BÄR
& KARRER

Welche Neuerungen birgt das revidierte Datenschutzgesetz im Arbeitsverhältnis?

Rehana Harasgama, Datenschutzexpertin

Versammlung der Fördergesellschaft des FAA, 29. November 2022

Agenda

BÄR & KARRER

Überblick über die Rechtsgrundlagen und wichtigsten Änderungen im revidierten Datenschutzgesetz	3
Umsetzung in der Praxis	9
Key Takeaways und Handlungsempfehlungen	18
Fragen und Diskussion	21
Kontakt	22

BÄR
& KARRER

Überblick über die Rechtsgrundlagen und wichtigsten Änderungen im revidierten Datenschutzgesetz

Obligationenrechtliche Grundlagen bleiben gleich

BÄR & KARRER

Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen **Eignung für das Arbeitsverhältnis** betreffen oder zur **Durchführung des Arbeitsvertrages** erforderlich sind. Im Übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (OR 328b).

"**Eignung** des Arbeitnehmers"

- Alle Personendaten über den Arbeitnehmer, deren Bearbeitung nach objektiven Gesichtspunkten **Aufschluss über die Eignung** des betreffenden Arbeitnehmers **für die jeweils zur Diskussion stehende Stelle** des Arbeitgebers oder der **zu erfüllenden Aufgaben geben** können.

"**Durchführung** des Arbeitsvertrags"

- Alle Personendaten über den Arbeitnehmer, deren Bearbeitung objektiv nötig ist, **um ein berechtigtes Interesse** des Arbeitgebers oder Arbeitnehmers **im Zusammenhang mit der Abwicklung des Arbeitsvertrages** des betroffenen Arbeitnehmers zu **erfüllen**.

Keine Bearbeitung von **privaten** Daten / Informationen

Grundsätzliches **Verbot von Verhaltensüberwachungen**

Datenschutzgrundsätze bleiben auch gleich

Ich darf Daten nur soweit notwendig teilen

Ich darf nicht mehr Daten bearbeiten als notwendig

Ich muss Daten irgendwann löschen

Ich darf Daten nur für einen bestimmten Zweck bearbeiten

Ich muss Daten korrigieren, wenn sie falsch sind

Ich muss Personen darüber informieren, wenn ich ihre Daten bearbeite

Einführung neuer Pflichten

Datensicherheit / Privacy-by-Design / Privacy-by-Default

Meldung von Verletzungen der Datensicherheit

Informationspflicht (Achtung bei automatisierten Einzelfallentscheiden)

Führung eines Datenbearbeitungsverzeichnisses

Durchführung von Datenschutz-Folgenabschätzungen

Outsourcing von Datenbearbeitungsprozessen

Transfer von Daten ins Ausland

Einführung eines neuen Rechtes

Auskunftsrecht

Berichtigungsrecht

Löschungsrecht

Widerspruchsrecht

Datenherausgabe oder -Übertragung

Beschwerde an Aufsichtsbehörde

Einschränkungsrecht

Schadenersatz / Genugtuung

Einführung höherer Bussen

BÄR & KARRER

- **Keine Busse** für die **Verletzung der Datenschutzgrundsätze** → zivilrechtliche **Ansprüche** der betroffenen Person (Löschung, Korrektur, Schadenersatz, Unterlassung etc.)
- **Untersuchungen / Verfügungen des EDÖB**
- **Busse** von max. **CHF 250'000.-** gegen **Individuen** (auf Antrag) für bestimmte, **vorsätzliche** Verstösse (z.B.):
  - Falsche oder unvollständige Information
  - Falsche oder unvollständige Auskunft
  - Nichterfüllung der festgelegten Mindeststandards an Datensicherheit
  - Verletzung der Sorgfaltspflichten für Auslanddatentransfers
  - Verletzung der Sorgfaltspflichten für Outsourcing von Datenbearbeitungsprozessen
  - Missachten von Verfügungen des EDÖB
- Busse von max. **CHF 50'000.-** gegen das **Unternehmen**

