

Fragen und Antworten zu Reglement Umgang mit Daten

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

Kapitel	Fragen	Antworten
1	Social Media: die SoMe-Kanäle (z.B. Facebook (META) sowie LinkedIn sind ja jeweils mit privaten Profilen verknüpft (technisch nicht anders lösbar). Was bedeutet das konkret für die Personen in den jeweiligen Kompetenzzentren, deren private Accounts, mit denen des Kompetenzzentrums verknüpft ist. Ist hier eine Veränderung/Anpassung geplant?	Da es keine Verbindung zu unseren Daten gibt und wir bestimmen, welche Daten wir vermitteln, wird es wie bisher gehandhabt. Wichtig zu beachten ist dabei der Umgang mit Bildern, siehe hier: R:\ALLGEMEIN\6_BILDER . Siehe zudem nächste Antwort.
	Private Nutzung lässt sich bei Social Media technisch nicht von der dienstlichen Nutzung trennen. Wie ist damit umzugehen. (Geschäftskonten und Kanäle sind immer an irgendwelche Privaten Account geknüpft)	Social media-Handy über das Projektbudget mit eigener Telefonnummer via Daniel besorgen. Alternativ Social Media über Computer erstellen. Thomas für eine Telefonnummer zur Authentifizierung (MFA) anfragen. Man kann einen "privaten Account" erstellen und diesen leer lassen. Damit kann auch eine Businessseite erstellt werden. Wichtig ist, dass man als Telefonnummer die von Thomas erstellte Nummer (sms-gateway) benutzt, sonst gelangen die Anfragen zur MFA an die private Nummer.

Kapitel	Fragen	Antworten
	Darf WhatsApp für Beratungen genutzt werden? Wie sieht es mit WhatsApp-Kanal aus?	Wichtig zu wissen: WhatsApp Daten werden über die Infrastruktur von Meta verarbeitet. Eine nachträgliche Löschung von Daten ist nur eingeschränkt möglich. Grundsätzlich kann WhatsApp für Beratungen genutzt werden. Allerdings müssen die datenschutzrechtlichen Anforderungen eingehalten werden. Es muss immer eine Einwilligung der Ratsuchenden eingeholt werden. Es muss vorab geklärt und dokumentiert werden, wie die Einwilligung erfolgt. Müssen Ratsuchende informiert werden? Ja. Sie müssen über die Datenbearbeitung informiert werden. Welche Daten sollen Ratsuchende nicht übermitteln? Besonders schützenswerte Personendaten wie Gesundheitsdaten sollen nicht über WhatsApp gesendet werden. Für Beratungen nie die private, sondern immer eine separate Geschäftsnummer verwenden. D.h. WhatsApp Business mit einer geschäftlichen Telefonnummer verwenden. WhatsApp Kanäle mit einer einseitigen Kommunikation (wir senden) sind gut geeignet. Hierzu keine Personendaten übermitteln und Bildrechte berücksichtigen.
	WhatsApp wird von unseren "Kunden" bevorzugt genutzt. Oft werden uns so auch Personendaten zugestellt. Wir dürfen solche also empfangen, aber keine senden (wie z.B. eine Natelnummer o.ä., also keine sensiblen Daten)? Das wird für die Kunden schwierig zu verstehen sein.	1) Kunden werden aktiv auf den korrekten Kommunikationskanal hingewiesen (z.B. E-Mail). Dieser Hinweis erfolgt einmalig und klar. UND 2) Werden Personendaten unaufgefordert via WhatsApp zugestellt, werden diese nicht in WhatsApp weiterbearbeitet. Die weiteren Schritte erfolgen über den vorgesehenen Kanal.

