ARBEITSANWEISUNG ZUM UMGANG MIT DATEN UND KI

Version: 01.12.2025

Liebe alle,

für ipcenter ist der ordnungsgemäße Umgang mit personenbezogenen Daten gemäß Datenschutzgrundverordnung (DSGVO) sowie der Schutz firmenbezogener Daten ein wichtiges Anliegen. Dies beinhaltet das Erfassen, Erheben, Aufbewahren/Speichern, jegliche Handhabung und die Löschung dieser Daten.

Die Einhaltung der **Datenschutzvorgaben** und die Sicherstellung der **Datensicherheit** tragen wesentlich zum nachhaltigen Unternehmenserfolg bei.

Im Unternehmen werden neben Teilnehmer:innen-Daten im Schulungs- und Beratungskontext, Kund:innen- und Geschäftspartner:innen-Daten auch Mitarbeiter:innen-Daten verarbeitet. Aufgrund gesetzlicher und/oder vertraglicher Verpflichtungen geben wir Daten an Dritte weiter.

Zusätzlich hat sich ipcenter den Branchenrichtlinien der BABE (Berufsvereinigung der Arbeitgeber:innen privater Bildungseinrichtungen) unterworfen. Dieser „Code of Conduct“ bildet die Basis für unseren Umgang mit dem Thema Datenschutz.

Darüber hinaus gewährleistet ipcenter einen sicheren und verantwortungsvollen Umgang mit neuen technischen Entwicklungen, insbesondere beim Einsatz von **Künstlicher Intelligenz (KI), siehe dazu Kapitel 11.** Diese Richtlinie beinhaltet daher Klarstellungen und Vorgaben auf Seiten der Organisation, die die Erfüllung der Vorgaben der seit 01.08.2024 gültigen EU-KI-Verordnung („EU – AI Act“) sicherstellen.

Die sorgfältige Beachtung und Umsetzung, sowohl der Datenschutzrichtlinie als auch dieser Arbeitsanweisung, ist daher eine wesentliche Voraussetzung für unsere Zusammenarbeit.

Ich darf euch hiermit die Arbeitsanweisung der Geschäftsführung übermitteln:

Inhalt

1 EINLEITUNG

Wie bereits in den Unterweisungen zu Dienstbeginn als auch im Rahmen von Schulungen und Anweisungen im Verlauf Ihres Dienstverhältnisses wiederholt betont wurde, ist der richtige und sorgsame Umgang mit Daten besonders wichtig. Dabei ist besonders Augenmerk auf personenbezogene Daten zu richten, da diese vom Schutz der Datenschutz-Grundverordnung (DSGVO) erfasst sind. Zum besseren Verständnis seien einige der Begriffe, die von der DSGVO vorgegeben werden, kurz erklärt:

„***Personenbezogene Daten***" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (=„betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

„***Verarbeitung***" umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„***Einwilligung***" der betroffenen Person umfasst jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Die DSGVO räumt Betroffenen, also natürlichen Personen, deren personenbezogene Daten verarbeitet wurden, folgende Rechte ein, die gem. DSGVO geltend gemacht werden können (**Betroffenenrechte**):

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung / „Vergessenwerden" (Art 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art 20 DSGVO)
- Widerspruchsrecht (Art 21 DSGVO)

Alle Maßnahmen zur Wahrung der Rechte der Betroffenen sind mit höchster Sorgfalt zu setzen und jede Weitergabe von personenbezogenen Daten in Erfüllung der Betroffenen-Rechte sind in Absprache mit Datenschutzkoordination (datenschutz@ipcenter.at) zu klären.

2 Datenschutz Anlaufstelle

Wenn Ihnen – auf welchem Weg oder in welchem Zusammenhang auch immer – Umstände und Sachverhalte im Zusammenhang mit Relevanz für den Datenschutz bekannt werden (oder wenn Sie einen solchen Zusammenhang vermuten), ist dies der Datenschutzkoordination zu melden.

Kontakt: datenschutz@ipcenter.at

Ein falscher Alarm hat für Sie keinerlei dienstliche Konsequenzen. Eine Nichtmeldung kann für das Unternehmen schwerwiegende Folgen verursachen, einschließlich behördlicher Verfahren mit erheblichen Strafen, für die Sie verantwortlich wären, wenn Sie diese Dienstanweisung nicht befolgen.

Umstände mit Datenschutzrelevanz können auf unterschiedliche Weise auftreten; z.B. per E-Mail, per Telefon und/oder im persönlichen Gespräch. Nicht immer werden die Begriffe „Daten" oder „Datenschutz" dabei ausdrücklich genannt.

Wenn Ihnen von Betroffenen, von Kolleg:innen oder aus anderen Quellen Umstände mitgeteilt werden, wie insbesondere die Information, dass jemand Unterlagen, die nicht für ihn:sie bestimmt waren, erhalten hat, ist dieser Vorfall unverzüglich an die Datenschutzkoordination zu melden.

Bitte beachten Sie, dass jede:r Mitarbeiter:in zur Mitteilung von potenziellen Datenschutzverletzungen an die Datenschutzkoordination unter datenschutz@ipcenter.at verpflichtet ist. Die weitere Bearbeitung und Beantwortung aller Anfragen erfolgt ausschließlich zentral durch die Datenschutz-koordination. Die Anfragen sind demnach nur weiterzuleiten und keinesfalls selbst zu beantworten.