- Im Gegensatz dazu sieht **EU-DSGVO Bussen bis zu 4% des weltweiten Umsatzes oder EUR 20 mio**. vor (was höher ist)
- Im Gegensatz zur EU-DSGVO werden grundsätzlich die **verantwortlichen Individuen gebüsst** und nicht das Unternehmen
- Verantwortliche Individuen: **Verwaltungsrat**, **Geschäftsleitung**, **Abteilungsleiter** etc. → Personen, die Entscheide über den Datenschutz treffen

BÄR
& KARRER

Umsetzung in der Praxis

Drei Säulen

BÄR & KARRER

Säule 1

Datenschutz-organisation

Säule 2

Richtlinien & Prozesse

Säule 3

Schulungen & Stresstests

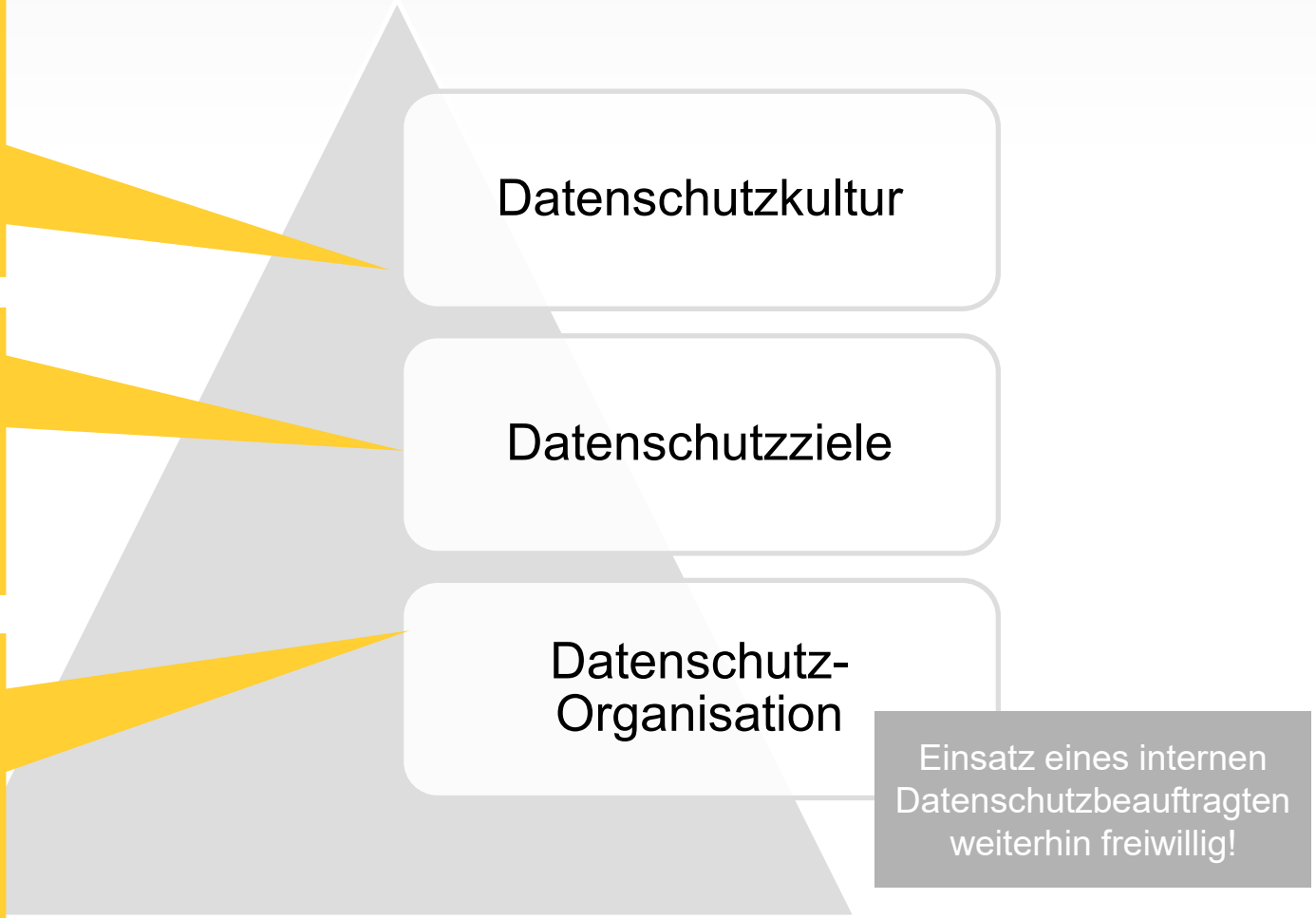
