

Dr. Sybille Wünsche, Steuerberater

**WJ-Themenabend:
Datenschutzgrundverordnung**

Bautzen, 10.04.2018

Inhaltsverzeichnis

I. Überblick DSGVO

II. Pflichten der Unternehmer

1. Informationspflichten an den Betroffenen
2. Verzeichnisse
3. Datenschutzbeauftragter
4. Meldepflichten bei „Datenpannen“
5. Beispiel: Wesentliche DSGVO-Anforderungen für Einzelhändler

III. Rechte der Betroffenen

1. Auskunftsrecht
2. Recht auf Löschung / „Vergessenwerden“
3. Recht auf Berichtigung und Sperrung

I. Überblick DSGVO



99 / 88



I. Überblick DSGVO

25. Mai 2018

innerhalb der EU, auch Niederlassungen ausländischer Unternehmen in der EU

jede personenbezogene Datenverarbeitung im Unternehmen unabhängig von Rechtsform und Art der Verarbeitung (nicht- /automatisiert)

Personenbezogene Daten = alle Informationen, die eine Identifizierung einer **natürlichen** Person unmittelbar oder mittelbar ermöglichen

Pflichten der Unternehmer:

- Informationspflichten
- Verarbeitungsverzeichnis
- Datenschutzbeauftragter
- Meldepflichten
- ➔ Bei Verstößen: Bußgeld

Rechte der Betroffenen:

- Auskunftsrecht
- Recht auf Löschung
- Recht auf Berichtigung und Sperrung

I. Überblick DSGVO

Wann dürfen personenbezogene Daten verarbeitet werden?

Grundsatz: Datenverarbeitung ist verboten!

Ausnahme: Sie ist nur gestattet, wenn ausdrücklich durch Verordnung oder Gesetz erlaubt!

Relevante Ausnahmetatbestände:

- Erfüllung eines Vertrages oder rechtlicher Verpflichtung
- Wahrung berechtigter Interessen des Verantwortlichen oder Dritter
- Schutz lebenswichtiger Interessen des Betroffenen
- Wahrnehmung einer Aufgabe im öffentlichen Interesse
- Ausdrückliche Einwilligung des Betroffenen

II. Pflichten der Unternehmer



1. Informationspflichten an den Betroffenen

Betroffener	Welche Daten	Ersterhebung	Information durch Datenschutzhinweis
Besucher der Homepage	z.B. IP-Adresse, bei Nutzung von Kontaktformularen	IP-Adresse sofort beim Aufruf der Homepage, Formulardaten beim Absenden des Formulars	Muss sofort beim Aufruf der Homepage einsehbar sein (Direktverlinkung von der Startseite)
Interessent, telefonische Kontaktaufnahme	Name, Kontaktdaten	Notiz der Informationen während des Gesprächs	Anrufer muss auf Datenschutzinformation hingewiesen werden (z. B. Link auf Homepage) & kann diese vor Herausgabe der Daten anfordern
Mitarbeiter	alle im Rahmen des Arbeitsvertrages erforderlichen Daten	bei Abschluss Arbeitsvertrag	in gleicher Form wie Arbeitsvertrag, idR schriftlich

(in Anlehnung an: Haufe, Serie Steuerberater, Datenschutz und die EU-Datenschutz-Grundverordnung; www.haufe.de)

2. Verarbeitungsverzeichnis

Verzeichnis von Verarbeitungstätigkeiten: Übersicht über **alle** Verarbeitungsvorgänge, die für personenbezogene Daten relevant sind

Wesentliche Inhalte:

- Name, Kontaktdaten des Verantwortlichen, Vertretung / ggf. Datenschutzbeauftragter
- Verfahrensbezeichnung & Zweck der Verarbeitung
- Beschreibung betroffener Personengruppen, der personenbezogenen Daten oder Datenkategorien
- Kategorien von Empfängern, gegenüber denen personenbezogene Daten offengelegt worden sind
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Beispielhafte

