Compliance aus dem Blickwinkel der aktuariellen Arbeit am Beispiel von End User Computing

Überlegungen zu regulatorischen Vorgaben, neues Datenschutzgesetz und Lösungen für Erleichterung im Umgang mit EUCs

Olivia Gradenwitz, Marius Moser

15.03.2023

mazars

Ablauf

1. Einführung
2. Beispielfall
3. Neues Datenschutzgesetz
4. Fazit

01

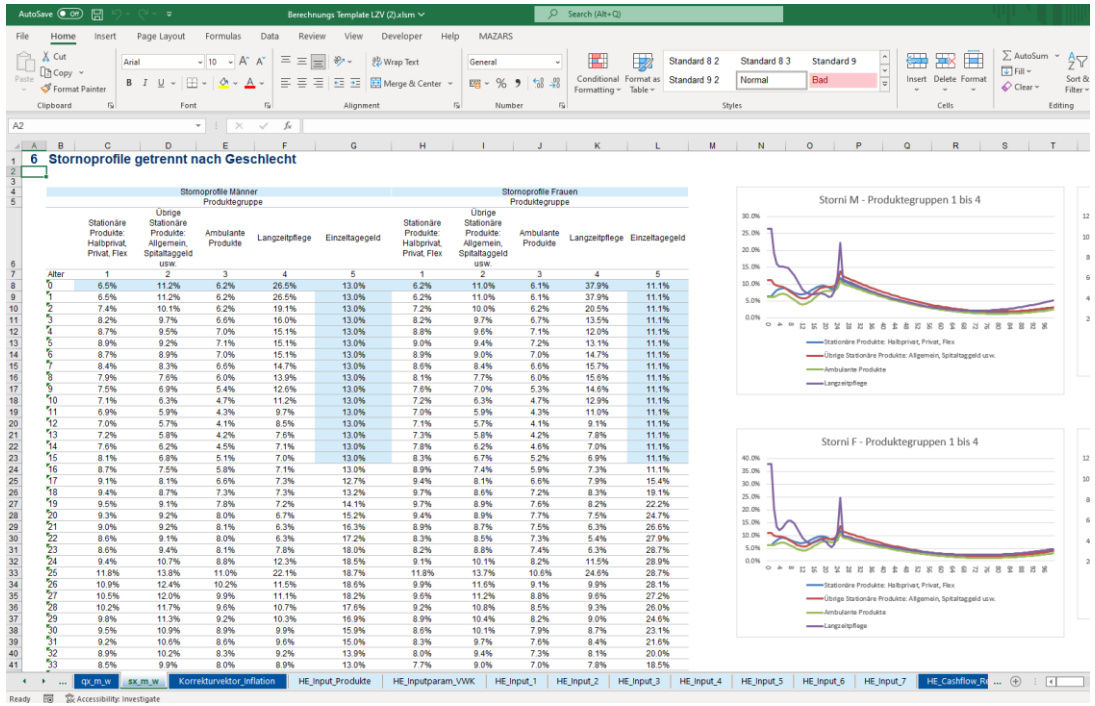
Sektion 01:

Einführung

Was sind EUC?