Datenschutzorganisation

BÄR & KARRER

- Muss zur Organisation passen
- Muss von allen (vor-)gelebt werden
- Muss institutionalisiert werden
- Legt den Stellenwert von Datenschutz innerhalb der Organisation fest

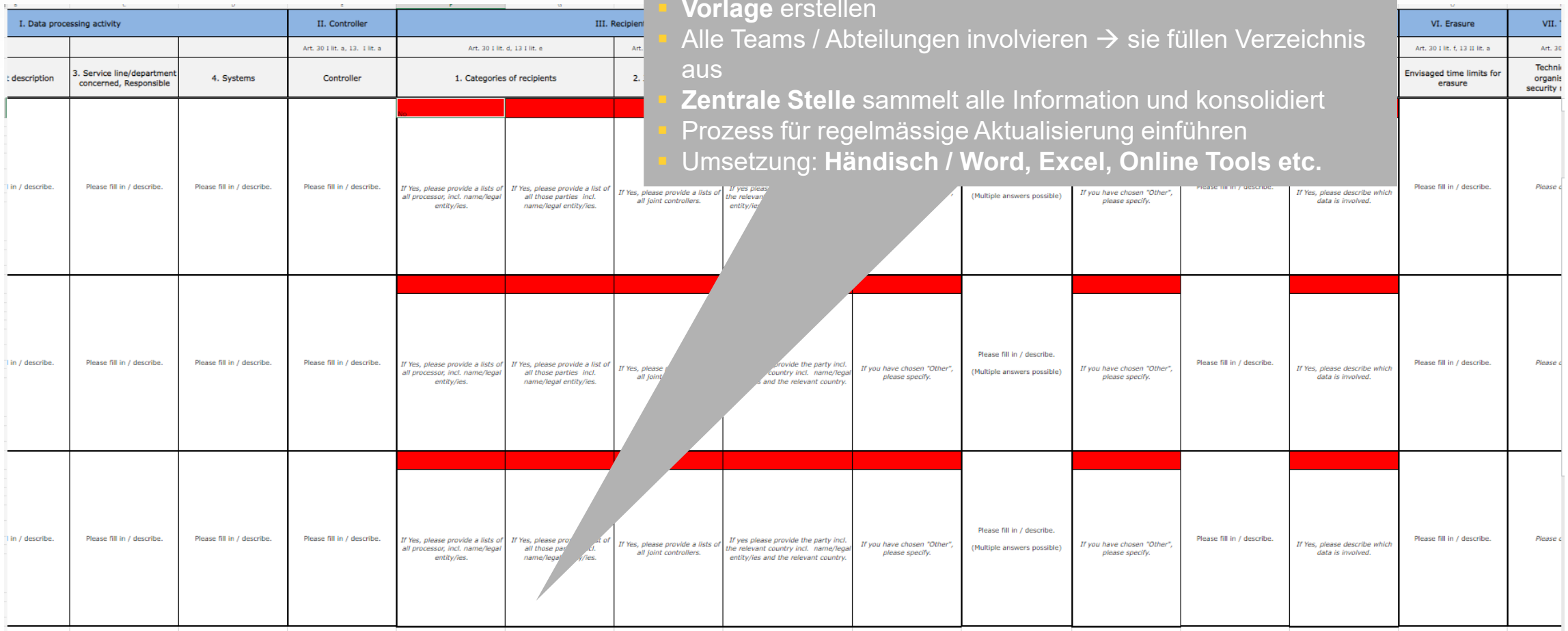
- Prioritäten in Bezug auf Datenschutz festlegen
- Datenethik (was werden wir sicher nie mit Daten machen?)
- Ziele für Organisation und Mitarbeitende festlegen

- Welche Rollen soll es geben?
- Soll Datenschutz zentral oder dezentral geregelt werden?
- Zusammenarbeit mit IT-/Cyber-Security Team?
- Wie viele "Lines of Defence" brauchen wir?



