Bern, im Mai 2023

Q&A zum revidierten Datenschutzrecht

Was sind die grundlegendsten Änderungen per 1. September 2023?

- Wer Daten bearbeitet, muss ein Bearbeitungsverzeichnis führen
- Für jede Datensammlung muss es eine datenschutzverantwortliche Person geben
- Datenschutz muss durch Technik sichergestellt sein (Zugriffsrechte auf Dokumente, verschlüsselte Mails)
- Wer Daten bearbeitet, muss Betroffene informieren und auf Anfrage Auskunft erteilen
- Daten müssen so abgelegt sein, dass sie brauchbar reproduziert und auch versandt werden können («Datenportabilität», z. B. als PDF oder Excel)
- Neu ist die Datenlöschung ausdrücklich geregelt: wer Daten bearbeitet, muss sie auch rechtzeitig wieder löschen
- Androhung bei absichtlichen Verstössen: Busse bis zu CHF 250'000.00 möglich

Ist eine datenschutzverantwortliche Person zwingend?
Im Gesetz ist immer wieder die Rede von «Datenverantwortlichen». Daher muss eine solche Person für alle Datensammlungen existieren, welche die (Mit-)Verantwortung trägt und als Ansprechperson dient (auch für Behörden und Gerichte).

Welche Anforderungen muss die datenschutzverantwortliche Person erfüllen?
Es bestehen keine gesetzlichen Vorgaben. Aus den Umständen ergibt sich, dass die Person Zugang zu allen Datensammlungen/-bearbeitungen haben und über das nötige Fachwissen verfügen muss. Fachwissen bedeutet Kenntnisse im Datenschutzrecht sowie IT.

Müssen Betriebe mit weniger als 250 Mitarbeitenden ein Bearbeitungsverzeichnis führen?
Gemäss Art. 24 nDSV sind Betriebe mit weniger als 250 Mitarbeitenden von dieser Pflicht befreit, ausser wenn besonders schützenswerte Personendaten im grösseren Umfang bearbeitet werden. Da Gesundheitsdaten als besonders schützenswert gelten, sind Therapeut*innen verpflichtet, ein Verzeichnis zu führen.

Wie müssen Therapeut*innen ihre Kunden informieren?
Das nDSG gibt nicht vor, wie betroffene Personen informiert werden müssen. In der Praxis sind Datenschutzerklärungen zu empfehlen, ausreichend ist aber auch eine Information in den AGB, ein Einwilligungsformular oder eine mündliche Information (z. B. Tonbandansage). Ungenügend ist dagegen die blosse Angabe einer Kontaktperson für weitere Fragen.
Ob die betroffene Person die Datenschutzerklärung tatsächlich anschaut, spielt keine Rolle.

OdA ARTECURA
Rainweg 9H, 3068 Utzigen
071 330 01 00, info@artecura.ch, www.artecura.ch

Was muss an der eigenen Website geändert werden?
Die betroffenen Personen müssen neu über die Datenbearbeitung informiert werden. Daher sollte eine Datenschutzerklärung auf der Website aufgeschaltet werden, welche einfach zu finden ist (es muss aber nicht eine Einverständniserklärung aufpoppen).

Muss auf Visitenkarten, in E-Mails usw. auf die Datenschutzerklärung hingewiesen werden?
Sofern die Datenschutzerklärung auf der Website gut zugänglich und erkennbar ist, muss in Alltagssituationen wie etwa bei einer Terminvereinbarung am Schalter oder per E-Mail nicht auch noch auf die Datenschutzerklärung hingewiesen werden. Denn der betroffenen Person ist zuzumuten, dass sie die Datenschutzerklärung auf der Website abruft.

Müssen Arbeitnehmende informiert werden?
Durch Art. 328b OR besteht eine gesetzliche Grundlage für die Datenbearbeitung von Arbeitnehmenden. Trotzdem wird empfohlen, im Arbeitsvertrag oder im Personalreglement auf die Datenschutzerklärung explizit hinzuweisen.

Wann ist eine Übermittlung an Dritte erlaubt?
Sofern die Datenbearbeitung rechtmässig ist, den datenschutzrechtlichen Grundsätzen entspricht und die betroffenen Personen über die Weiterleitung informiert sind.

Dürfen Rechnungen, Berichte usw. per E-Mail an Klienten/Krankenversicherungen versendet werden?
Hier sind technische Massnahmen zu ergreifen, damit keine unberechtigten Dritte die Daten einsehen können. Dies kann z. B. durch eine Verschlüsselung erreicht werden (z. B. mit HIN-Mail). Bei höchstpersönlichen Daten sollte immer das explizite Einverständnis vorliegen oder noch besser der Transfer via betroffene Person erfolgen.

Wann müssen Verletzungen der Datensicherheit dem EDÖB gemeldet werden?
Eine Verletzung liegt dann vor, wenn die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten beeinträchtigt wird, also Personendaten gelöscht, verloren, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden. Gemeldet werden müssen aber nur solche Verletzungen, die ein hohes Risiko für negative Folgen für die betroffenen Personen aufweisen.

Was muss ich tun, wenn ich eine Mail an den falschen Adressaten sende oder einen Stick mit Daten verliere?
Es ist eine Einzelfallbeurteilung nötig, ob eine Meldung an den EDÖB nötig ist. Wird z.B. eine E-Mail mit Personendaten falsch an eine Person versendet, die vertrauenswürdig und dem*der Sender*in bekannt ist, besteht kein hohes Risiko. Geht dagegen ein Stick mit Mitarbeiterdaten und deren Gehälter verloren, ist eine Meldung erforderlich.

Welche Folgen hat ein Verstoss gegen die neuen Vorschriften?
Bei vorsätzlichem (absichtlichem) Handeln bzw. Unterlassen droht eine Busse von bis zu CHF 250'000.00, und zwar als Privatperson. Fahrlässigkeit wird dagegen nicht bestraft. Sanktioniert werden also nur jene, die nicht die minimalen Massnahmen zur Datensicherheit treffen. Ausnahmsweise kann der Geschäftsbetrieb bis zu CHF 50'000.00 gebüsst werden, wenn die Ermittlung der natürlichen Person mit einem unverhältnismässigen Aufwand verbunden ist.
Nur auf Antrag bestraft werden die Missachtung von Informations-, Auskunfts- und Meldepflichten sowie die Verletzung von Sorgfaltspflichten und der beruflichen Schweigepflicht.