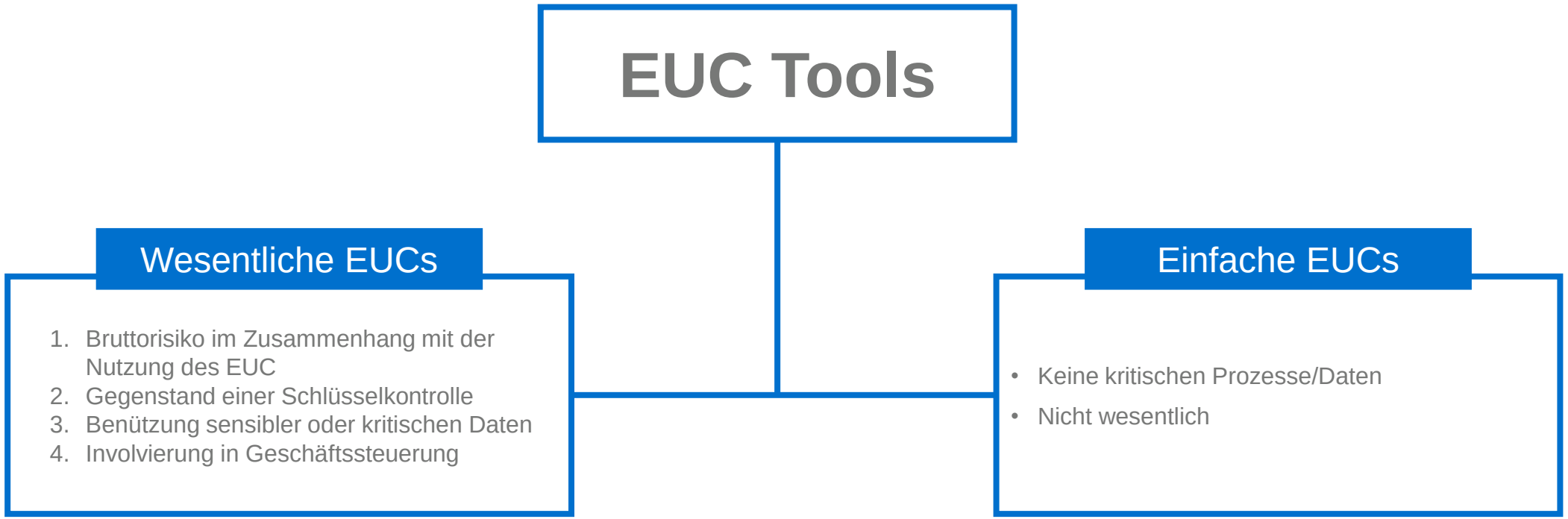
Mögliche Definition:

EUC/EUT ≈ IT-Lösungen ohne zentrales Monitoring der IT-Abteilung



Wesentlichkeiten bei EUC

Nicht jedes „Spread Sheet“ ist automatisch ein wesentliches EUC.
Die Abgrenzungsverantwortung liegt i.d.R. beim Fachbereich.



Beispiele von wesentliche aktuarielle EUCs

- Excel Datei zur Berechnung der IBNR Rückstellungen
- MS Office Makro zur Datenverarbeitung
- R Code zur Simulation von Jahresschadenereignissen zur Solvenzbestimmung im SST
- SAS Code zur Aufarbeitung von aktuariellen Bestandes- oder Schadenslisten

?

Regulatorische Vorgaben EUC

Externe Anforderungen	Erläuterungen
Anforderungen an das Interne Kontrollsystem (IKS)	
Art. 716a III.2.1 OR	Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben: […] die Ausgestaltung des Rechnungswesens, der **Finanzkontrolle** sowie der Finanzplanung.
Art. 728a OR	Die Revisionsstelle prüft, ob ein **internes Kontrollsystem** existiert. Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfangs der Prüfung das interne Kontrollsystem.
Art. 728b OR	Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das **interne Kontrollsystem** sowie die Durchführung und das Ergebnis der Revision. → **OR verlangt Existenz eines IKS für die finanzielle Berichterstattung**
VAG Art. 27	Das Versicherungsunternehmen richtet ein **wirksames internes Kontrollsystem** ein, das seine gesamte Geschäftstätigkeit umfasst. Zudem bestellt es eine von der Geschäftsführung unabhängige interne Revisionsstelle (Inspektorat). → **VAG verlangt ein wirksames IKS**
FINMA RS 2017/02 Corporate Governance Versicherer	Das Versicherungsunternehmen richtet ein internes Kontrollsystem ein, um eine angemessene Sicherheit bezüglich der Risiken der Geschäftsführung zu gewährleisten, insbesondere in Bezug auf die **Wirksamkeit von Geschäftsprozessen, die Zuverlässigkeit der finanziellen Berichterstattung und die Befolgung von Rechtsnormen und internen Vorschriften**. Die Grundsätze des internen Kontrollsystems sind sowohl auf wesentliche Auslagerungen als auch auf übrige Beziehungen mit Drittpersonen anwendbar. Das Versicherungsunternehmen definiert **hinreichende Kontrollaktivitäten** auf Unternehmens- und Prozessebene, um zu gewährleisten, dass die vom Verwaltungsrat und von der Geschäftsleitung angeordneten Vorgänge, Methoden oder Massnahmen, mit welchen den wesentlichen Risiken der Geschäftsführung begegnet werden soll, eingehalten und ausgeführt werden. → FINMA präzisiert gesamte Geschäftstätigkeit sowie gleichbleibende Verantwortung für wesentliche Auslagerungen