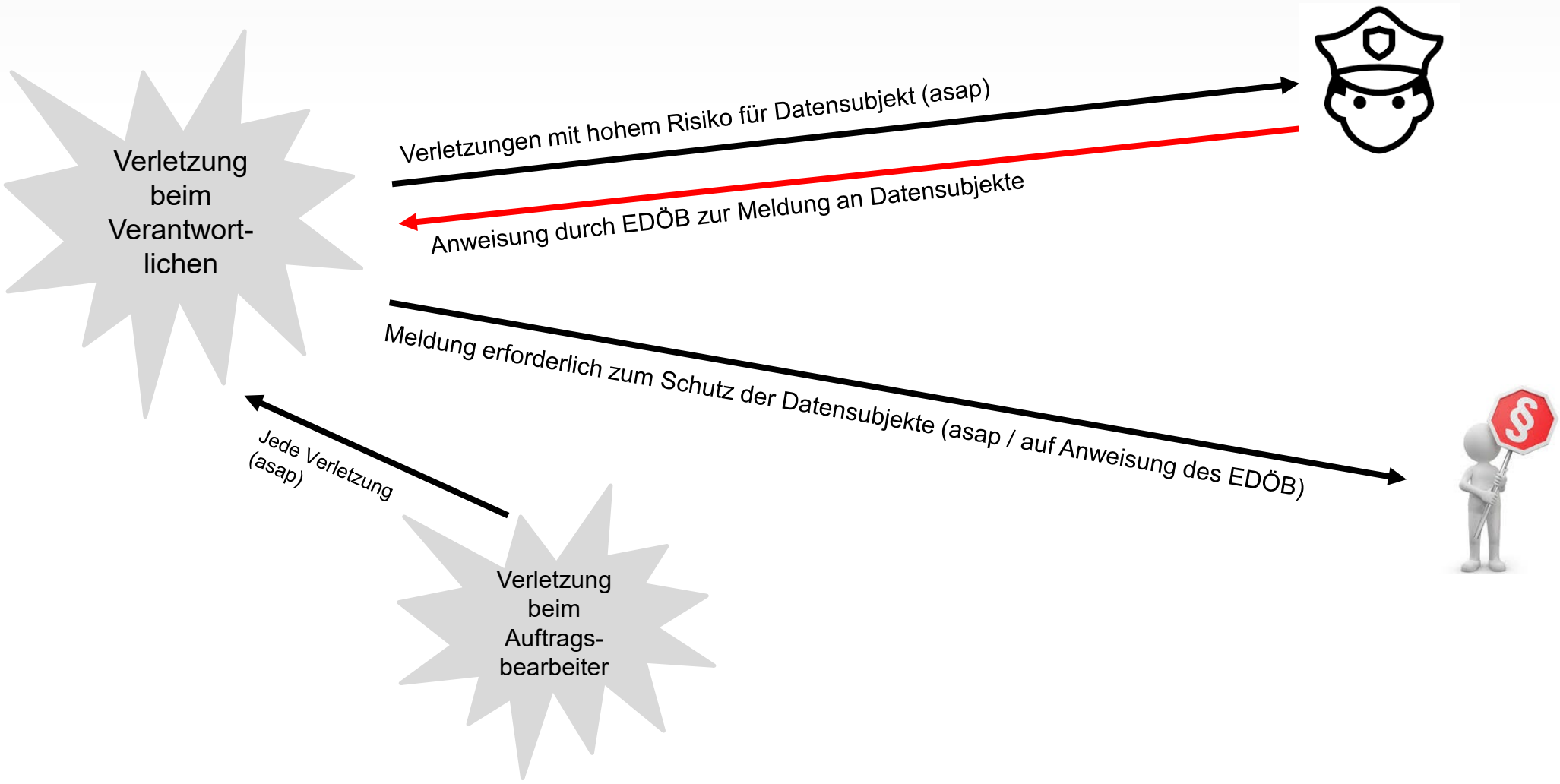
Datenbearbeitungsverzeichnis

- **Data Mapping** durchführen
- Verantwortlichkeit für Datenbearbeitungsverzeichnis festlegen
- **Vorlage** erstellen
- Alle Teams / Abteilungen involvieren → sie füllen Verzeichnis aus
- **Zentrale Stelle** sammelt alle Information und konsolidiert
- Prozess für regelmässige Aktualisierung einführen
- Umsetzung: **Händisch / Word, Excel, Online Tools etc.**



