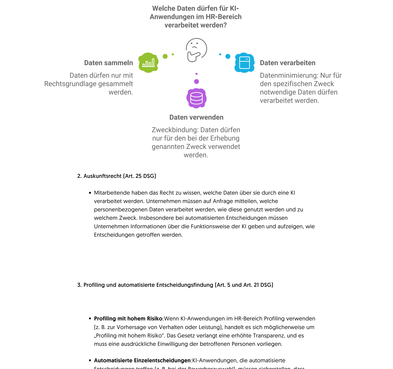
Schweizerisches Datenschutzgesetz

Das schweizerische Datenschutzgesetz (DSG) wurde 2023 revidiert, und es gibt einige spezifische Punkte, die für den Einsatz von KI-Anwendungen, insbesondere in der Personalabteilung, relevant sind. Hier sind die zentralen Aspekte des Schweizer Datenschutzgesetzes im Zusammenhang mit KI-Anwendungen:

1. Prinzipien des DSG und ihre Anwendung auf KI

- **Rechtmässigkeit, Treu und Glauben:** Jede Verarbeitung personenbezogener Daten, auch durch KI-Anwendungen, muss rechtmässig erfolgen und auf Treu und Glauben basieren. Das bedeutet, dass Unternehmen keine Daten ohne Rechtsgrundlage sammeln oder verwenden dürfen.
- **Verhältnismässigkeit:** Die Verarbeitung von personenbezogenen Daten muss verhältnismässig sein, d. h., es dürfen nur diejenigen Daten erhoben werden, die für den spezifischen Zweck notwendig sind (Datenminimierung). Für KI im HR-Bereich bedeutet das, dass nur die für einen Rekrutierungsprozess oder für die Verwaltung von Mitarbeitenden unbedingt erforderlichen Daten verarbeitet werden dürfen.
- **Zweckbindung:** Personenbezogene Daten dürfen nur für den Zweck verwendet werden, der bei ihrer Erhebung genannt wurde. KI-Systeme dürfen diese Daten also nicht für andere als die ursprünglich definierten Zwecke verwenden, z. B. für Marketing oder Profiling.

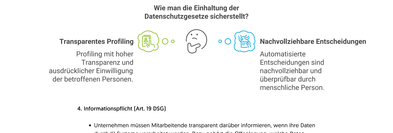


2. Auskunftsrecht (Art. 25 DSG)

- Mitarbeitende haben das Recht zu wissen, welche Daten über sie durch eine KI verarbeitet werden. Unternehmen müssen auf Anfrage mitteilen, welche personenbezogenen Daten verarbeitet werden, wie diese genutzt werden und zu welchem Zweck. Insbesondere bei automatisierten Entscheidungen müssen Unternehmen Informationen über die Funktionsweise der KI geben und aufzeigen, wie Entscheidungen getroffen werden.

3. Profiling und automatisierte Entscheidungsfindung (Art. 5 und Art. 21 DSG)

- **Profiling mit hohem Risiko:** Wenn KI-Anwendungen im HR-Bereich Profiling verwenden (z. B. zur Vorhersage von Verhalten oder Leistung), handelt es sich möglicherweise um „Profiling mit hohem Risiko". Das Gesetz verlangt eine erhöhte Transparenz, und es muss eine ausdrückliche Einwilligung der betroffenen Personen vorliegen.
- **Automatisierte Einzelentscheidungen:** KI-Anwendungen, die automatisierte Entscheidungen treffen (z. B. bei der Bewerberauswahl), müssen sicherstellen, dass diese Entscheidungen nachvollziehbar sind und betroffene Personen die Möglichkeit haben, die Entscheidung von einer menschlichen Person überprüfen zu lassen. Eine rein automatisierte Entscheidung ohne menschliches Eingreifen ist problematisch und kann unter Umständen unrechtmässig sein, es sei denn, die betroffene Person hat ausdrücklich eingewilligt.



4. Informationspflicht (Art. 19 DSG)

- Unternehmen müssen Mitarbeitende transparent darüber informieren, wenn ihre Daten durch KI-Systeme verarbeitet werden. Dazu gehört die Offenlegung, welche Daten gesammelt werden, zu welchem Zweck und wie die KI diese Daten verarbeitet. Besonders bei sensiblen Daten, wie sie im HR-Bereich oft vorkommen, ist eine umfassende Information erforderlich.

5. Datensicherheit (Art. 8 DSG)

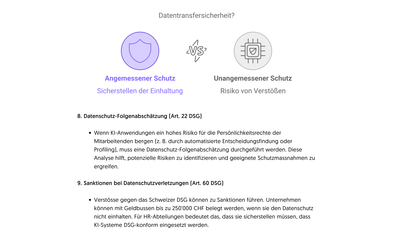
- Unternehmen müssen technische und organisatorische Massnahmen treffen, um die Datensicherheit zu gewährleisten. Bei KI-Anwendungen bedeutet dies, dass die Systeme vor unbefugtem Zugriff, Datenverlust und Missbrauch geschützt werden müssen. Dazu gehören verschlüsselte Datenspeicherung, Zugriffsmanagement und regelmässige Audits der Sicherheitssysteme.