02

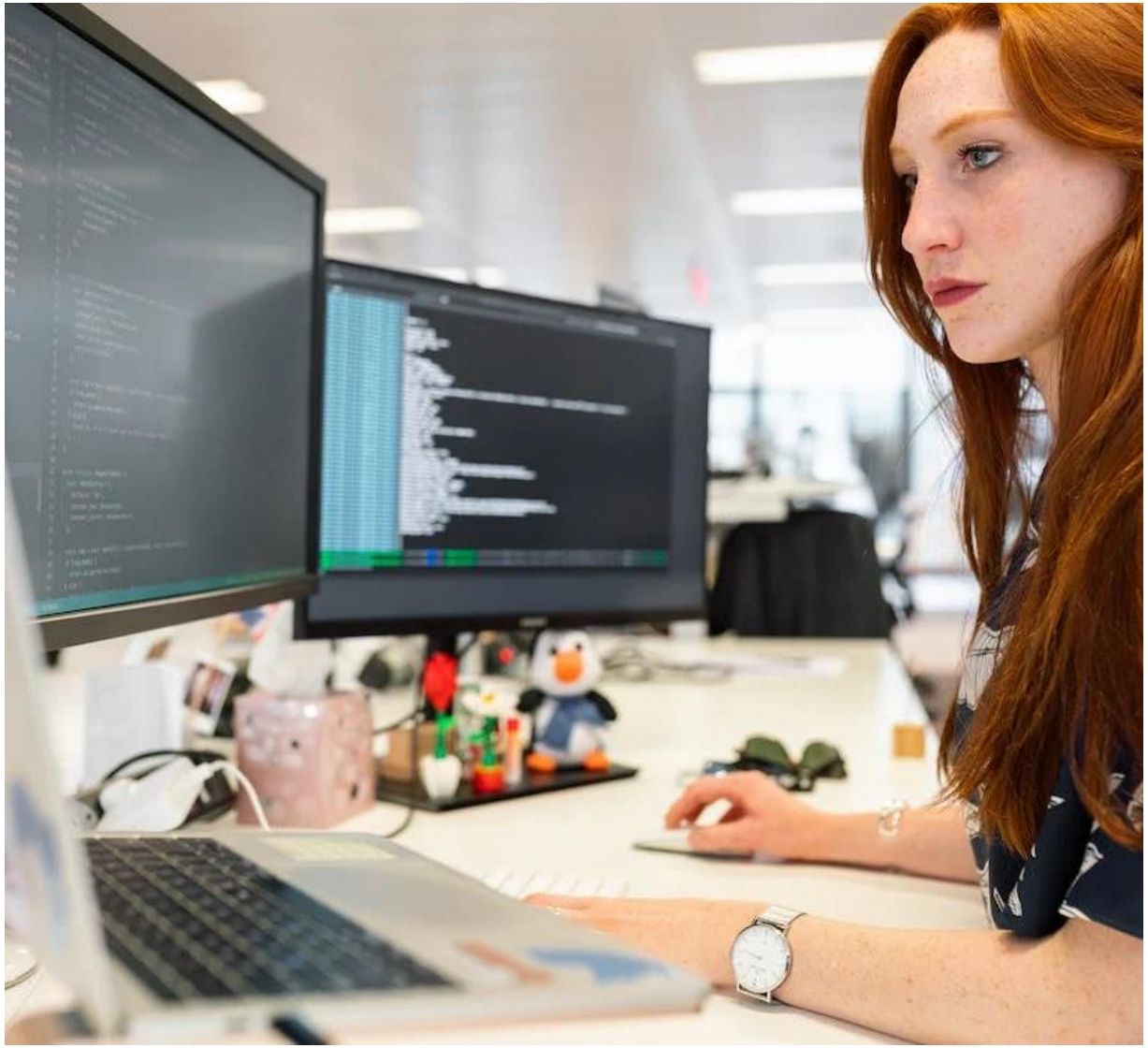
Sektion 02:

Beispielfall

02 Beispielfall
Alterungsrückstellungen berechnen

Ausgangslage

- **Anna** ist neu die **Verantwortliche Aktuarin** bei der kleinen Krankenversicherung **«Sicher Gesund».**
- «Sicher Gesund» vertreibt Spitalversicherungsprodukte mit Bedarf an **Alterungsrückstellungen** (AR).
- Anna nimmt die Berechnung der AR selber in die Hand.