Verarbeitungsvorgänge:

- Personalwesen und Bewerbermanagement
- Angebotserstellung für Interessenten
- Datenpflege der Bestandskunden
- Angaben in Jahresabschlüssen
- Werbung

- regelmäßige Aktualisierung bei neuen Vorgängen
- ggf. Durchführung einer Datenschutz-Folgenabschätzung

2. Verarbeitungsverzeichnis

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten“ gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lida.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für
Datenschutzaufsicht



Muster 3: Handwerksbetrieb – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:

ABC Install GmbH
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@abcinstall.de
Web: www.abcinstall.de

Geschäftsführerin: Susanne Kühnlein, geb. 03.12.1952

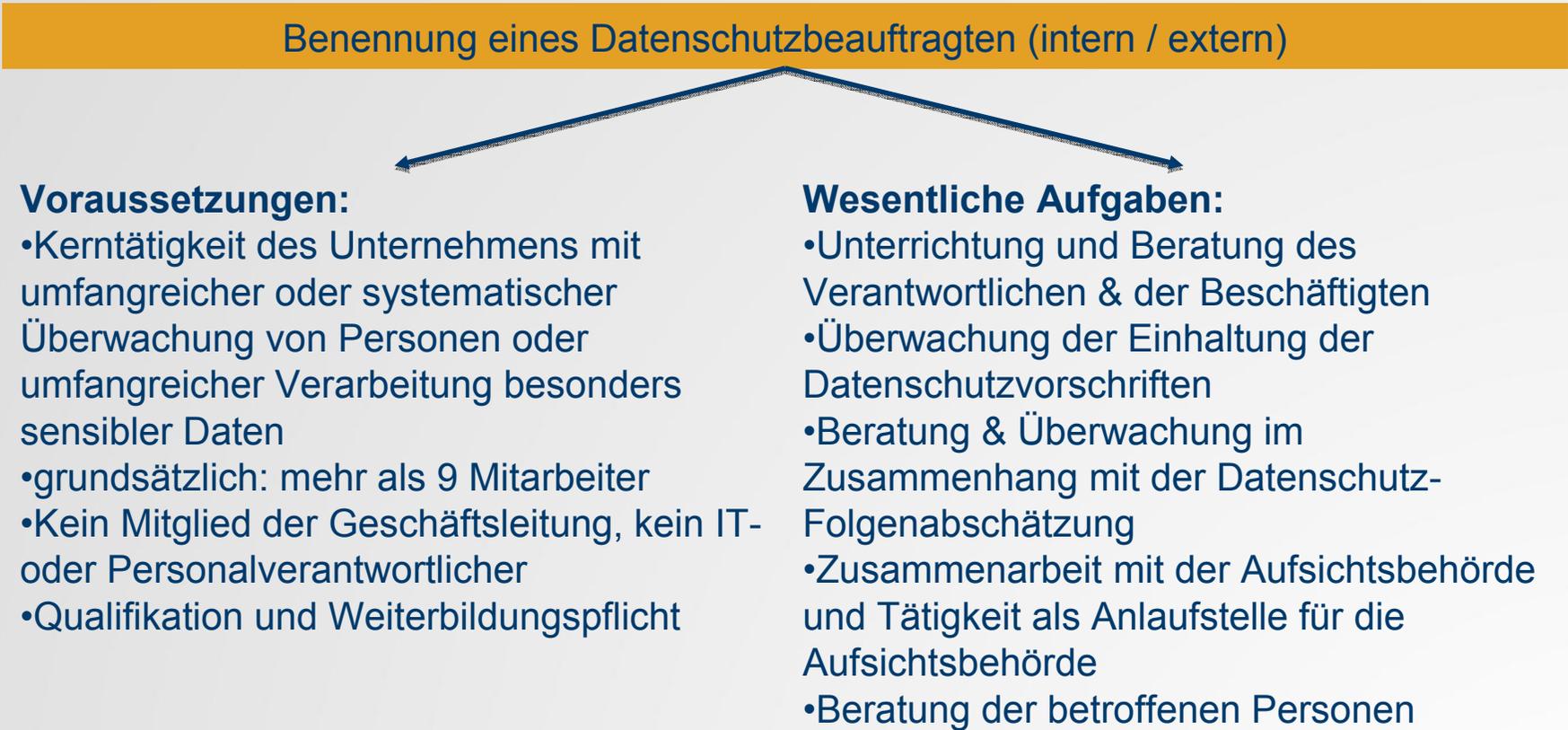
Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbezogenen Daten	Kategorie von Empfängern	Drittlandstransfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über Steuerberater)	Herbert Bauer 0981/123456-1 herbert@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> Auszahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern 	Beschäftigte	<ul style="list-style-type: none"> Name, Geburtsdatum Adresse Bankverbindungsdaten Lohn-/Entgelt Daten ggf. Religionszugehörigkeit Sozialversicherungsdaten Steuerdaten (Steuerklasse, Freibeträge,...) Berufsgenossenschaftsangaben 	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Personalverwaltung	Herbert Bauer 0981/123456-1 herbert@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> Personaladministration Personalführung Arbeitszeitverwaltung Personalbeschaffung (betrifft Bewerber) 	<ul style="list-style-type: none"> Beschäftigte Auszubildende Bewerber 	<ul style="list-style-type: none"> Name, Adressen Zeitzwirtschaftsdaten Daten zur Arbeitsleistung Leistungsbeurteilung Lebenslauf und Bewerbungsunterlagen (betr. Bewerber) 	Keine	Keine	<ul style="list-style-type: none"> Beschäftigte: in der Regel ca. 3 Jahre nach Ausscheiden abgelehnte Bewerber: 6 Monate nach Abschluss des Bewerbungsverfahrens 	Siehe IT-Sicherheitskonzept
Betrieb der Firmenwebseite (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@abcinstall.de	28.02.2018	Außendarstellung	<ul style="list-style-type: none"> Webseitenbesucher 	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Kundenverwaltung	Janine Kleinlein 0981/123456-2 janine@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> Bearbeitung von Aufträgen inkl. Rechnungstellung postalische Werbung 	Kunden	<ul style="list-style-type: none"> Name, Adresse Angaben zum Auftrag ggf. Bankverbindungsdaten 	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Aktueller Virens Scanner/Sicherheitssoftware
- ✓ Papieraktenvernichtung mit Standard-Shredder

