

Fragen und Antworten zu **Reglement Schutz von Daten**

Stand 25.8.2026 > Weitere Fragen bitte fortlaufend an Yves (Datenschutzkoordinator RADIX) richten.

Kapitel	Fragen	Antworten
4	Wenn eine Person ein Heft des SuchtMagazin kauft, kopieren wir die Mailadresse standardmässig in den Verteiler für den SuchtMagazin-Newsletter (4 x pro Jahr). Ich gehe davon aus, dass wir ein Opt-In einrichten müssen. Richtig? (MR)	Spezifische Abklärungen bitte immer direkt mit Datenschutz-Koordinator besprechen.
5	Aufbewahrungsfristen: Wir bearbeiten grundsätzlich fast keine RADIX-Daten, sondern "nur" eigene Projektdaten für unseren Auftraggeber. Dessen Datenschutzvorgaben geben andere Fristen und Vorgaben vor. Diese sind für uns verpflichtend. Wie wird sichergestellt, dass dessen Datenschutzvorgaben übergeordnet gelten und angewendet werden?	Korrekt. Daten von Auftraggebern können anderen Datenschutzvorgaben entsprechen. RADIX ist für die Einhaltung der eigenen Datenschutzvorgaben verantwortlich. Das Gleiche gilt für den Auftraggeber. Gibt der Auftraggeber Datenschutzvorgaben vor, halten wir diese selbstverständlich ein. Der Auftraggeber ist für die Überprüfung der Einhaltung verantwortlich.
	Dienstleistungsverträge/Kooperationsvereinbarungen/Leistungsvereinbarungen Kanton: Aufbewahrungsdauer 10 Jahre gemäss OR. Dürfen sie auch länger aufbewahrt werden oder müssen sie nach 10 Jahren vernichtet werden? Und wenn sie vernichtet werden müssen: auch die digitalen Ablagen?	Sie dürfen länger aufbewahrt werden (z.B. laufende Rechtsverfahren, gesetzliche Sonderpflicht). Den Antrag zur längeren Aufbewahrung stellt die Leitung des Kompetenzzentrums bei der Geschäftsleitung, mit Begründung. Der Stiftungsrat entscheidet dann bzgl. der längeren Aufbewahrung. Bei eigenen

Kapitel	Fragen	Antworten
		Rechtsformen liegt die Entscheidung bei deren Stiftungsräten, rsp. Vorständen.
	Geschäftskorrespondenz (inkl. Emails) müssen 10 Jahre aufbewahrt werden. Mails werden zukünftig nach 15 Monaten gelöscht. Welche Mails zählen alles zur Geschäftskorrespondenz und müssen separat abgelegt werden?	Nach 2 Jahren werden die Mails automatisch gelöscht. Geschäftskorrespondenz dient der Abwicklung wichtiger Geschäftsabläufe, v.a. auf strategischer Ebene. Beispiele: Vertragsverhandlungen, Auftragsbestätigungen oder wichtige Behördenkorrespondenz. Diese Mails sollen im R-Laufwerk abgelegt werden. Andere, operative Korrespondenz, wie z.B. Projektkorrespondenz, Austausch mit Akteuren, Swiss-Support, interne Korrespondenz etc. muss nicht gespeichert werden.
	Präzisierung, welche Kompetenzzentren betroffen sind (z.B. Psychotherapeutische / medizinische Daten)?	Es gilt für alle, die mit entsprechenden Daten zu tun haben.
6	Bräuchte es hier eine Klärung, dass es nur um Radix-Daten geht? Und nicht um Daten aus den einzelnen Projekten? Klienten etc. ist in diesem Zusammenhang missverständlich.	Klienten haben wir im Zentrum für Spielsucht, d.h. Einzelpersonen, die unser Beratungsangebot nutzen. Auch diesen steht das Recht der betroffenen Personen zu. Projekt- wie auch Klientendaten sind auch RADIX-Daten.
	So können Kunden, Auftraggebende.... ihre Rechte geltend machen: Mail an info-zh@radix.ch. Dies gilt nur für RADIX-Daten und wird für die von uns bearbeiteten, eigenen Daten separat geregelt.	Die E-Mail info-zh@radix.ch gilt für Rechteanfragen (Auskunft, Löschung usw.) und für die Meldung von Verstössen durch Kunden, Auftraggebende. Bei SGE und VP (eigene Rechtsformen) kann hier in Absprache mit der GL eine eigene Adresse angegeben werden. RADIX-Mitarbeitende wenden sich an die Vorgesetzte oder direkt an den internen Datenschutzkoordinator.
8	Gilt es auch als Datenschutzverletzung, wenn eine Mail ohne sensible Inhalte an eine falsche Person verschickt wird? (z.B. eine Sitzungseinladung oder die Bitte um ein Logo o.ä.)	Technisch gesehen liegt eine Datenschutzverletzung vor. Das Risiko ist in der Regel gering. Trotzdem: intern dokumentieren und die zuständige Person für Datenschutz des Kompetenzzentrums informieren und dokumentieren.
	Umgang in bundesnahen Projekten? Die Mitarbeitenden müssen an wen melden, damit sie ihrer Meldepflicht nachkommen? In welcher Frist? Was geschieht, wenn der Datenschutzberater abwesend oder nicht erreichbar ist. Bzw. gibt es einen/eine Stv?	Die Meldung erfolgt umgehend an die Vorgesetzte sowie den internen Datenschutzkoordinator. Stellvertretend fungieren die stv. Leitung des Kompetenzzentrums und die Geschäftsführerin. Diese nehmen zusammen mit dem externen Datenschutzberater sofort eine Risikobewertung vor und je nach Resultat erfolgt eine