02 Beispielfall
Prozess Alterungsrückstellungen

Berechnung der AR anhand einer eigens erstellten MS Excel Datei **Alterungsrück_v4.2.xlsm** ohne zentrales Monitoring der IT-Abteilung

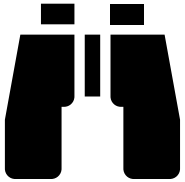
⇒ **EUC**

Input:
Vollständige Policen- und Schadensliste aus dem Primärsystem

Berechnungsschritt:
Berechnung der AR via EUC

Output:
AR an die Buchhaltung

02 Beispielfall
Beobachtungen



Annas Beobachtungen

- Kompletter Policenbestand inkl. Namen, Adressen, etc.
- EUC liegt auf einem Ordner, auf welchen alle Mitarbeiter Zugriff haben
- Unklar, ob die aktuelle Version des Berechnungstools getestet wurde
- Fehlende Dokumentation der Versionen
- Es gibt verschiedene Versionen der Datei und es ist nicht klar welche Version aktuell ist
- Keine spezielle Ablage, Prozessbeschreibung und Kontrollen rund um das EUC

Risiken

- Unbefugter Zugriff auf die Daten
- Besonders sensible Daten sind ungeschützt (Namen, Wohnadressen, etc.)
- Änderungen im Berechnungtools werden möglicherweise nicht ordnungsgemäß abgenommen => Berechnungsfehler und falsche Rückstellungen
- Daten und Versionen der Datei können im Falle eines Ausfalls verloren gehen oder nicht mehr verfügbar sein
- Es wird eine veraltete Version der Berechnungsdatei verwendet

02 Beispielfall
Beispiel 1 – Berechnung von Altersrückstellungen ohne Kontrolle

Situation

Dateninput mit Einträgen in unerwarteten Format (EUR anstatt CHF)

⇒ Gewisse Dateneinträge werden vom EUC nicht eingelesen

⇒ Berechnungsgrundlagen sind unvollständig

⇒ AR werden falsch berechnet und zur Buchung exportiert

Input:
Vollständige Policen- und Schadensliste in unerwarteten Format

Berechnungsschritt:
Berechnung der AR via EUC

Output:
Unzureichende AR an die Buchhaltung

Frage für das Publikum

Kennen Sie einfache Kontrollen um fehlerhafte Dateneingaben identifizieren zu können?

Beispiel 1 – Berechnung von Altersrückstellungen mit Kontrolle

Situation

Dateninput mit Einträgen in unerwarteten Format (EUR anstatt CHF)

⇒ Gewisse Dateneinträge werden vom EUC nicht eingelesen

⇒ Berechnungsgrundlagen sind unvollständig

⇒ AR werden falsch berechnet und zur Buchung exportiert

Kontrolle

Kontrolle zur Identifikation von unerwartetem Format des Inputs

⇒ Ausnahmebericht wird erstellt

⇒ Fehlerquelle wird identifiziert

⇒ Datenquelle kann überprüft und EUC angepasst werden

⇒ AR werden neu und korrekt berechnet

Input:
Vollständige Policen- und Schadensliste in unerwarteten Format

Berechnungsschritt:
Berechnung der AR via EUC

Output:
Fehlermeldung / Ausnahmebericht

02 Beispielfall
Beispiel 2 – Berechnung von Altersrückstellungen ohne Kontrolle

Situation

Änderungen an der Logik des EUC werden möglicherweise nicht ordnungsgemäß genehmigt oder sind nicht korrekt, was zu fehlerhaften Finanzdaten führen kann.

Input:
Vollständige Policen- und Schadensliste aus dem Primärsystem

Berechnungsschritt:
Berechnungen verlaufen nicht wie vorgesehen

Output:
Fehlerhafte AR an die Buchhaltung

Frage für das Publikum

Wichtigste Verhaltensregeln bei Änderungen innerhalb von EUC und Kontrollen für dauerhafte Funktionssicherheit?