In diesem Sinne sind sämtliche Meldungen (mündlich und, schriftlich), die Datenschutz berühren, ausschließlich an die Datenschutzkoordination weiterzuleiten und nicht selbst zu beantworten. Insbesondere gilt dies, wenn der Betreff, die Überschrift oder der Inhalt Anlass zur Annahme einer Datenschutzrelevanz gibt (z.B. im Fließtext wird von einer Datenschutzverletzung geschrieben).

3 Betroffenenrechte: Erledigung von Anfragen und Beschwerden

Jede:r Betroffene hat das Recht auf Einhaltung der Betroffenenrechte. Dazu gehört insbesondere auch die Möglichkeit, Auskunft über ihre:seine gespeicherten Daten zu verlangen. Dabei ist zu unterscheiden, ob es sich um reine Datenpflege oder ein offizielles Auskunftsbegehren im Sinne der DSGVO handelt.

Weiters besteht die Verpflichtung, einem berechtigten Löschbegehren einer betroffenen Person nachzukommen. Die Bearbeitung von Anfragen und Verlangen in Bezug auf Betroffenenrechte müssen dokumentiert werden, um aus rechtlicher Sicht bei etwaigen Einsprüchen von Betroffenen den Nachweis einer ordentlichen Ausführung/Erledigung erbringen zu können.

Um die korrekte Bearbeitung von Anfragen und Beschwerden im Zusammenhang mit Betroffenenrechten sicherzustellen, sind diese ausnahmslos an datenschutz@ipcenter.at zu richten. Sollten Anfragen oder Meldungen bei anderen Adressen ankommen, sind diese sofort an datenschutz@ipcenter.at weiterzuleiten. **Es gilt: jede:r hat zu melden!** Mehrfachmeldungen sind besser als keine Meldung!

3.1 Datenpflege

Selbstverständlich wollen wir personenbezogene Daten (z.B. Telefonnummer, Adresse, E-Mail-Adresse etc.) aktuell halten. Daher ist die erforderliche Aktualisierung von Daten mit Teilnehmer:innen, Kund:innen, Mitarbeiter:innen, Geschäftspartner:innen etc. unbedenklich.

3.2 Auskunftsbegehren im Sinne der DSGVO

Szenario: Eine Person nimmt ausdrücklich auf den Datenschutz Bezug oder will wissen, welche persönlichen Daten von ihm:ihr im ipcenter gespeichert sind.

Diese Anfragen sind schriftlich und mit Identifikationsnachweis (Ausweiskopie) einzubringen und ausnahmslos an das Datenschutzteam (datenschutz@ipcenter.at) weiterzuleiten, das diese Begehren sachgemäß behandeln wird. Eigenmächtige Recherchen und Erledigungen solcher Anfragen sind auch dann untersagt, wenn Ihnen die anfragende Person persönlich bekannt oder sogar sympathisch ist.

Mit der Behandlung von Auskunftsanfragen sind rechtliche Fristen und Konsequenzen verbunden, daher dürfen Sie diese unter KEINEN Umständen Anfragen selbst und direkt beantworten!

3.3 Löschbegehren im Sinne der DSGVO

Szenario: Jemand verlangt die Löschung all seiner:ihrer Daten aus der Kursdatenbank oder einer anderen Datenablage (digital und physisch).

Diese Aufforderungen sind ebenfalls schriftlich und mit Identifikationsnachweis (Ausweiskopie) einzubringen und unbedingt an das Datenschutzteam (datenschutz@ipcenter.at) weiterzuleiten, das diese Begehren sachgemäß behandelt.

Vor der Durchführung einer „gewünschten" Löschung muss geprüft werden, ob es zulässig ist, dem Löschbegehren nachzukommen. Zudem sind solche beantragten Löschungen nachvollziehbar zu dokumentieren. Daher dürfen Sie Daten NIEMALS selbstständig löschen!

4 Telefonische Auskünfte

Telefonische Auskünfte über Kund:innen, Partner:innen, aktive bzw. ehemalige Mitarbeiter:innen oder Teilnehmer:innen via Telefon an betriebsfremde Personen sind jedenfalls und grundsätzlich unzulässig.

Telefonische Weitergabe von personenbezogenen Daten ist nicht zulässig, außer Sie sind zu 100% sicher, dass Sie mit der richtigen Person (=Person, mit der Sie annehmen zu sprechen) und zugleich mit einer berechtigten Person telefonieren (Stimme, Nummernkennung etc.). Dies gilt sowohl für die Kontaktaufnahme über das unternehmensinterne Festnetz, als auch über mobile Geräte.

Szenario: Jemand ruft Sie an und behauptet, von der Geschäftsführung zu sein. Sie sind neu und sind sich nicht sicher, da Sie „den:die Chef:in" noch nicht persönlich kennen!

Mögliche Lösung: Sie ziehen eine:n langjährige:n Kolleg:in bei, die die Person identifizieren kann.

4.1 Auskünfte an ipcenter-Mitarbeiter:innen

Sie dürfen Informationen an Kolleg:innen nur dann am Telefon weitergeben, wenn Sie zu 100% sicherstellen können, dass Sie mit dem:der richtigen Ansprechperson telefonieren (bspw. Sie kennen die Stimme und Ausdrucksweise des:der Gesprächspartner:in ganz genau).

Achtung: Aktuelle (KI)-Technologien können sowohl Anruf-Kennungen und E-Mails fälschen sowie auch Stimmen oder Videos täuschend echt wiedergeben.

