Ihr Unternehmen auch tun dürfte (dazu gehört zum Beispiel keine Datennutzung für sich selbst). Die ADV müssen auf die Richtigkeit geprüft werden.

Datensicherheit & Datenschutz erledigt: ☐ Ja ☐ Nein ☐ später

Verantwortlichkeit der Mitarbeiter thematisieren:

Interne organisatorische Massnahmen werden eingeleitet z.B. Mitarbeiterschulung und -Sensibilisierung, Erlass von Weisungen, Definition von Zuständigkeiten und Prüfung von Logs

Daten werden durch technische Massnahmen geschützt z.B. mit Firewalls, Antimalware-Software, Pseudonymisierung Backups on- und offline

Meldepflicht bei Verletzung erledigt: ☐ Ja ☐ Nein ☐ später

Meldepflicht: Wenn die Vertraulichkeit, Ehrlichkeit oder Bereitstellung von Personendaten verletzt und das Risiko negativer Folgen für einzelne Personen zu hoch (nicht nur lässig) wird, gilt eine Meldepflicht beim Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). (siehe Formular: databreach.edoeb.admin.ch/report)

Daten und Ausland erledigt: ☐ Ja ☐ Nein ☐ später

Hier gilt es die DSGVO Vorschriften zu beachten und allfällige Vorkehrungen zu treffen.

Recht auf Persönlichkeitsschutz erledigt: ☐ Ja ☐ Nein ☐ später

Recht auf Auskunft innert 30 Tagen. Auskunftsbegehren sind schriftlich per Post und unter Beilage einer unterzeichneten Kopie Ihrer Identitätskarte oder Ihres Passes zu stellen.

Recht auf Berichtigung der Daten. Daten sollen möglichst aktuell und richtig gehalten sein. Sollten falsche Personendaten gespeichert sein, werden diese auf Aufforderung hin gerne berichtigt.

Recht auf Widerspruch, wenn diese Verarbeitung nicht zwingend für die Durchführung des Vertrags erforderlich ist, keine gesetzliche Grundlage dafür besteht oder keine überwiegenden oder berechtigten Interessen vorliegen. Dieser Widerspruch tritt sofort in Kraft und gilt für zukünftige Verarbeitungen.

Recht auf Löschung und Einschränkung der persönlichen Daten zu verlangen oder die Verarbeitung einzuschränken, wenn diese Verarbeitung nicht zwingend für die Durchführung des Vertrags erforderlich ist, keine gesetzliche Grundlage dafür besteht (z. B. Aufbewahrungspflichten) oder keine berechtigten Interessen vorliegen.

Recht auf Datenübertragung der Personendaten in einem elektronischen Format oder an einen anderen Verantwortlichen übertragen und/oder herausgeben zu lassen.

Weitere Rechte, wie bei einer möglichen Verletzung der Datenschutzrechte, sich die Person an die zuständige Datenschutzbehörde zu wenden.

Wir verlassen uns nicht auf Einwilligungen erledigt: ☐ Ja ☐ Nein ☐ später

Es sollte sich grundsätzlich nicht auf Einwilligungen verlassen werden. Allfällige Einwilligungen müssen informiert und freiwillig unterzeichnet werden.

Privacy by Default erledigt: ☐ Ja ☐ Nein ☐ später

Wenn Sie irgendwelche Soziale Dienste mit Einstellungen zum Datenschutz haben, werden diese auf das Minimum eingestellt.

Bei Verletzung des Berufsgeheimnisses, kann eine Straffe von bis zu CHF 250'000.00 folgen!

Datenschutz-Folgenabschätzung (DSFA) erledigt: ☐ Ja ☐ Nein ☐ später

Es ist immer eine Datenschutz- Folgenabschätzung (DSFA) zu machen. Bei grossen Risiken ist diese Abschätzung ein Prozess, in dem dokumentiert wird, wie das Risiko zu erkennen, zu bewerten und zu bewältigen ist. Sie ist in allen Fällen aufzubewahren.

Interne Stelle für folgende Anliegen ist:

	Zuständig 1	Zuständig 2
Wenn eine Person ihre Rechte beansprucht:		
Der Datenschutz aufgrund veränderter Situationen geprüft werden muss		
Daten in falsche Hände geraten, verloren gehen, manipuliert werden oder es einen Cyberangriff gibt		