Beispiel 2 – Berechnung von Altersrückstellungen mit Kontrolle

Situation

Änderungen an der Logik des EUC werden möglicherweise nicht ordnungsgemäß genehmigt oder sind nicht korrekt, was zu fehlerhaften Finanzdaten führen kann.

Kontrolle

Es muss sichergestellt werden, dass jede Änderung im EUC verfolgt und in einem Änderungsprotokoll dokumentiert wird:

- Namen der Personen, die die Änderungen durchgeführt und freigegeben haben (4-Augen-Prinzip)
- Das Datum und die Version der Freigabe
- Die Beschreibung der Änderungen

Input:
Vollständige Policen- und Schadensliste aus dem Primärsystem

Berechnungsschritt:
Berechnung der AR via EUC

Output:
AR an die Buchhaltung

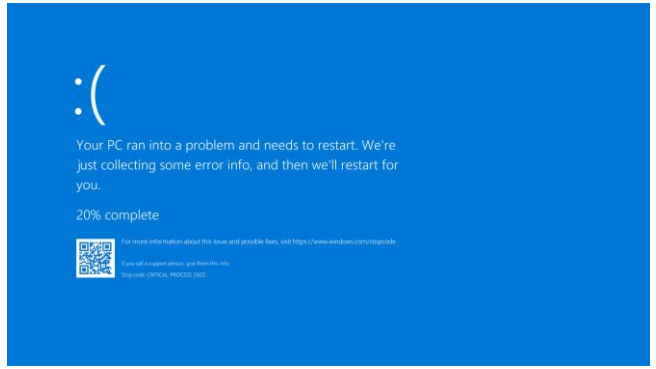
02 Beispielfall
Beispiel 3 – Berechnung von Altersrückstellungen ohne Kontrolle

Situation

EUC stürzt aufgrund eines technischen Fehlers ab

⇒ EUC Version v4.4 kann nicht mehr benützt werden

⇒ Entwicklungsfortschritt der EUC Version v4.4 geht permanent verloren



Input:
Vollständige Policen- und Schadensliste aus dem Primärsystem

Berechnungsschritt:
Systemabsturz – EUC nicht mehr benützbar

Output:
Es kann kein Output generiert werden

Beispiel 3 – Berechnung von Altersrückstellungen mit Kontrolle

Situation

EUC stürzt aufgrund eines technischen Fehlers ab

⇒ EUC Version v4.4 kann nicht mehr benützt werden

⇒ Entwicklungsfortschritt der EUC Version v4.4 geht permanent verloren

Kontrolle

Dokumentiertes Sicherungs- und Wiederherstellungsverfahren vorhanden

⇒ Sicherheitskopie der EUC Version v4.4 wurde zuvor auf einem separaten Drive im Server abgelegt

⇒ Version v4.4 kann zur Berechnung der AR wiederhergestellt werden

Input:
Vollständige Policen- und Schadensliste aus dem Primärsystem

Berechnungsschritt:
Systemabsturz – EUC kann durch eine Sicherheitskopie ersetzt werden.

Output:
AR an die Buchhaltung

Beispiel 4 – Berechnung von Altersrückstellungen ohne Kontrolle

Situation

Luzia, im Marketing tätig, hat Zugang auf das EUC.

Sie stellt fest, dass die Informationen in der Datei zu den Versicherungsnehmern für sie von grossem Interesse sind.

Sie schickt sich die sensiblen Vertragsinformationen auf die private E-Mailadresse.