4.2 Auskünfte an befugte Stellen wie Behörden oder Partnerorganisationen

Stellen Sie sicher, dass Ihr:e Gesprächspartner:in tatsächlich befugt ist, Auskünfte zu erhalten. Sind Gesprächspartner:in oder Rufnummer nicht 100% bekannt, so ist die Anfrage per E-Mail an Sie zu richten und Sie rufen zurück oder Sie antworten kurz auf das E-Mail, sofern es sich um eine offizielle email-Adresse der Partnerorganisation handelt.

Achtung: Nicht nur den Absendernamen (Alias) überprüfen, sondern wirklich die dahinter liegende E-Mail-Adresse inklusive Domäne.

4.3 Sonstige Auskünfte

An betriebsfremde Personen, die nicht unter Punkt 4.2 fallen, dürfen keine Informationen oder Daten weitergegeben werden. Bitte beachten Sie, dass auch ehemalige Mitarbeiter:innen, Angehörige von Mitarbeiter:innen, aktive oder ehemalige Teilnehmer:innen oder auch Personen anderer Unternehmen im Konzernverbund von ipcenter betriebsfremde Personen sind.

5 Physische Sichtbarkeit personenbezogener Daten

Sämtliche Maßnahmen zum Schutz von personenbezogenen Daten betreffen sowohl das Arbeiten im Büro, als auch Telearbeit:

- Stellen Sie sicher, dass keine persönlichen Daten oder Dokumente (z.B. Motivationsschreiben, Lebensläufe, Zeugnisse, Krankenstandsbelege etc.) von Teilnehmer:innen, Mitarbeiter:innen, Bewerber:innen, Kund:innen, Geschäftspartner:innen oder Kolleg:innen für andere Personen einsehbar sind. Dies gilt sowohl für elektronische Daten als auch für Daten in Papierform.
- Lassen Sie niemals Dokumente unbeaufsichtigt liegen, loggen Sie sich aus Datenbanken, Onlineportalen oder Programmen ordnungsgemäß aus und aktivieren Sie die Bildschirmsperre *([Win]-[L])* am Arbeitsplatz, wenn Sie diesen – auch wenn „nur für einen Moment“ – verlassen. Bitten an Kolleg:innen „auf den Computer aufzupassen“ sind nicht ausreichend.
- Ausdrucke, welche personenbezogenen Daten beinhalten, sind auf das notwendigste Minimum zu reduzieren bzw. beim Arbeiten außerhalb des Büros weitestgehend zu vermeiden.
- Entsorgen Sie Ausdrucke, die personenbezogene Informationen enthalten, nicht im Altpapier, sondern vernichten Sie diese ordnungsgemäß in den Shredder-Geräten an den Standorten.

Achten Sie besonders darauf, dass personenbezogene Daten niemals auf

- Schreibtischen und Ablageflächen
- Bildschirmen

- Beamer & Overheads
- Flipcharts & Plakaten
- Ablageflächen bei Kopierern, Besprechungsräumen, Küchen etc.

allgemein einsehbar sind! Dies gilt insbesondere auch bei Bildschirm-Sharings im Zuge von Video-Konferenzen.

6 Speicherung personenbezogener Daten

Als elektronischer Speicherort von personenbezogenen Daten sind ausschließlich zulässig – stets in Absprache mit dem:der Vorgesetzen:

- die dafür vorgesehenen Ablageorte am Fileserver oder
- Cloud-Lösungen mit Firmenlizenzen (MS Teams, Sharepoint, Nextcloud, Dropbox Business), die vom EDV-Team eigens für diesen Zweck eingerichtet wurden oder
- die Kursdatenbank, ipmoodle oder
- andere Datenbanken, die speziell für den Auftragszweck eingerichtet wurden

Keinesfalls dürfen Daten an folgenden Speicherorten abgelegt werden:

- Desktop
- USB-Stick *(siehe 6.2)*
- sonstige externe Medien bspw. Festplatte *(siehe 6.2)*
- private Cloud-Lösungen oder private Netzwerk-Laufwerke
- Privatgeräte (Mobiltelefone, Tablets, Privat-PCs etc.) *(siehe auch Kapitel 8 bzw. 9)*

6.1 Fileserver

Für einzelne Bildungsangebote gibt es eine vorgegebene eindeutige und klare Struktur für die Ablage personenbezogener Daten. Diese ist unbedingt einzuhalten und- im Bedarfsfall – in Absprache mit der Abteilungsleitung Implementation zu erstellen.

Diese Daten unterliegen strengen Löschvorgaben und -fristen seitens unserer Auftraggeber. Diese Daten dürfen daher ohne Rücksprache mit EDV und Führungskraft keinesfalls an andere Speicherorte oder -medien verschoben oder kopiert werden.

6.2 Externe Datenträger (USB-Sticks, externe Festplatten etc.)

Grundsätzlich dürfen KEINE personenbezogenen Daten auf externe Datenträger gespeichert werden. Sollte es für Ihre Arbeit notwendig sein (bspw. Lebensläufe zur Weiterbearbeitung von Teilnehmer:innen), ist der Datenträger zu **verschlüsseln, sodass ausschließlich der:die Besitzer:in mit dem Passwort darauf zugreifen kann**. Eine Anleitung zur Verschlüsselung von externen Datenträgern ist auf dem Mitarbeiter:innen-Portal InfoPaula in der Rubrik „Vorlagen und Dokumente“ abrufbar.