Kapitel	Fragen	Antworten
		Telefonnummern gelten als Personendaten, d.h. schützenswerte Daten. Für einen anderen Ansatz ist ein schriftliches Gesuch mit Begründung (Dokumentation) der Ausnahme an die GL möglich.
	WhatsApp: wir nutzen unsere privaten Accounts für die Arbeit (Kommunikation mit den FW) - also nicht nur eine Verknüpfung, sondern den effektiven Account. WhatsApp lässt die Nutzung von zwei Accounts auf die gleiche Telefonnummer nicht zu. Die private Nutzung lässt sich daher nicht trennen von der dienstlichen. Wie sollen wir dies handhaben?	Option eines Whatsapp business Accounts prüfen oder Social media/whatsapp-Handy über das Projektbudget besorgen. Fürs Handy mit Daniel absprechen und für die Telefonnummer mit Thomas.
2/3	Wo befindet sich der interne Verhaltenskodex und das Dokument zu den Bildrechten?	R:\ALLGEMEIN\8_KI\VERHALTENSKODEX R:\ALLGEMEIN\6_BILDER\BILDNUTZUNG Ein Handbuch mit allen Reglementen folgt 2027, bis dahin sind alle Unterlagen unter Allgemein abgelegt.
	Bilderstellung mit KI: Die Erstellung von Bildern mit Co-Pilot ist unzufriedenstellend. Andere KI-Tools (ChatGPT, Gemini) liefern hier deutlich bessere Ergebnisse (auch mit deutlich weniger Zeitaufwand), dürfen aber nicht mehr verwendet werden. Wenn ich mit meinem privaten Account und auf einem privaten Rechner ein Bild erstelle und mir dieses dann selber per Mail zusende. Kann ich dieses dann verwenden? (z.B. für Infomaterialien oder SoMe-Beiträge)? Falls die Antwort "nein" ist: Ist die Einführung anderer KI-Tools zur Erstellung von Bildern geplant?	ja, ein Bild, das auf einem privaten Gerät oder Tagungs-/Website-Notebook erstellt wurde, darf weitergeleitet werden. Ergänzung: wenn Apps oder Tools notwendig sind, können diese beantragt werden. Wichtig ist, dass wir den Überblick haben und dass diese regelmässig "gewartet" (updates ...) werden. Also eher nur für Ausnahmefälle geeignet. R:\ALLGEMEIN\2_REGLEMENTE\ANTRÄGE
3	Bildrechte: bei jeder Erkennbarkeit von Personen, das Einverständnis einholen, und nur eigene Bilder verwenden ist für die Bewirtschaftung von Social Media (z.B. Instagram) ist nicht umsetzbar. Wir haben aber einen externen Auftrag einen Social Media Account zu bewirtschaften. Wie ist damit umzugehen?	Lizenzfreie oder Stockbilder sind möglich, dazu braucht es ein Abo. Bitte bei Silvia Fasani nachfragen.
4	Clear Desk Policy: Müssen Dokumente und Geräte (z. B. Notebooks) in abschliessbare Schränke verräumt werden? Falls ja, wie wird	Dokumente mit Personendaten und besonders schützenswerten Daten sind einzuschliessen. Wo kein abschliessbarer Schrank vorhanden ist,