I. Data processing activity			II. Controller	III. Recipient						VI. Erasure	VII.
			Art. 30 I lit. a, 13. I lit. a	Art. 30 I lit. d, 13 I lit. e	Art.					Art. 30 I lit. f, 13 II lit. a	Art. 30
description	3. Service line/department concerned, Responsible	4. Systems	Controller	1. Categories of recipients	2.					Envisaged time limits for erasure	Technical organisational security
in / describe.	Please fill in / describe.	Please fill in / describe.	Please fill in / describe.	If Yes, please provide a lists of all processor, incl. name/legal entity/ies.	If Yes, please provide a list of all those parties incl. name/legal entity/ies.	If Yes, please provide a lists of all joint controllers.	If yes pleas the relevant entity/ies		(Multiple answers possible)	If you have chosen "Other", please specify.		If Yes, please describe which data is involved.	Please fill in / describe.	Please
in / describe.	Please fill in / describe.	Please fill in / describe.	Please fill in / describe.	If Yes, please provide a lists of all processor, incl. name/legal entity/ies.	If Yes, please provide a list of all those parties incl. name/legal entity/ies.	If Yes, please all joint	provide the party incl. country incl. name/legal and the relevant country.	If you have chosen "Other", please specify.	Please fill in / describe. (Multiple answers possible)	If you have chosen "Other", please specify.	Please fill in / describe.	If Yes, please describe which data is involved.	Please fill in / describe.	Please
in / describe.	Please fill in / describe.	Please fill in / describe.	Please fill in / describe.	If Yes, please provide a lists of all processor, incl. name/legal entity/ies.	If Yes, please pro all those par name/legal	If Yes, please provide a lists of all joint controllers.	If yes please provide the party incl. the relevant country incl. name/legal entity/ies and the relevant country.	If you have chosen "Other", please specify.	Please fill in / describe. (Multiple answers possible)	If you have chosen "Other", please specify.	Please fill in / describe.	If Yes, please describe which data is involved.	Please fill in / describe.	Please