Bei anderen Daten wie Kursbeispielen und Präsentationen, die bspw. auf einem Schulungs-PC oder bei einem Kund:innentermin vor Ort verwendet werden, kann die Verschlüsselung unterbleiben – jedenfalls ist stets auf eine sorgsame Verwahrung zu achten. **Dabei ist besonders darauf zu achten, dass keine personenbezogenen Daten (irrtümlich) mitgespeichert werden.**

6.3 Kund:innen-Karteien

Für Projekte und Tätigkeiten, die das Speichern von Informationen über Kund:innen – entweder als Ausbildungsziel oder als Projektinhalt – erfordern (bspw. Lehrausbildung an Modellen oder Eventmanagement), ist zu definieren, welche ausgewählten Personen Kund:innenkontakte einsehen und bearbeiten dürfen. Andere Personen (bspw. Lehrlinge, Gäste oder weitere Mitarbeiter:innen) dürfen nur unter Aufsicht mit diesen Daten hantieren. Bei elektronisch abgespeicherten Kund:innen-Informationen muss sichergestellt sein, dass das Passwort nicht weitergegeben wird oder allgemein einsehbar ist.
Wenn Sie merken, dass Sie Zugriff auf personenbezogene Daten haben, obwohl Sie nicht den zu den Zugriffsberechtigten gehören, ist die Datenschutzkoordination (datenschutz@ipcenter.at) zu informieren.

7 Austausch personenbezogener Daten

Grundsätzlich ist der E-Mail-Verkehr als nicht sicher anzusehen und daher ist vom elektronischen Versand personenbezogener Daten via E-Mail abzusehen. Für langfristige und regelmäßige Geschäftsbeziehungen können verschlüsselte, sichere E-Mail-Kanäle eingerichtet werden. Diese sind vorab schriftlich an EDV (Helpdesk) zwecks Überprüfung und etwaiger Adaptierung bekanntzugeben.

- Personenbezogene Daten dürfen nur über Shared-Postfächer übermittelt werden. Die dafür explizit vorgesehenen Löschroutinen werden von der EDV zentral sichergestellt. Dazu ist folgende Vorgehensweise in der Arbeit mit Postfächern ausdrücklich einzuhalten:
    - E-Mails/Daten, die aufzubewahren sind, sind in Unterverzeichnisse zu verschieben. Personenbezogene Daten dürfen hier nur mit datenschutzrechtlicher Begründung mitumfasst sein.
    - Alle nicht verschobenen E-Mails im Postfach „Posteingang“ und „Gesendete Objekte“ unterliegen einer automatisierten Löschfrist von 6 Monaten.
    - Aus gesetzlichen/vertraglichen Gründen kann es in bestimmten Postfächern abweichende Regelungen geben; diese werden von der zuständigen Abteilungsleitung kommuniziert und verantwortet.
- Der firmeninterne Austausch von personenbezogenen Daten hat ausschließlich über den dafür vorgesehenen Ort am Server (Fileserver, Nextcloud, Sharepoint/Teams, Kursdatenbank oder ipmoodle) zu erfolgen.
- Der Austausch von personenbezogenen Daten mit externen Personen oder Firmen (z.B. Partner:innen, Kund:innen, Prüfungsinstituten, etc.) wird individuell geregelt. Bei Unklarheiten wenden Sie sich bitte an Ihre:n Vorgesetzte:n.
- Für neue Bildungsangebote oder Projektpartner:innen sind die Anforderungen einer Transfermöglichkeit (eigene Plattformen, Laufwerke, sichere E-Mail-Verbindung etc.) gesondert an EDV (Helpdesk) bekannt zu geben.
- Für den Austausch von Informationen mit dem AMS ist das eAMS-Portal vorgesehen und zwingend und ausschließlich zu verwenden. Auch bei Nachfrage oder Wunsch des AMS-

Personals verweisen Sie auf die Datenaustauschmöglichkeit über eAMS; insistiert das AMS-Personal, schalten Sie Ihre:n Vorgesetzte:n ein.

- Für den Austausch von Informationen mit dem ÖIF ist die ÖIF-Webanwendung vorgesehen und zwingend und ausschließlich zu verwenden. Auch bei Nachfrage oder Wunsch des ÖIF-Personals verweisen Sie auf die Datenaustauschmöglichkeit über die Webanwendung; insistiert das ÖIF-Personal, schalten Sie Ihre:n Vorgesetzte:n ein.
- Bereinigen Sie Ihren Posteingang stets von möglicherweise dort kurzfristig abgelegten personenbezogenen Daten (auch Anhänge) – dies gilt ebenfalls für den Ordner „Gesendete Objekte".
- Die Bekanntgabe von oder der Verweis auf personenbezogene Daten, über die Sie aufgrund der Erfüllung ihrer Arbeitsleistung bei ipcenter Kenntnis erlangen, nach außen ist absolut untersagt. Dies gilt insbesondere auch für soziale Medien wie z.B. WhatsApp, Facebook, Instagram etc.
- Die Kommunikation mit Teilnehmer:innen, wenn damit personenbezogene Daten verbunden sind, hat ausschließlich über ipmoodle oder Fileserver zu erfolgen, wenn nicht einer der obigen Kommunikationswege gesondert festgelegt wird.

Wenn Ihnen ein:e Kund:in eigene Daten per E-Mail sendet (z.B. Lebenslauf), schlagen Sie die weitere Kommunikation mittels eines sicheren Kommunikationsweges (siehe die Aufzählung in diesem Punkt 7.) vor.