Kapitel	Fragen	Antworten
		sofortige Meldung durch die Verantwortlichen (Datenschutzkoordinator/Datenschutzberater) an den Auftraggeber/die Auftraggeberin. Diese entscheidet dann über Meldung und weitere Handhabung. Die Frist und der Meldeweg oder auch Stellvertretung werden vom Auftraggeber des Projektes festgelegt.
9	Unsere Vertragspartner (Gemeinden) haben Zugriff auf den internen Bereich der jeweiligen Gemeinde mit den Personendaten der Freiwilligen und können diese bearbeiten und herunterladen. Ebenso alle Freiwilligen. Was bedeutet dies zukünftig? Müssen diese alle eine Erklärung / einen Vertrag unterschreiben (wht nicht umsetzbar mit den Freiwilligen FW)? Oder müssen wir diesen Zugang wieder verunmöglichen und alle Änderungen wieder selbst vornehmen und verschicken? (und falls ja: in welcher Form dürfen diese dann verschickt werden an die Freiwilligen und Gemeinden??) Präzisierung zu Zeile 9 (dieses Dokument), Punkt 9 (Reglement): Es geht um den internen Bereich der Webseite zämegolaufe.ch, dort haben die Gemeinden und die Freiwilligen einen Zugang mit Benutzername und Passwort. In diesem Bereich werden auch die Personendaten der Freiwilligen erfasst und verwaltet und können als Excel-Tabelle heruntergeladen werden (nur von jenen mit einem Login für den jeweiligen Standort). Es geht hier nicht um den Sharepoint, Teams oder OneDrive. Die Nutzung dieser Kanäle ist für die Arbeit mit den Freiwilligen mehrheitlich ungeeignet, auch für das Teilen von Zugangsdaten, da doch so einige dafür zu wenig IT-affin sind (alle 60+) Was bedeutet "Ist die Vertraulichkeitsverpflichtung der mandatierten Organisationen vorhanden"?	Alle mit Zugang zum internen Bereich unterschreiben eine Nutzungsvereinbarung und stimmen den Regeln zu. Bei der Anmeldung erscheint einmalig eine Checkbox. Wer das Kästchen ankreuzt, stimmt den «Spielregeln» zu. Wer nicht ankreuzt, erhält keinen Zugang. Die Spielregeln: Zweck des Zugriffs ist die Koordination der Freiwilligen am Standort, Daten sind vertraulich zu behandeln, keine Weitergabe an Dritte, Daten nur für diesen Zweck nutzen, bei Vertragsende Daten löschen oder zurückgeben. Die Zugriffsberechtigungen im internen Bereich werden je nach Rolle eingeschränkt. Nicht alle dürfen dasselbe. Die Checkbox ist von vielen Webseiten bekannt. Freiwillige merken nichts ausser der Checkbox bei der Registrierung. Für die Umsetzung mit Umbraco bitte mit Yves Kontakt aufnehmen. Eine Vertraulichkeitsverpflichtung hält fest, dass sensible Informationen, Geschäftsgeheimnisse oder Daten nicht an Dritte weitergegeben oder zweckentfremdet verwendet werden sollen. Als beauftragte Organisationen unterliegen auch wir als Auftragnehmerin dieser Vertraulichkeitsverpflichtung. Handeln wir als Auftraggeberin und vergeben einen Auftrag, unterliegen unsere Partner-Organisationen und Dienstleister ebenfalls dieser Vertraulichkeitsverpflichtung.

Kapitel	Fragen	Antworten
14	Wechselmedien - USB-Sticks und andere Wechselmedien müssen von der Geschäftsleitung freigegeben werden. - Private USB-Sticks dürfen nicht an geschäftlichen Geräten verwendet werden. - Gefundene USB-Sticks oder Speichermedien von externen Personen/Organisationen dürfen nicht angeschlossen werden. - Wechselmedien mit Personendaten müssen verschlüsselt werden. - Die Nutzung muss protokolliert werden.	Ja, dem ist so. Heute findet fast alles in der Cloud statt (Sharepoint, OneDrive). Der Einsatz von USB-Sticks oder andere Wechselmedien ist daher seltener geworden. Mit Wechselmedien sind Kosten verbunden. Zudem stellen diese eine grössere Gefahr da. Die Freigabe zur Nutzung ist schriftlich bei der Geschäftsleitung zu beantragen, Die Nutzung im Protokoll festzuhalten (Datum, Person, Zweck). Verschlüsselung des Inhaltes gemäss IT-Vorgabe (z.B. mit BitLocker)
Allg.	Beide Docs beziehen sich auf alle Kompetenzzentren, obwohl bspw. Die SGE meines Wissens nach keinem Zugriff zu besonders schützenswerten Daten hat. Was sind die Überlegungen, dass das Reglement dann trotzdem auch für die SGE gilt?	Beide Dokumente sind für alle MA in allen Kompetenzzentren gültig. Ein Inzident in einem Kompetenzzentrum betrifft die gesamte Stiftung. Die Pflichten richten sich nach der Art der Daten: Wer keine besonders schützenswerten Daten bearbeitet, erfüllt das Reglement mit weniger Aufwand. Je nach Auftrag kann sich die Datenlage verändern, dies kann auch die SGE betreffen (z.B. Anfragen von Personen an die SGE per Mail, KI ...).
Allg.	Wir haben ja das Umfragetool "SurveyMonkey". SM nutzt Rechenzentren in den USA. Gäbe es Alternativen? Bei einfachen Umfragen SPRINT aber wenn es etwas komplexer ist? Wie wäre es z.B. mit LimeSurvey?	Solche Hinweise sind sehr wertvoll. Bitte immer an den Datenschutzkoordinator adressieren, sie werden unabhängig von den Reglementen bearbeitet.