3. Datenschutzbeauftragter

Benennung eines Datenschutzbeauftragten (intern / extern)



Voraussetzungen:

- Kerntätigkeit des Unternehmens mit umfangreicher oder systematischer Überwachung von Personen oder umfangreicher Verarbeitung besonders sensibler Daten
- grundsätzlich: mehr als 9 Mitarbeiter
- Kein Mitglied der Geschäftsleitung, kein IT- oder Personalverantwortlicher
- Qualifikation und Weiterbildungspflicht

Wesentliche Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen & der Beschäftigten
- Überwachung der Einhaltung der Datenschutzvorschriften
- Beratung & Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde und Tätigkeit als Anlaufstelle für die Aufsichtsbehörde
- Beratung der betroffenen Personen

4. Meldepflichten bei „Datenpannen“

Personenbezogene Daten gelangen in unbefugte Hände
(Verlust, Offenlegung, Fremdzugriff)

und

Voraussichtliches Risiko für Betroffenen

- Meldung an Aufsichtsbehörde innerhalb 72 Stunden
Bundesbeauftragte für Datenschutz – www.bfdi.bund.de/DE/Datenschutz
- Einhaltung des Datenschutzrechts durch Unternehmen nachzuweisen
- Sanktionierung: Bußgeld 10 Mio. EUR / 2% des Umsatzes
- Benachrichtigung der betroffenen Person, wenn hohes Risiko für deren Rechte und Freiheiten besteht

5. Beispiel: Wesentliche DSGVO-Anforderungen für Einzelhändler

Bayerisches Landesamt für
Datenschutzaufsicht



Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc.