8 Verwendung von Mobiltelefonen

Dieses Kapitel regelt die zulässige Nutzung von Firmen-Mobiltelefonen sowie den Umgang mit privaten Mobiltelefonen im beruflichen Kontext. Ziel ist der Schutz von Firmendaten und die klare Trennung zwischen dienstlicher und privater Nutzung mobiler Endgeräte.

8.1 Firmen-Mobiltelefone

Für die Verwendung von **Firmen-**Mobiltelefonen gilt die „Vereinbarung Nutzung Firmen-Mobiltelefon" in der jeweils aktuellen Fassung. Firmendaten (z.B. E-Mail, Kalender, Kontakte) dürfen dabei ausschließlich im dafür vorgesehenen Workspace (Arbeitsbereich von Android Work) gespeichert und eingerichtet werden. Eine Anleitung dafür ist im Intranet (InfoPaula) zu finden; bei Unklarheiten unterstützt Sie unser EDV-Team gerne.

8.2 Private Mobiltelefone

Grundsätzlich dürfen KEINE Firmendaten auf Ihren **privaten** Mobiltelefonen abgerufen oder bearbeitet werden.

- Firmenkontaktdaten (z.B. Teilnehmer:innen, Kund:innen bzw. Geschäftskontakte): Speichern Sie niemals Telefonnummern oder andere Kontaktdaten auf Ihren privaten Mobiltelefonen (Kontakte von ipcenter-Mitarbeiter:innen sind davon ausgenommen).
- Firmen-E-Mail-Adresse: Ihre Firmen-E-Mail-Adresse darf NICHT über eine eigene App auf Ihrem privaten Mobiltelefon abgefragt werden – AUSSCHLIESSLICH über Webmail!

- sonstige Firmendaten: Sollten Sie auf Ihrem privaten Mobiltelefon (aus welchem Grund auch immer) firmenbezogene Daten gespeichert haben, löschen Sie diese unverzüglich!
- WhatsApp oder andere Social Media Anwendungen: Jegliche Kommunikation mit beruflichen Kontakten über Social Media ist UNZULÄSSIG!

Für die mobile Erreichbarkeit während Exkursionen oder über Standorte hinweg sind die dafür vorgesehenen Firmen-Mobiltelefone zu verwenden. Diese Mobiltelefone dürfen ausschließlich für den jeweiligen Bedarfsfall ausgeborgt und müssen nach Beendigung unverzüglich retourniert werden.

9 Web und Computer außerhalb des Unternehmens (z.B. private PCs)

Unter den folgenden Voraussetzungen ist es zulässig mittels Webanwendungen (Kursdatenbank, Webmail etc.) oder Terminalserver von außerhalb des Unternehmens auf Informationen zuzugreifen:

- Bei Nutzung der ipcenter.at E-Mail-Adresse über den Browser (Webmail) dürfen Zugangsdaten NIE automatisch gespeichert werden.
- Anhänge mit personenbezogenen Daten, die Sie per E-Mail erhalten, dürfen NIEMALS auf Ihrem privaten Gerät abgespeichert werden. Sollte dies für die Erfüllung Ihrer Arbeitsleistung unabdingbar sein, dann ist das Speichermedium unbedingt zu verschlüsseln *(siehe 6.2).*
- Firmendaten dürfen unter keinen Umständen, auch nicht temporär, am privaten PC/Laptop gespeichert werden.
- Sollte Ihr Dienstverhältnis mit ipcenter enden, sind sämtliche Firmendaten und -dateien von Ihrem privaten Gerät zu löschen (v.a. Download-Verzeichnis)

Wenn Sie eine Vielzahl an unterschiedlichen Passwörtern für unterschiedliche Anwendungen in Verwendung haben, unterstützt Sie unsere EDV-Team gerne bei der Verwendung eines Tools zur Kennwortverwaltung (KeePass bzw. Vaultwarden). Außerdem ist die Richtlinie „Umgang mit Passwörtern“ auf dem Mitarbeiter:innen-Portal InfoPaula, in der Rubrik „Paula erklärt Sicherheitsfragen“, strikt einzuhalten.

10 Verwendung von Online-Tools & Online Diensten

Online-Tools, bspw. Teams, SharePoint und Zoom, erleichtern uns den Arbeitsalltag. Mit den richtigen Tools lassen sich Aufgaben effizient organisieren, im Team diskutieren und schneller erledigen. Auch die Nutzung von Online-Diensten, bspw. YouTube und Google Maps, unterstützen uns. Damit wir als Unternehmen allen Vorgaben zum Datenschutz und zur Datensicherheit nachkommen können, müssen bei der Verwendung ausnahmslos folgende „Spielregeln“ eingehalten werden:

> Hinweis: KI-Tools (z.B.:ChatGPT, Co-Pilot) sind von diesen Regelungen ausgenommen. Für diese Anwendungen gelten die unter Punkt 11.4 beschriebenen Bestimmungen.

- Es dürfen nur jene Tools/Dienste verwendet werden, die vom Unternehmen zur Verfügung gestellt, vom EDV-Team „betreut“ werden und/oder für die Nutzung freigegeben wurden (die Aufstellung dazu finden Sie im Intranet (InfoPaula) unter „Aufstellung Online-Tools_Online-Dienste“); für die Anmeldung/Registrierung ist ausschließlich die vom Unternehmen zur Verfügung gestellte ipcenter.at E-Mail-Adresse zu verwenden.