Kapitel	Fragen	Antworten
	festgelegt, was bei Dokumenten eingeschlossen werden muss. Abschliessbare Schränke fehlen	gilt: Bürotür schliessen und abschliessen. Ziel ist es, externen Dritten den Zugriff auf Radix-Daten und geschäftlichen Geräten so schwer wie möglich zu machen.
5	Der Punkt "Browser dürfen keine Passwörter speichern" stelle ich mir sehr umständlich und mit höherem verbundenem aufwand vor. Gilt der Punkt auch für Logins, wo keine besonders schützenswerten Daten gespeichert sind. Denn Passbolt ist teils sehr verschachtelt und langsam. Bsp: Ich nutze Umbraco täglich. Dabei werde ich bei wenigen Minuten inaktivität automatisch ausgeloggt. Dann nutze ich das gespeicherte Passwort, um den Umweg über passbolt zu umgehen. ähnlich mache ich es für social media, google analytics, mailchimp und viele weitere tools, die über den browser genutzt werden.	siehe unten. Eine pragmatische Lösung für die Arbeit mit Umbraco bitte mit Yves besprechen.
	Hier heisst es: "Browser dürfen Passwörter nicht speichern." Gilt das für alle Anwendungen? Auch für Antragsplattformen für Gesuche wie z. B. Promotion digitale von Gesundheitsförderung Schweiz?	Grundsätzlich immer Passbolt nutzen. Einfaches Handling über Browser : passbolt.radix.ch - Passwort und Code einmal eingeben, <u>Häkchen "bis zum Logout merken" setzen</u> - ODT fakultativ wählen - danach direkt auf URL klicken.
	Zugriffsrechte externer Personen: die FW und die Kontaktpersonen der Standorte haben Zugriff auf den jeweiligen internen Bereich der Webseite. Müssen wir diesen zukünftig zeitlich begrenzen und dann die Passwörter ändern und allen neu zukommen lassen? Oder ist dies ein Fall, wo ein Gesuch für eine Ausnahmeregelung an die GL gestellt werden kann?	Alle mit Zugang zum internen Bereich stimmen der Nutzungsvereinbarung zu. Bei der Anmeldung erscheint einmalig eine Checkbox. Wer das Kästchen ankreuzt, stimmt den Spielregeln zu. Wer nicht ankreuzt, erhält keinen Zugang. Die Spielregeln: Zugriff nur zur Koordination der Freiwilligen am Standort, Daten vertraulich behandeln, keine Weitergabe an Dritte, Daten nur für diesen Zweck nutzen, bei Vertragsende können Daten gelöscht oder zurückgegeben werden. Die Zugriffsrechte 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 an Yves wenden.
6	Software für Online-Videokonferenz = MS Teams. Können andere Lösungen (wie z.B. Zoom) weiterhin genutzt werden, da dies keine Software-Installation benötigen. Brauchen solche ebenfalls eine Genehmigung der Geschäftsleitung und dies immer?	Bekannte, webbasierte Tools (Zugang über Web-Browser), die nicht installiert werden müssen, können genutzt werden.

Kapitel	Fragen	Antworten
	Unverschlüsselte E-Mail-Kommunikation ist nur für allgemeine Information zulässig. Beinhaltet dies auch Personen-, also Kontaktdaten?	Reine Kontaktdaten (Name, E-Mail-Adresse, Telefonnummer, Postadresse) gelten nicht als besonders schützenswerte Personendaten. Der unverschlüsselte Versand ist deshalb grundsätzlich zulässig. Voraussetzung: Es liegen keine zusätzlichen besonders schützenswerten Personendaten vor, vgl. dazu die Datenklassifikation, S. 2 im Dokument «Reglement zum Schutz von Daten. Beim Vorhandensein von besonders schützenswerten Personendaten ist die E-Mail-Kommunikation zu verschlüsseln.
8	Schützenswerte Personendaten: RADIX SharePoint (OneDrive), Teams --> Ist noch aktuell, dass grössere Datenablagen mit Externen nur via Teams oder Sharepoint geteilt werden sollen und nicht über das "eigene" OneDrive? Begründung war, dass so die Datenablage bei Ausfall oder Kündigung an andere Mitarbeitende "übertragen" werden kann.	Ja, das ist richtig und gilt für alle Dokumente. OneDrive ist persönlich und bei einem Personalwechsel gehen diese Daten verloren. Deshalb ist OneDrive ein Zwischenspeicher. Bitte alle relevanten Dokumente unter R speichern. Dies ist unser relevanter, gesicherter und unabhängiger Speicher mit Backup.
	«Nicht schützenswerte Daten: Andere genehmigte Cloud-Anbieter (z. B. Dropbox) .» Lesquels sont agréés exactement? Google Docs?	Eine Webanwendung wie Google Docs ist geeignet. Was Dropbox betrifft, prüft bitte, ob dies wirklich notwendig ist oder ob ein Teams-Kanal, ein freigegebener Ordner auf OneDrive oder ein separater Ordner auf SharePoint RADIX (der von Thomas eingerichtet werden muss) ausreicht.
11	Geschäftliche E-Mail-Nutzung: Ablegen von wichtigen Mails auf dem Server : Bei der Mehrheit der Mails, die ich in Ordnern ablegen will, ist der Name «ungültig»; d.h. die Mails enthalten vermutlich Zeichen, die nicht Explorer-kompatibel sind.	Es ist sinnvoll, die Mails beim Speichern auf R mit Stichworten neu zu benennen, so dass sie danach auch schnell wiedergefunden werden (Thema, Organisation, Datum ...).
	Geschäftliche E-Mail-Nutzung: Dürfen private Mails auf den RADIX-Mailaccount weitergeleitet werden?	Die systematische Weiterleitung privater Mails auf den RADIX-Mailaccount ist nicht erlaubt. Einzelne Mails sind in Ordnung.
	Geschäftliche E-Mail-Nutzung: Wo sollen persönliche Unterlagen gespeichert werden, zB Unterlagen des Beurteilungsgesprächs, Unfallmeldungen etc? Wenn die Weiterleitung an die private Mail-Adresse nicht möglich ist, ist es nicht möglich, diese Unterlagen der privaten Ablage hinzuzufügen.	Persönliche Daten können auf eigenes Risiko im OneDrive abgelegt werden. Wenn es sich um besonders schützenswerte Daten handelt, empfehlen wir mit der Verschlüsselung gemäss Vorgabe (R:VALLGEMEIN\2_REGLEMENTE\IT-SICHERHEIT\Verschlüsseln) vorzugehen.
	Geschäftliche E-Mail-Nutzung: Grundsätzlich ist das Weiterleiten von	