Muster 12: Einzelhändler

Hinweis:

Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist ein sog. *Verantwortlicher*. Dieser ist insb. dafür verantwortlich, dass er die Anforderungen der DS-GVO einhält. In der folgenden Übersicht werden die *wesentlichen* Anforderungen exemplarisch zusammengestellt – ohne Anspruch auf Vollständigkeit. Zu beachten ist daher, dass nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. In diesem Muster wird deshalb der vereinfachte Regelfall angenommen. Erläuterungen zu den jeweiligen Anforderungen sind auf der Rückseite dieses Papiers zu finden.

🏠 Kurzbeschreibung des Einzelhändlers

Ein Einzelhändler für Bekleidung hat 20 Beschäftigte im Verkauf, zwei Änderungsschneiderinnen sowie zwei Beschäftigte in der Verwaltung. Der Einzelhändler gibt für Stammkunden eine Kundenkarte mit Rabattfunktion und für Marketing-Aktionen heraus. Lohnabrechnung und Finanzbuchhaltung macht ein externes Buchhaltungsbüro. Auf einer Webseite stellt sich der Einzelhändler mit seinem Unternehmen dar und nennt seine Öffnungszeiten.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohnabrechnung (über das externe Buchhaltungsbüro)
- Betrieb der Webseite (über Hosting-Paket eines externen Dienstleisters)
- Kundenkartenverwaltung
- Abwicklung von EC-Karten- und Kreditkartenzahlungen (über einen Zahlungsdienstleister)
- Werbemaßnahmen zur Kundengewinnung und -bindung mittels gelegentlichen Werbebriefaktionen

5. Beispiel: Wesentliche DSGVO-Anforderungen für Einzelhändler

☑ Wesentliche DS-GVO-Anforderungen für den Einzelhändler

A Datenschutzbeauftragter (DSB)

Muss ein DSB vom Händler benannt werden?

- ja
 nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

B Verzeichnis von Verarbeitungstätigkeiten

Ist ein solches Verzeichnis erforderlich?

- ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)
 nein

C Datenschutz-Verpflichtung von Beschäftigten

Ist eine solche Verpflichtung durchzuführen?

- ja (bei den Mitarbeitern, die mit personenbezogenen Daten umgehen)
 nein

D Information- und Auskunftspflichten

Bestehen irgendwelche Informationspflichten?

- ja (insb. auf der Webseite in der Datenschutzerklärung sowie bei Kundenkarten)
 nein

E Löschen von Daten

Gibt es eine Anforderung zur Datenlöschung?

- ja (insb. der Kundendaten, aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
 nein

F Sicherheit

Müssen die Daten besonders gesichert werden?

- ja
 nein (etablierte Standardmaßnahmen sind ausreichend, um die Daten effektiv zu schützen)

G Auftragsverarbeitung

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

- ja (u.a. mit dem Zahlungsdienstleister und Buchhaltungsbüro)
 nein

H Datenschutzverletzungen

Müssen bestimmte Vorfälle gemeldet werden?

- ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)
 nein

I Datenschutz-Folgeabschätzung (DSFA)

Muss eine DSFA vom Händler durchgeführt werden?