Meldung von Verletzungen der Datensicherheit

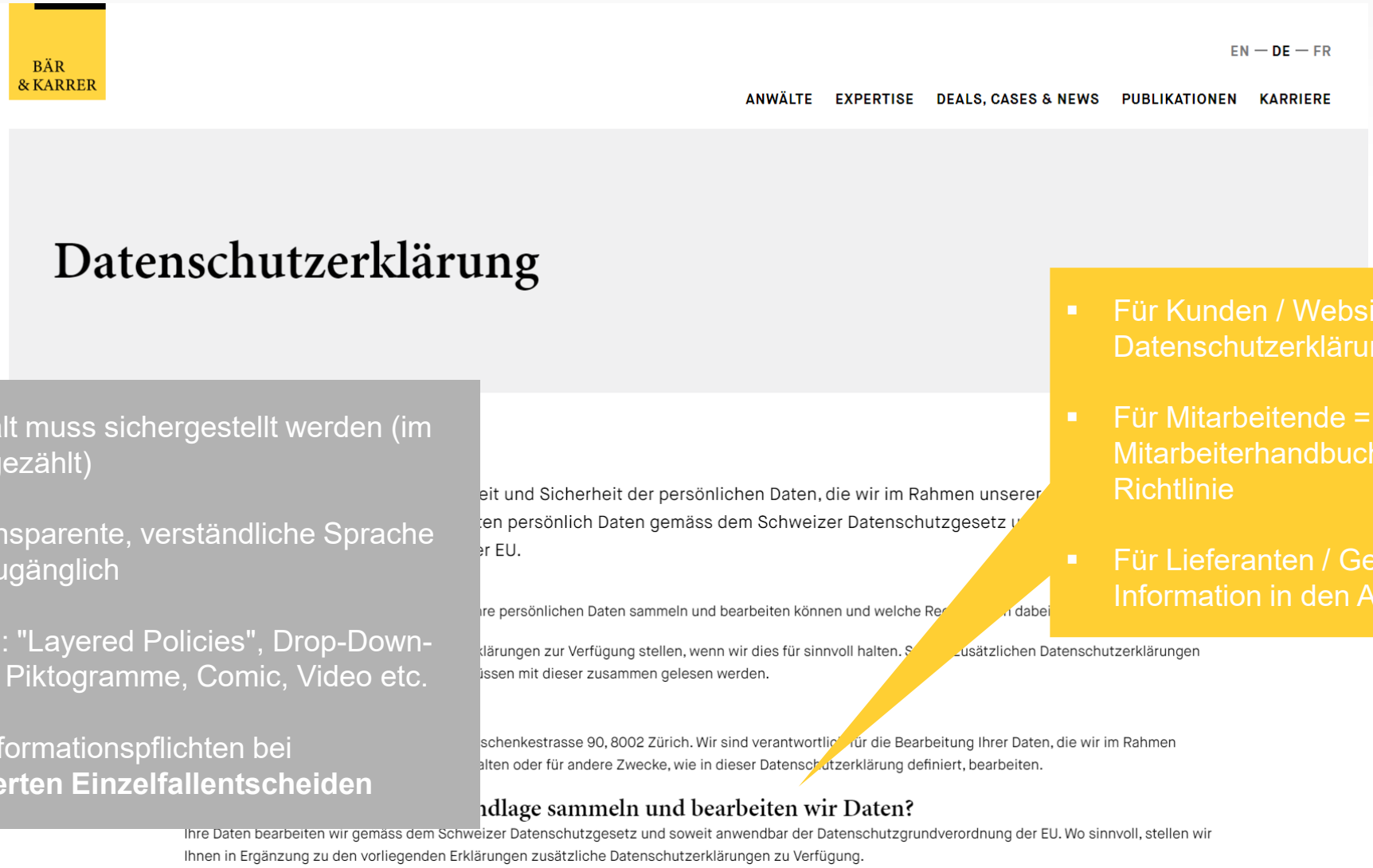


Meldung von Verletzungen der Datensicherheit

BÄR & KARRER

- Klare Verantwortlichkeiten festlegen und Mitarbeitenden mitteilen
- **Mitarbeitende schulen** bzgl. was gemeldet und an wen gemeldet werden muss
- **Formular** für interne Meldung an verantwortliche Person erstellen
- **Internen Prozess** definieren bzgl. wie Verantwortliche vorgehen müssen (z.B. Untersuchung und Analyse des Vorfalls, Massnahmen definieren, Meldung vornehmen etc.) und wen sie hinzuziehen müssen (z.B. Rechtsberater, IT-Spezialisten, Kommunikationsabteilung, Versicherung etc.)
- Prozess muss so aufgesetzt sein, dass Meldungen rasch behandelt und analysiert werden können und Meldungen an den EDÖB oder die Betroffenen innert kurzer Frist (in der EU: 72 Stunden) vorgenommen werden können → gestaffelte Meldungen möglich
- **Cyber-Versicherung** abschliessen?
- **Bitcoin-Account** erstellen? → bei Ransomware-Attacks wird Lösegeld oft in Bitcoins verlangt
- Meldungen bzw. auch Entscheide, nicht zu melden, müssen während **zwei Jahren aufbewahrt** werden

Informationspflicht



- Mindestinhalt muss sichergestellt werden (im Gesetz aufgezählt)
- Präzise, transparente, verständliche Sprache und leicht zugänglich
- Empfehlung: "Layered Policies", Drop-Down-Funktionen, Piktogramme, Comic, Video etc.
- Spezielle Informationspflichten bei **automatisierten Einzelfallentscheiden**

- Für Kunden / Website-Besucher = Datenschutzerklärung
- Für Mitarbeitende = Information in Mitarbeiterhandbuch oder interner Richtlinie
- Für Lieferanten / Geschäftspartner = Information in den AGB