Kapitel	Fragen	Antworten
	Emails nicht gestattet: Wenn man eine Email erhält, die für das ganze Team oder für jemanden aus dem Team relevant ist - wie geht man dann vor?	ja, Mails können auf private Mailadressen weitergeleitet werden. Private Mails dürfen jedoch nicht automatisch/systematisch an die RADIX-Adresse weiter- oder umgeleitet werden.
13	Private Nutzung der IT: Auf den Smartphones steckt auch viel IT. Wie wird die Nutzung der Smartphones geregelt? Vgl. dazu auch die Frage 15 in diesem Dokument	Der Zugriff auf RADIX-Daten via private Handys wird per 30. November 2026 via MAM zentral gesichert. D.h. Zugriffe sind verschlüsselt, mit Pin-Eingabe, weiterhin möglich.
	Private Nutzung der IT: Ist sämtliche Nutzung des Internets zu privaten Zwecken verboten?	Die Internetnutzung ist grundsätzlich auf geschäftliche Zwecke beschränkt. Eine kurze, gelegentliche private Nutzung ist zulässig, sofern sie die Arbeit nicht beeinträchtigt und keine Sicherheits- oder Datenschutzrisiken verursacht. Privates Webmail (z. B. private E-Mail-Konten) darf nicht genutzt werden.
15	Wo ist das offizielle Formular für Software-Beschaffungsanträge zu finden?	R:\ALLGEMEIN\2_REGLEMENTE\ANTRÄGE
	Wo ist die Software-Whitelist zu finden?	Whitelist heisst: ms-App-Store und zahlreiche, potenziell sicherheitsgefährdende Websites sind gesperrt. Zugriffe auf diese Websites sind über Website-Laptops möglich (Isusw, Zentrum Spielsucht). Zudem gilt die Regel: es sind keine Software-Downloads erlaubt. Anträge für Ausnahmen können an die GL gestellt werden, diese müssen von Swiss-Support installiert und gewartet werden (Updates etc.).
16	Anleitung zum korrekten Starten des vpns wäre hilfreich	rechte Maustaste auf netbird und connecten, bei weiteren Fragen bitte Thomas kontaktieren
	Arbeitsplatz Homeoffice, "Der Arbeitsbereich muss abschliessbar sein, damit geschäftliche Geräte und Dokumente eingeschlossen werden können" -> Wie handhabe ich dies, wenn ich den Laptop nach Hause nehmen muss (wegen externen Terminen oder Homeoffice), daheim aber keinen abschliessbaren Schrank habe?	Ein abschliessbarer Schrank ist nicht zwingend. Die Wohnungstür ist im Regelfall abgeschlossen. Ein Arbeitszimmer mit geschlossener Tür ist ebenfalls ausreichend. Ziel ist es, externen Dritten den Zugriff auf Radix-Daten und geschäftlichen Geräte so schwer wie möglich zu machen.
	Gilt die Regelung der Vernichtung von ausgedruckten Dokumenten durch Schreddern oder Rückgabe grundsätzlich für alle Dokumente oder nur für solche mit Personendaten?	Der Fokus liegt auf ausgedruckten Dokumenten mit Personendaten.