Beispiel 4 – Berechnung von Altersrückstellungen mit Kontrolle

Situation

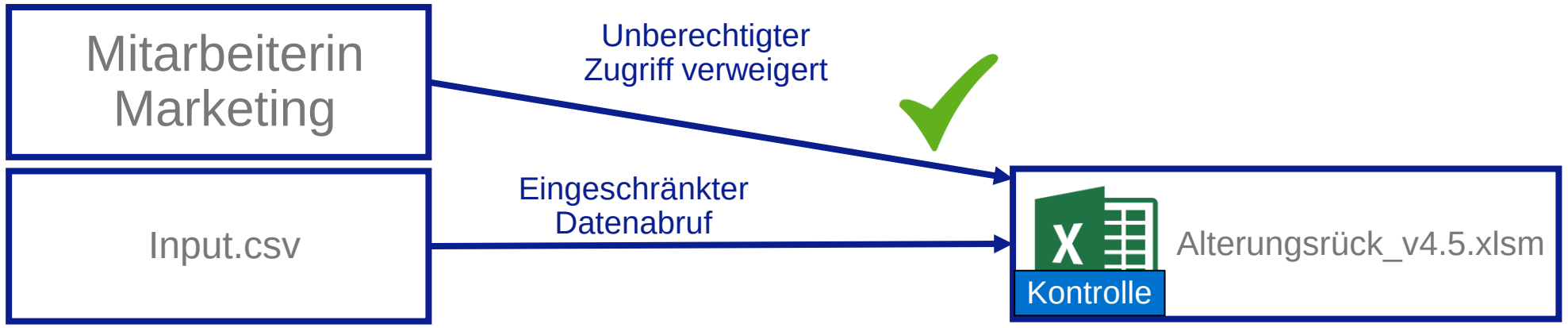
Luzia, im Marketing tätig, hat Zugang auf das EUC.

Sie stellt fest, dass die Informationen in der Datei zu den Versicherungsnehmern für sie von grossem Interesse sind.

Sie schickt sich die sensiblen Vertragsinformationen auf die private E-Mailadresse.

Kontrolle

Ein dokumentiertes Verfahren zur Verwaltung des Benutzerzugriffs muss beschreiben, wie unbefugte Zugriffe auf die EUC verhindert werden. Das Verfahren muss festlegen, wer auf die EUC zugreifen kann, wo sie sich befindet, wie auf sie zugegriffen werden kann (Speicherort, Passwort...) und zu welchem Zweck. Regelmässige Überprüfung der Liste der Benutzer, die Zugriff auf die EUC haben, und ggf. Aktualisierung dieser Liste.



03

Sektion 03:

Neues Datenschutzgesetz

Neues Schweizer Datenschutzgesetz ab 1.9.2023

Wichtige Änderungen und Angleich an EU

nicht abschliessend

Wo gilt es?

- Im In- und Ausland. Wirkungsbereich ist relevant
- Umgekehrtes gilt auch für die EU
- Datenschutzverantwortlicher in CH nicht Pflicht, aber Pflicht für EU Daten

Welche Daten?

- Neu nur von natürlichen Personen wie in EU
- Auch genetische und biometrische Daten sind besonders schützenswert

Transparenz

- Betroffene müssen immer informiert werden bei Datenbeschaffung. Auch bei nicht besonders schützenswerten Daten
- Informiert wird wer wo Daten erhebt und warum: **Strenger als EU**

Folgeabschätzung

- Neu muss bei der Bearbeitung von Daten, die ein hohes Risiko von Eingriff in Grundrechte und Persönlichkeitsrechte darstellen, eine dokumentierte Folgeabschätzung durchgeführt werden

Profiling

- Automatische Verarbeitung von Verhalten und persönlichen Aspekten
- Informationspflicht nur bei Profiling mit hohem Risiko: **weniger streng als EU**

Meldung bei Verlust

- So rasch als möglich an EDÖB melden (**EU in 72h)**
- Meldung an Betroffene, wenn nötig zu ihrem Schutz oder von Behörde verlangt

Privacy- by -Design

- Technik und Voreinstellungen der Applikationen müssen von Anfang an in der Architektur berücksichtigt werden
- Verzeichnis führen zur Datenerhebung (Ausnahmen für kleine Unternehmen)

Einwilligung

- Wenn über die Erhebung transparent informiert wird, braucht es diese **nicht. Anders als EU**
- Ausnahme: Schützenswerte Daten und Weitergabe an Dritte

Quelle: Neues DSG – was müssen Firmen beachten? (axa.ch)

04

Sektion 04:

Fazit

Unser Beispielfall
Alterungsrückstellungen Rechnen

Fazit: Welche Optimierung konnte Anna erreichen!

- Anonymisierter Input
- Zugriffsbeschränkung
- Review- und Genehmigungsprozess für Änderungen am EUC
- Sicherstellung, dass nur aktuellste Version verwendet wird
- Regelmässige Backups

Fragen?

Olivia Gradenwitz

olivia.gradenwitz@mazars.ch

+41 79 212 53 10

Marius Moser

marius.moser@mazars.ch

+41 75 433 58 71

Mazars

Herostrasse 12

8048 Zürich