- Möchten Sie ein Tool/einen Dienst verwenden und finden dieses/diesen nicht in der Aufstellung, ist ausnahmslos VOR der Anmeldung/Registrierung eine schriftliche Anfrage mit geplantem Zweck der Nutzung beim EDV-Team einzubringen, damit geprüft werden kann, ob die Nutzung des Dienstes/ Tools aufgrund der geltenden Datensicherheits- und Datenschutzbestimmungen zulässig ist.
- Möchten Sie ein „freigegebenes" Tool nutzen, so ist die „gewünschte" Registrierung per E-Mail an EDV (Helpdesk) zu melden; das EDV-Team führt laufend Dokumentation über die aktiven firmenbezogenen User-Accounts. Zugänge bzw. Berechtigungen für Online-Shops werden ausschließlich von Mitarbeiter:innen des Teams Einkauf verwaltet.

Für die Durchführung von Kursen im Arbeitsmarktkontext und der damit verbundenen Kommunikation und den Austausch von Dateien mit Teilnehmer:innen steht Ihnen ipmoodle zur Verfügung. Dieses ist ausschließlich zu verwenden, wenn personenbezogene Daten ausgetauscht werden. Es ist strikt darauf zu achten, dass Dateien mit personenbezogenen Daten (etwa Prüfungsergebnisse, Lebensläufe, Kontaktdaten) nur mit jeweils Betroffenen durch Hochladen in deren geschütztem Bereich ausgetauscht werden. Achten Sie darauf, dass nur jene personenbezogenen Daten von Teilnehmenden gespeichert werden, die für die Kursabwicklung unbedingt notwendig sind.

Die freiwillige und private Kommunikation zwischen den Teilnehmer:innen untereinander ist von diesen Regeln nicht betroffen. Teilnehmer:innen untereinander können persönliche personenbezogene Daten im jeweils eigenen Ermessen austauschen.

11 Verantwortungsbewusster Umgang mit KI-Anwendungen

ipcenter setzt auf die Vorteile Künstlicher Intelligenz (KI) und ermöglicht seinen Mitarbeiter:innen die Nutzung von KI-Anwendungen und -Services für berufliche Zwecke. Um einen sicheren und verantwortungsvollen Umgang mit dieser Technologie zu gewährleisten und die neuen Vorgaben der seit 01.08.2024 gültigen EU-KI-Verordnung („EU - AI Act") zu erfüllen, wurden die folgenden Richtlinien erstellt.

11.1 Nutzung von KI im Unternehmen

KI-Anwendungen können für u.a. folgende Zwecke eingesetzt werden:

- Erstellung von Schulungsunterlagen: z.B. automatisierte Erstellung von Präsentationen, Übungsaufgaben und Texten.
- Recherchen: z.B. schnelle Informationsbeschaffung, automatisierte Zusammenfassung von Artikeln.
- Analyse-Instrument: z.B. Auswertung von anonymisierten Lernerfolgskontrollen, Analyse von anonymisiertem Teilnnahmefeedback.
- Optimierung laufender Prozesse: z.B. Automatisierung von administrativen Aufgaben ohne Personenbezug.
- Unterstützung bei Vor- und Nachbereitung von Trainings: z.B. durch die Bereitstellung von individualisierten Lernmaterialien und -empfehlungen.
- Erstellung von Medieninhalten: z.B. Generierung von Bildern und Videos für Marketingmaterialien oder -beiträge.

Beispiele:

- Eine KI kann Texte für ein Handout generieren oder Bilder für eine Präsentation vorschlagen.
- Eine KI kann bei der Recherche von aktuellen Studien und Fachartikeln unterstützen.
- Eine KI kann Feedbackbögen analysieren und die Ergebnisse zusammenfassen.

11.2 Zugang und Transparenz

- Welche Tools und Systeme für betriebliche Zwecke eingesetzt werden dürfen ist in Kapitel 10 geregelt.
- KI-generierte Inhalte müssen als solche gekennzeichnet werden. Wurde ein KI-Tool bei der Erstellung einer Präsentation eingesetzt, muss dies kenntlich gemacht werden.

Vorgaben für die Kennzeichnung:

- Einen Vermerk im Impressum der Schulungsunterlagen: *"Teile dieser Unterlagen wurden unter Verwendung von KI erstellt und von unseren Trainer:innen überarbeitet."*
- Eine Fußzeile in Präsentationen: *"Mit KI-Unterstützung erstellt und von Trainer:innen validiert"*
- Bei Bildmaterial einen Quellenvermerk: *"Illustration: KI-generiert mit [Tool-Name], bearbeitet durch ipcenter [Abteilung]."*

11.3 Vertraulichkeit und Datenschutz

- Auf keinen Fall dürfen **personenbezogene Daten** (z.B. Teilnehmer:innen, Mitarbeiter:innen) in ein KI-Tool / System eingegeben, eingefügt oder verarbeitet werden, wenn es dazu keine explizite Freigabe durch die Datenschutzkoordination (datenschutz@ipcenter.at) gibt.
- Abhängig von der Datenart gelten unterschiedliche Richtlinien für den Umgang mit KI-Tools (siehe Punkt 11.4)
- Bei allen Aktivitäten im Zusammenhang mit KI sind die geltenden Gesetze und Datenschutzbestimmungen, insbesondere Urheber-, Persönlichkeits- und Markenrechte, zu beachten.