6. Verarbeitung von besonders schützenswerten Daten (Art. 5 DSG)

- Im HR-Bereich wird häufig mit besonders schützenswerten Daten gearbeitet, wie Gesundheitsdaten oder Daten zu religiösen Überzeugungen. Diese Daten dürfen nur unter strengen Voraussetzungen verarbeitet werden, und KI-Anwendungen, die diese Daten analysieren oder verarbeiten, müssen sicherstellen, dass eine ausdrückliche Einwilligung der betroffenen Person vorliegt oder eine gesetzliche Grundlage gegeben ist.

7. Datenübermittlung ins Ausland (Art. 16–17 DSG)

- Wenn KI-Anwendungen in der Schweiz personenbezogene Daten ins Ausland übermitteln (z. B. an eine Cloud oder ein Rechenzentrum in einem anderen Land), muss das Unternehmen sicherstellen, dass im Zielland ein ausreichendes Datenschutzniveau vorhanden ist. Dies gilt insbesondere für Drittstaaten ausserhalb der EU, die nicht dem Europäischen Datenschutzstandard entsprechen.



8. Datenschutz-Folgenabschätzung (Art. 22 DSG)

- Wenn KI-Anwendungen ein hohes Risiko für die Persönlichkeitsrechte der Mitarbeitenden bergen (z. B. durch automatisierte Entscheidungsfindung oder Profiling), muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Diese Analyse hilft, potenzielle Risiken zu identifizieren und geeignete Schutzmassnahmen zu ergreifen.

9. Sanktionen bei Datenschutzverletzungen (Art. 60 DSG)

- Verstösse gegen das Schweizer DSG können zu Sanktionen führen. Unternehmen können mit Geldbussen bis zu 250'000 CHF belegt werden, wenn sie den Datenschutz nicht einhalten. Für HR-Abteilungen bedeutet das, dass sie sicherstellen müssen, dass KI-Systeme DSG-konform eingesetzt werden.

Fazit

Für den Einsatz von KI im HR-Bereich in der Schweiz sind Transparenz, Datensicherheit, das Recht auf Auskunft, die Vermeidung von Diskriminierung und die Einhaltung der Zweckbindung entscheidend. Besonders im Fokus stehen automatisierte Entscheidungen, Profiling sowie die Verarbeitung von sensiblen Daten, die durch das neue DSG stärker reglementiert werden.
Diese Punkte kannst du in deinem Workshop verwenden, um den Teilnehmern die spezifischen Anforderungen des Schweizer Datenschutzgesetzes für KI-Anwendungen verständlich zu machen.

Warum ist es kritisch, datenschutzgeschützte Daten in eine Cloud einzugeben?

1. Verlust der Kontrolle:
- Sobald Daten in die Cloud geladen werden, liegen sie nicht mehr vollständig unter der Kontrolle des Unternehmens. Es gibt keine direkte Kontrolle über, **wer auf die Daten zugreifen** kann oder wo sie gespeichert werden.

2. Datenzugriff durch Dritte:
- Cloud-Anbieter oder ihre Mitarbeitenden könnten **Zugriff auf sensible Daten** haben, selbst wenn dies nicht beabsichtigt ist. Wenn nicht klar geregelt ist, wer Zugriff hat, können Datenschutzverletzungen entstehen.

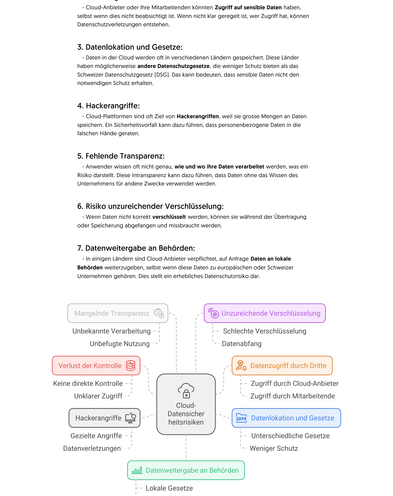
3. Datenlokation und Gesetze:
- Daten in der Cloud werden oft in verschiedenen Ländern gespeichert. Diese Länder haben möglicherweise **andere Datenschutzgesetze**, die weniger Schutz bieten als das Schweizer Datenschutzgesetz (DSG). Das kann bedeuten, dass sensible Daten nicht den notwendigen Schutz erhalten.

4. Hackerangriffe:
- Cloud-Plattformen sind oft Ziel von **Hackerangriffen**, weil sie grosse Mengen an Daten speichern. Ein Sicherheitsvorfall kann dazu führen, dass personenbezogene Daten in die falschen Hände geraten.

5. Fehlende Transparenz:
- Anwender wissen oft nicht genau, **wie und wo ihre Daten verarbeitet** werden, was ein Risiko darstellt. Diese Intransparenz kann dazu führen, dass Daten ohne das Wissen des Unternehmens für andere Zwecke verwendet werden.

6. Risiko unzureichender Verschlüsselung:
- Wenn Daten nicht korrekt **verschlüsselt** werden, können sie während der Übertragung oder Speicherung abgefangen und missbraucht werden.

7. Datenweitergabe an Behörden:
- In einigen Ländern sind Cloud-Anbieter verpflichtet, auf Anfrage **Daten an lokale Behörden** weiterzugeben, selbst wenn diese Daten zu europäischen oder Schweizer Unternehmen gehören. Dies stellt ein erhebliches Datenschutzrisiko dar.



Diese Punkte machen deutlich, warum es riskant ist, datenschutzgeschützte Daten in eine Cloud einzugeben, und welche Risiken Anwender dabei beachten müssen. Die meisten KI Anwendungen die wir täglich brauchen, sind Cloud basiert.