Datenschutz-Folgenabschätzung

BÄR & KARRER

Nur wenn: **hohes Risiko** für die Persönlichkeit oder die Grundrechte der betroffenen Person → gilt **nur für neue Datenbearbeitungsprozesse**

- Neue Technologien
- Zweck der Bearbeitung
- Umfang der Bearbeitung
- Art der Bearbeitung

Umsetzung:

- **Interne Richtlinie** einführen, die klar bestimmt, wann eine Datenschutz-Folgenabschätzung durchgeführt werden muss (z.B. beim Einsatz neuer Technologien zu Marketingzwecken oder wenn sensible Daten bearbeitet werden)
- Wenn neue Produkte entwickelt werden, Voreinschätzung durchführen und dann je nach Komplexität und Art der bearbeiteten Daten oder eingesetzter Technologien Datenschutz-Folgenabschätzung durchführen
- **Verantwortlichkeiten** definieren
- **Kontaktperson** für Fragen / Voreinschätzung definieren

Achtung: Besonders schützenswerte Daten oder Profiling mit hohem Risiko

BÄR & KARRER

Protokollierungspflicht

Wann?

- Automatisierte Bearbeitung;
- Umfangreiche Bearbeitung besonders schützenswerter Daten oder Profiling mit hohem Risiko; und
- Massnahmen gemäss DSFA sind ungenügend

Wer?

- Organisation UND Dritte, die Daten für Organisation bearbeiten

Was?

- Speicherung, Veränderung, Lesen, Bekanntgabe, Löschung und Vernichtung
- Identität; Art, Datum und Uhrzeit der Bearbeitung; Empfänger
- Aufbewahrung mind. 1 Jahr getrennt vom "Ursprungs-"System

Bearbeitungsreglement

Wann?

- Automatisierte Bearbeitung;
- Umfangreiche Bearbeitung besonders schützenswerter Daten oder Profiling mit hohem Risiko; und
- Massnahmen gemäss DSFA sind ungenügend

Wer?

- Organisation UND Dritte, die Daten für Organisation bearbeiten

Was?

- Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Datensicherheitsmassnahmen
- Regelmässige Aktualisierung

BÄR
& KARRER

Key Takeaways und Handlungsempfehlungen

Key Takeaways

BÄR & KARRER

- Das neue Datenschutzgesetz tritt am **1. September 2023** in Kraft
- Organisationen haben weniger als ein Jahr Zeit, die neuen Vorgaben umzusetzen
- Grundsätze bleiben gleich → ABER: neue Pflichten kommen, Datenportabilität wir eingeführt, höhere Bussen drohen
- Arbeitsrechtliche Vorgaben bleiben gleich
- **Alles ist nicht auf einmal zu schaffen** → risiko-basiertes Vorgehen (Road-Map erstellen), gestaffelt Compliance erreichen
- Datenschutzorganisation → klare Zuständigkeiten schaffen
- Richtlinien und Prozesse implementieren
- **Schulungen der Mitarbeitenden** (periodisch) durchführen und regelmässig aktualisieren
- **Regelmässige Überprüfung / Aktualisierung** der Richtlinien, Massnahmen und Prozesse

Stufenplan

BÄR & KARRER

Stufe 1

- Durchführung einer **Gap-Analyse** bzgl. aktueller Umsetzung des Datenschutzes (insbesondere auch bzgl. EU-DSGVO)
- Überprüfung / Mapping aller **Datenbearbeitungsprozesse** (inkl. Profiling und automatisierter Einizelfallentscheide)
- Festlegung der **internen Verantwortlichkeiten** und Datenschutzorganisation

Stufe 2

- Überprüfung und Aktualisierung der **Datenschutzerklärung / Verträge**
- Überprüfung bestehender **Auftragsdatenbearbeitungen** durch Dritte / durch Organisation selber; Implementierung notwendiger Verträge und Massnahmen
- Überprüfung von **Auslanddatentransfers**; Implementierung notwendiger Verträge und Massnahmen