11.4 Regelung der KI-Nutzung nach Datenarten

A) Personenbezogene Daten (z.B. Teilnehmer:innen-Daten)

Da es sich um personenbezogene Daten handelt, also Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z.B. Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail, Sozialversicherungsnummer, Prüfungsergebnisse von Teilnehmer:innen), ist die Nutzung von KI für diese Datenart **ausschließlich in vom Unternehmen explizit für diese freigegebenen Anwendungsfällen zulässig** (zB Nutzung einer KI-integrierten Funktion in ipmoodle mit einem dafür vorgesehenen firmeninternen KI-Server). Sollte darüber hinaus ein sinnvoller Anwendungsfall gewünscht werden, ist zuvor die ausdrückliche Zustimmung der Datenschutzkoordination einzuholen.

B) geschützte Firmendaten

Schützenswerte Firmendaten wie beispielsweise interne Strategien, Finanzdaten, Kund:innenlisten, Konzepte oder Auswertungen von anonymisierten Teilnahme-Feedbacks dürfen nur mit einem von der Führungskraft angeforderten Account mit KI bearbeitet werden (zB automatisierte Zusammenfassungen oder Übersetzungen). Dazu gehören auch Geschäftsdaten, die uns von Dritten, wie z.B. Geschäftspartner:innen, anvertraut wurden.

C) allgemeine Firmendaten

Übliche Geschäftsdokumente, die nicht unbedingt schützenswert sind (zB allgemeine E-Mails, Stockwerkpläne, Brandschutzordnung, Standard-Formulare …) dürfen mit Accounts, die auf die Firmen-E-Mail-Adresse ausgestellt sind, zum Zwecke von Generierung, Überarbeitung oder Zusammenfassung von Texten oder Bildern oder automatisierte Erstellung von Meeting-Protokollen verwendet werden. Die KI-Tools sind frei wählbar.

D) sonstige Daten

Für sämtliche sonstigen Daten wie zB Kursbeispiele, Quizzes, Recherchen aller Art, die nicht in direktem Zusammenhang mit dem Unternehmen stehen, gibt es keine Einschränkungen. Sowohl Tools als auch der Account-Name sind frei wählbar.

Verwendete Tools, mit denen Sie gute Erfahrungen machen, sind willkommen an datenschutz@ipcenter.at zu melden. Im Sinne einer lernenden Organisation wird das Unternehmen Schulungen und Tipps dazu Kolleg:innen zugänglich machen.

11.5 Zulässige KI-Tools

Für die Datenarten A-C (siehe 11.4.) gilt: Arbeitnehmer:innen dürfen ausschließlich vom Unternehmen genehmigte und freigegebene KI-Tools verwenden. Die Anmeldung erfolgt je nach Datenart und Zweck über die Unternehmens-E-Mail-Adresse. Soweit der Arbeitgeber KI-Systeme zukauft oder eigene Nutzungsrechte vereinbart, ist sicherzustellen, dass der Datenschutz vertraglich geregelt ist.

11.6 Verbotene Nutzung

✓ Der Einsatz von KI für Zwecke, die gegen Recht, Ethik oder Unternehmensgrundsätze verstoßen, ist untersagt.

11.7 Qualitätskontrolle und Objektivität

- KI-generierte Inhalte müssen vor der Verwendung auf Richtigkeit und Zuverlässigkeit eigenverantwortlich von den Mitarbeiter:innen überprüft werden.
- Verzerrungen in den Inhalten sind zu identifizieren und zu korrigieren, um die Objektivität zu gewährleisten.

Was sind „Verzerrungen in den Inhalten"?

KI-Systeme können aufgrund von Verzerrungen in den Trainingsdaten fehlerhafte oder diskriminierende Ergebnisse liefern. Beispiele:

- Halluzinieren: Das beschreibt, dass das Modell falsche oder erfundene Informationen generiert, die nicht auf den Trainingsdaten oder der Realität basieren. Diese Halluzinationen können sich in verschiedenen Formen äußern, z. B.:
  - **Erfundene Fakten**: Die KI gibt falsche Informationen aus, als wären sie wahr (z. B. falsche Zitate, erfundene Statistiken oder nicht existierende Personen/Orte).
  - **Fehlinterpretationen**: Die KI zieht falsche Schlussfolgerungen oder verbindet nicht zusammenhängende Konzepte.
  - **Nicht existierende Quellen**: Die KI zitiert Bücher, Artikel oder Autor:innen, die es gar nicht gibt.

- **Logische Fehler**: Die KI macht unplausible oder widersprüchliche Aussagen.

- Geschlechterstereotype: Eine KI, die mit Texten trainiert wurde, in denen Frauen vor allem in fürsorglichen Berufen erscheinen, könnte weiblichen Jugendlichen Formulierungen mit Fokus auf soziale Kompetenzen vorschlagen, während sie bei männlichen Jugendlichen eher Durchsetzungsstärke und Führung betont.
- Ethnische Vorurteile: Wird eine KI mit einseitigen Trainingsdaten zur Erstellung von Schulungsunterlagen eingesetzt, kann sie andere ethnische Gruppen unterrepräsentiert oder stereotyp darstellen.
- Soziale Diskriminierung: Eine zur Analyse anonymisierter Bewerbungen eingesetzte KI könnte aufgrund verzerrter Trainingsdaten Jugendliche aus sozial benachteiligten Verhältnissen übergehen, indem sie deren Qualifikationen und Potenziale unterschätzt.