Kapitel	Fragen	Antworten
	Handys und Laptop dürfen nicht z.B. im Auto sichtbar liegen gelassen werden. Laptop muss teilweise im Auto gelassen werden, wenn wir so viel unterwegs sind. Dies selbstverständlich nicht sichtbar, sondern versteckt.	das ist bestens so.
	Mobiles Arbeiten: Keine öffentlichen WLAN-Netze nutzen > gilt das auch für Public-Netze an PHs oder anderen Hochschulen (z.B. an Weiterbildungen, Workshops etc.)?	Ideal ist immer die Nutzung des Hotspots, dieser führt automatisch über das Handy und nicht über ein Wlan. Gibt es keine oder eine nur unzureichende Verbindung, dann kann dank weiteren Schutzmassnahmen ein gesichertes, d.h. passwortgeschütztes, Wlan genutzt werden (z.B. zuhause, an einer Hochschule, Haus der Kantone, Bund etc.)
	Homeoffice und mobiles Arbeiten - Mobiles Arbeiten unterwegs: . öffentliche WLAN-Netze dürfen nicht genutzt werden. WLAN-Zugriff von unterwegs hat ausschliesslich über einen Hotspot des Mobiltelefons zu erfolgen.	Es dürfen auf keinen Fall öffentliche Wlan-Netze verwendet werden!
17	Da auch die Mobilgeräte sicher sein müssen und die Abtrennung von privaten Inhalten schwierig ist: Wäre es nicht sinnvoll, den Mitarbeitenden sichere Geschäftsmobiltelefone zur ausschliesslichen Nutzung für die Arbeit zur Verfügung zu stellen? Mobile Geräte für privaten und geschäftlichen Gebrauch erscheinen mir ein relativ grosses Sicherheitsrisiko zu sein. Würde RADIX nebst dem Abo auch die Kosten für ein eigenes einfaches Geschäftsnatel übernehmen?	Der Zugriff auf RADIX-Daten via private Handys wird per 30. November 2026 via MAM zentral gesichert. D.h. Zugriffe sind verschlüsselt, mit Pin-Eingabe, weiterhin möglich. Geschäftshandys können für die Social media-Nutzung wo nötig über das Projektbudget gekauft werden. - Für Hotspot, können private Handy genutzt werden - Für MFA am Arbeitsplatz, können private Handy genutzt werden. Wo dies nicht möglich ist, gibt es einen (physischen) Yubico Security Key C NFC. > Abokosten für privates Handy oder Passkey-Schlüssel werden von RADIX übernommen. - Auf RADIX Mails, Kalender, Teams, OneDrive, Sharepoint etc. kann mobil über das Notebook oder Handy mit MDM zugegriffen werden. Alle MA die mobil oder remote arbeiten, sind mit einem Geschäfts-Notebook ausgestattet, zudem verfügt jeder Standort über ein Reserve- (Tagungs- oder Website-) Notebook.