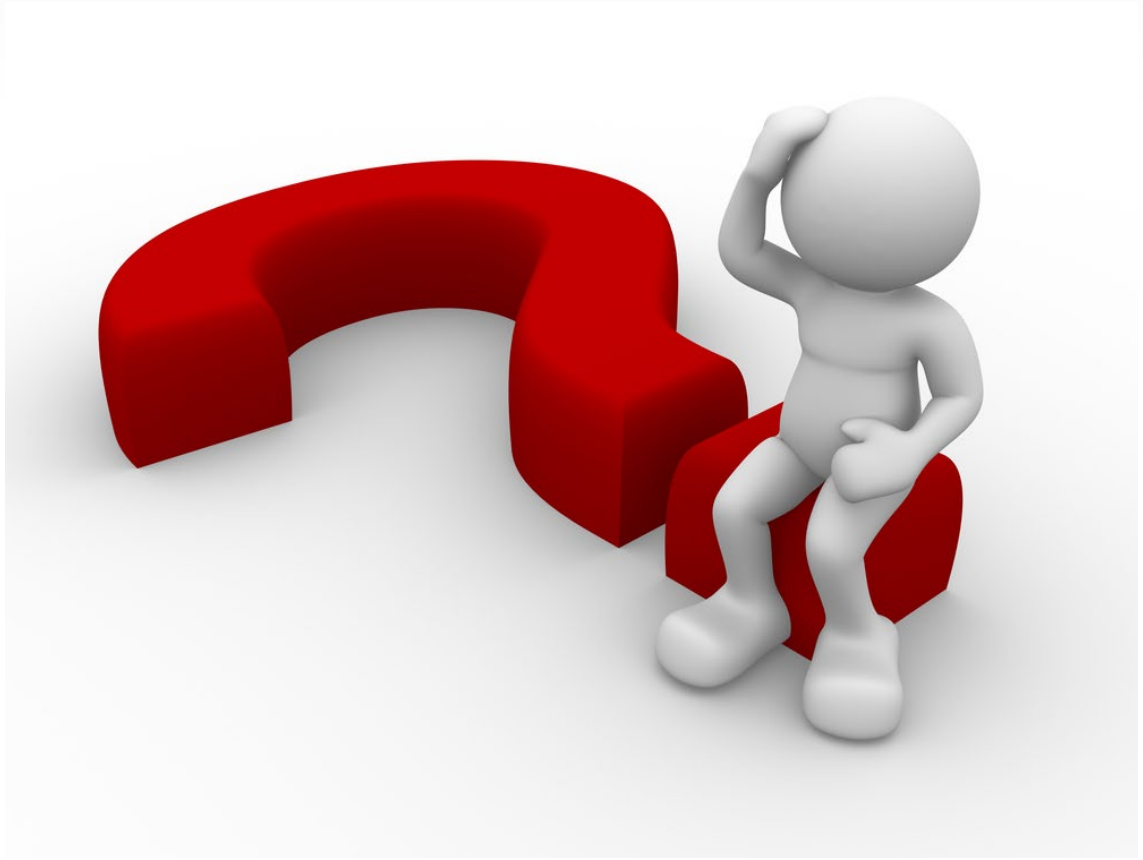
Stufe 3

- Überprüfung und Aktualisierung der **Datensicherheitsmassnahmen** → Protokollierung und Bearbeitungsreglement
- Überprüfung und Implementierung eines Prozess zur **Meldung von Datensicherheitsverletzungen**
- Überprüfung und Aktualisierung des Prozesses zur **Gewährung der Betroffenenrechte**
- Implementierung eines Prozesses / Festlegung der Verantwortlichkeiten für das **Datenverarbeitungsverzeichnis**

Stufe 4

- Überprüfung Notwendigkeit und Einführung eines Verfahrens / Zuweisung der Verantwortung für die **Datenschutz-Folgenabschätzung**
- Implementierung eines Verfahrens bzgl. **privacy-by-design und privacy-by-default**

Fragen und Diskussion



Kontakt

Zürich
Brandschenkestrasse 90
8027 Zürich

Basel
Lange Gasse 47
4052 Basel

Genf
12, quai de la Poste
1211 Genf 11

Zug
Baarerstrasse 8
6301 Zug

Lugano
Via Vegezzi 6
6901 Lugano