12 Sicherheitsrisiken

Neben dem Einsatz von Schadsoftware, wie bspw. Viren und Trojaner für Angriffe gegen unsere EDV-Infrastruktur, gegen die wir uns mit einem Virenschutz bzw. einer Firewall schützen, gibt es auch Gefahrenquellen, die auf die Unachtsamkeit/Unbedarftheit von Mitarbeiter:innen abzielen.
Um diesen wirksam entgegenwirken zu können, ist es wichtig, dass Sie bei Ihrer täglichen Arbeit sensibel und aufmerksam auf auffällige oder verdächtige Situationen reagieren. „Besondere Vorkommnisse“ sind umgehend dem EDV-Team zu melden; im Zweifel bitte immer nachfragen.

12.1 Social Engineering

Das Manipulieren von Personen mit dem Ziel unbefugt Zugang zu vertraulichen Unternehmens-informationen und/oder IT-System zu erhalten, wird Social Engineering genannt; meist erfolgt die Kontaktaufnahme per Telefon oder E-Mail.

Social Engineering kommt auch zum Einsatz, um Mitarbeiter:innen zu unbedachten Handlungen zu bewegen; dies kann die Installation eines unbekannten Programms oder fragwürdige Finanz-transaktionen umfassen.

Dieses Vorgehen kann Schäden in Millionenhöhe verursachen, daher ist besondere Vorsicht geboten. Angesichts der rasanten technischen Entwicklung gilt dies strikt für alle Kommunikationskanäle (E-Mails, Anrufe, SMS, …).

- Bei außergewöhnlichen Wünschen oder Aufträgen, die per Telefon oder E-Mail einlangen, ist unbedingt ein persönliches Gespräch zur Abklärung nötig (z.B. durch aktiven Rückruf an eine vertraute Person – unangekündigt).
- Verdächtige E-Mails sind immer an das EDV-Team weiterzuleiten.
- Oftmals sind betrügerische E-Mails an der Absenderadresse zu erkennen, die im Detail anders ist als die offizielle Domain des Unternehmens; z.B. steht als Absender der Name eines:einer Kolleg:in, die E-Mail-Adresse nach dem Klammeraffen (@) ist jedoch nicht „ipcenter.at“.
- Tauschen Sie sich mit Kolleg:innen über verdächtige Anrufe und E-Mails aus, damit Social Engineering nicht unentdeckt bleibt.
- Sicherheitsrelevante Informationen (z.B. Passwörter) sind niemals per E-Mail oder Telefon weiterzugeben! Hier gilt immer, das persönliche Gespräch zu suchen bzw. ggf. das EDV-Team um Rat zu fragen. In jedem Fall ist der:die Gesprächspartner:in eindeutig zu identifizieren.

- Bitte um besondere Vorsicht bei Anweisungen zu Einkäufen oder Zahlungen, die mittels Telefon, E-Mail oder zB Teams-Chat angefordert werden. Im Zweifelsfall bitte immer persönlichen Kontakt suchen oder die Person zurückrufen.

12.2 Phishing

Unter dem Begriff „Phishing“ (von „password fishing“) versteht man Versuche, über gefälschte Websites, E-Mails oder Kurznachrichten an persönliche Daten (z.B. Daten für das Online-Banking, für Online-Shops oder Soziale Netzwerke) von Internet-Benutzer:innen zu gelangen.

So schützen Sie sich:

- Klicken Sie auf keine Links in E-Mails oder sonstigen Nachrichten, in denen dazu aufgefordert wird, Kontodaten oder Passwörter bekannt zu geben.
- Übermitteln Sie keine vertraulichen Daten (Login-Daten, Passwörter, TANs) per E-Mail, per Chat oder telefonisch.
- Öffnen Sie keinesfalls unbekannte Datei-Anhänge in E-Mails oder sonstigen Nachrichten – darin sind oft Viren versteckt!
- Geben Sie vertrauliche und persönliche Daten ausschließlich über SSL-verschlüsselte Seiten bekannt – erkennbar an "https://" am Beginn der Internetadresse und an einem versperrten Schloss-Symbol am oberen oder unteren Bildschirmrand.

Im Zweifel bitte unbedingt an EDV (Helpdesk) wenden.

13 Telearbeit bzw. Arbeiten außerhalb der ipcenter-Standorte

Selbstverständlich gelten sämtliche in dieser Arbeitsanweisung beschriebenen Vorgaben zu Datenschutz und Datensicherheit auch und insbesondere außerhalb der ipcenter-Standorte bzw. in der Telearbeit.

14 Sonstiges

Bedingt durch die rasch fortschreitende technologische Entwicklung werden laufend weitere Maßnahmen und Regelungen getroffen, die Datensicherheit und Datenschutz im Unternehmen weiter erhöhen. Dazu zählt bspw. die 2-Faktor-Authentifizierung.

Sollten Sie auf ein Problem aufmerksam werden, das Datenschutz oder Datensicherheit bei ipcenter betrifft, informieren Sie unverzüglich datenschutz@ipcenter.at.

Sollten sich durch Regelungen in dieser Arbeitsanweisung schwerwiegende Probleme für Ihre tägliche Arbeit herausstellen, besprechen Sie diese bitte mit Ihrem:Ihrer Vorgesetzen; wir sind bemüht, eine passende Lösung zu finden.

Abschließend möchten wir Sie nochmals um Ihre Unterstützung bitten. Es gilt jedenfalls das Prinzip, lieber eine Falschmeldung als keine Meldung!