Kapitel	Fragen	Antworten
	Private Geräte: Was passiert bei Verlust und Wiederauffinden? Wie lange darf man zuwarten, bis z. B. Suchaufträge der SBB erledigt sind? Bzw. werden alle Inhalte, auch die privaten, vom privaten Mobile gelöscht?	Bitte sofort Thomas melden. Der Zugang zur RADIX Cloud-Umgebung wird sofort gesperrt und wieder frei gegeben, sobald das Handy wieder verfügbar ist.
	Private Geräte: Welche Befugnisse hat RADIX, wenn mein privates Mobile durch RADIX gesichert ist?	RADIX sichert ihren Zugang, nicht die privaten Handys. Wir werden anstelle von MDM (Mobil Device Management) MAM (Mobil App Management) einführen. Nachstehend werden Fragen zu MAM beantwortet, die ursprünglich zu MDM gestellt wurden. Was ist MAM? MAM (Mobile App Management) ermöglicht einen sicheren Zugriff auf die RADIX-Cloud über mobile Geräte. Kann RADIX mit MAM auf private Daten zugreifen? Nein. Die MAM-Lösung sichert die Daten bei RADIX. Via private Handys von Mitarbeitenden kann mit einem PIN darauf zugegriffen werden. Umgekehrt gibt es keinen Zugriff. Was geschieht, wenn der Zugang deaktiviert wird? Betroffen ist lediglich der Zugang zur RADIX-Cloud. Alles andere ist nicht betroffen. Wird MAM verpflichtend? Nein, Mitarbeitende entscheiden selbst, ob sie sich über die Apps, z.B. Kalender oder Outlook, für einen gesicherten Zugang bei RADIX anmelden wollen. Was passiert, wenn ich mich nicht anmelde? Ohne Anmeldung ist kein Zugriff auf die RADIX-Cloud über das Mobilgerät möglich. Die Anmeldung kann jedoch später jederzeit nachgeholt werden. Ist mein Handy betroffen, wenn die RADIX-Cloud gehackt wird?

Kapitel	Fragen	Antworten
		Nein. Bei einem Hack würde sicherheitshalber der Zugang bei RADIX gesperrt. Vis-versa bitten wir alle auch Hacks von privaten Handys zu melden. Kann ich meinen RADIX-Kalender auf dem Privathandy nutzen, ohne mich bei MAM anzumelden? Nein, aber meldet sich nur für die Apps an, die man nutzen möchte.
	Ist angedacht, dass RADIX geprüfte/formatierte USB-Sticks etc. zur Verfügung stellt?	RADIX stellt neue Sticks zur Verfügung. Benutzte Sticks können an einem Domänen-Notebook (kein Notebook mit Zugang R) neu formatiert und wieder verwendet werden. Siehe dazu: R:\ALLGEMEIN\2_REGLEMENTE\IT-SICHERHEIT\RADIX Devices
	Wäre es sinnvoll, wenn die MA, die auch im Zug arbeiten eine privacy display Schutzfolie erhielten?	Die Verwendung von Privacy-Display-Schutzfolien ist in solchen Fällen angebracht. RADIX übernimmt sowohl die Beschaffung als auch die vollständigen Kosten (Kontakt: mettler@radix.ch).
Allg.	Wird eine Überprüfung durchgeführt, um sicherzustellen, dass alle PPT-Präsentationen Bilder enthalten, für deren Verwendung wir die Rechte besitzen? Es ist ein erheblicher Aufwand, alle Bilder und Fotos in den PPT-Präsentationen unserer ehemaligen Kolleginnen erneut zu überprüfen. Wird Unterstützung bei der Überprüfung und Freigabe der vorhandenen Fotos angeboten, die sich auf unseren Datenträgern befinden?	Im Zweifelsfall das Bild nicht weiterverwenden und stattdessen neue Bilder auswählen. Bitte beachtet dazu die Richtlinien zur Bildnutzung. Evelyne oder Silvia können dabei helfen (prüfen, ob und welche Rechte wir an einem Shutterstock-Bild haben).