- ja
 nein (da kein hohes Risiko bei der Datenverarbeitung im Betrieb besteht)

J Videoüberwachung (VÜ)

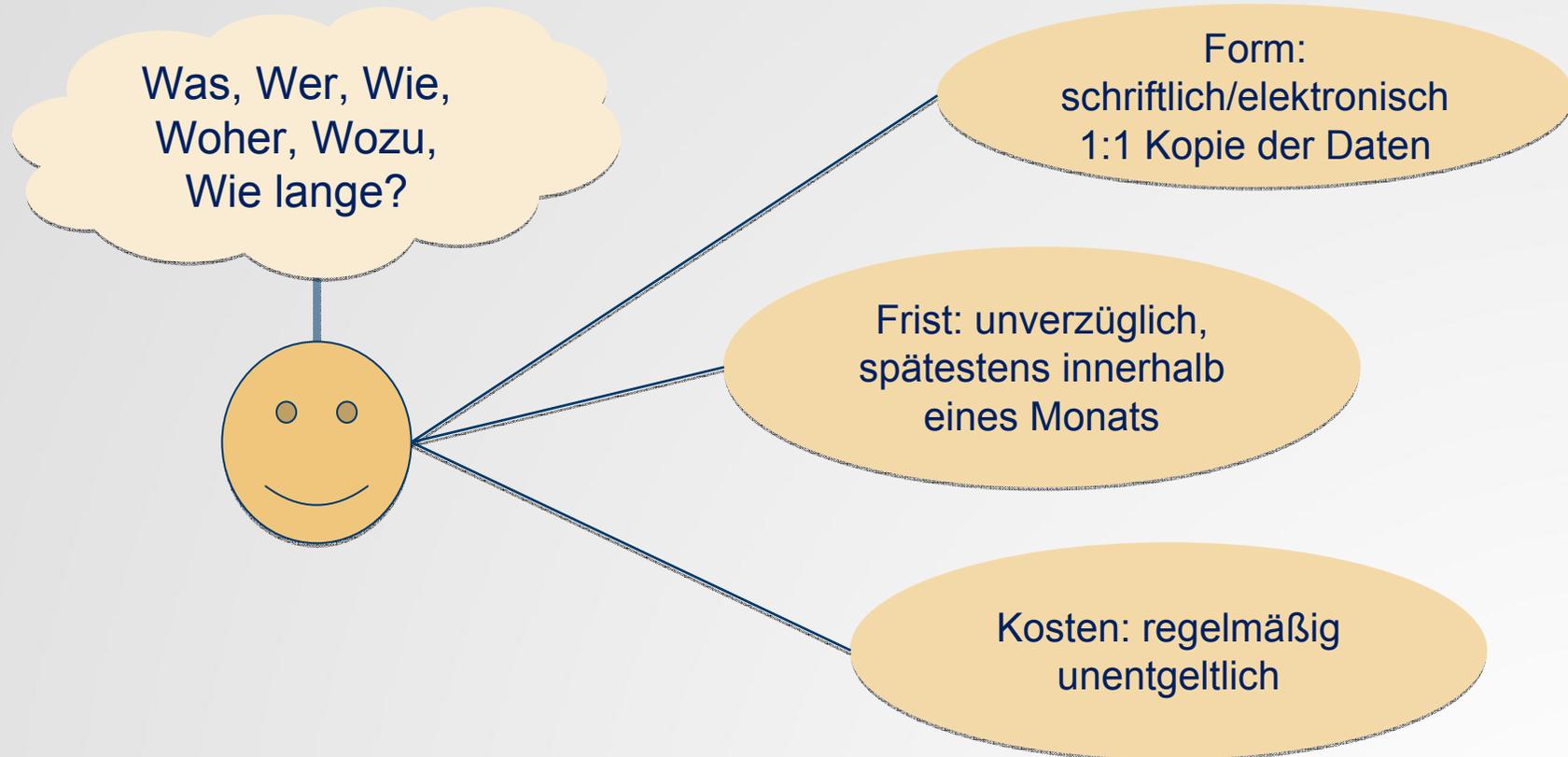
Besteht eine Ausschilderungspflicht bezüglich VÜ?

- ja
 nein (da keine Videoüberwachung vom Unternehmen durchgeführt wird)

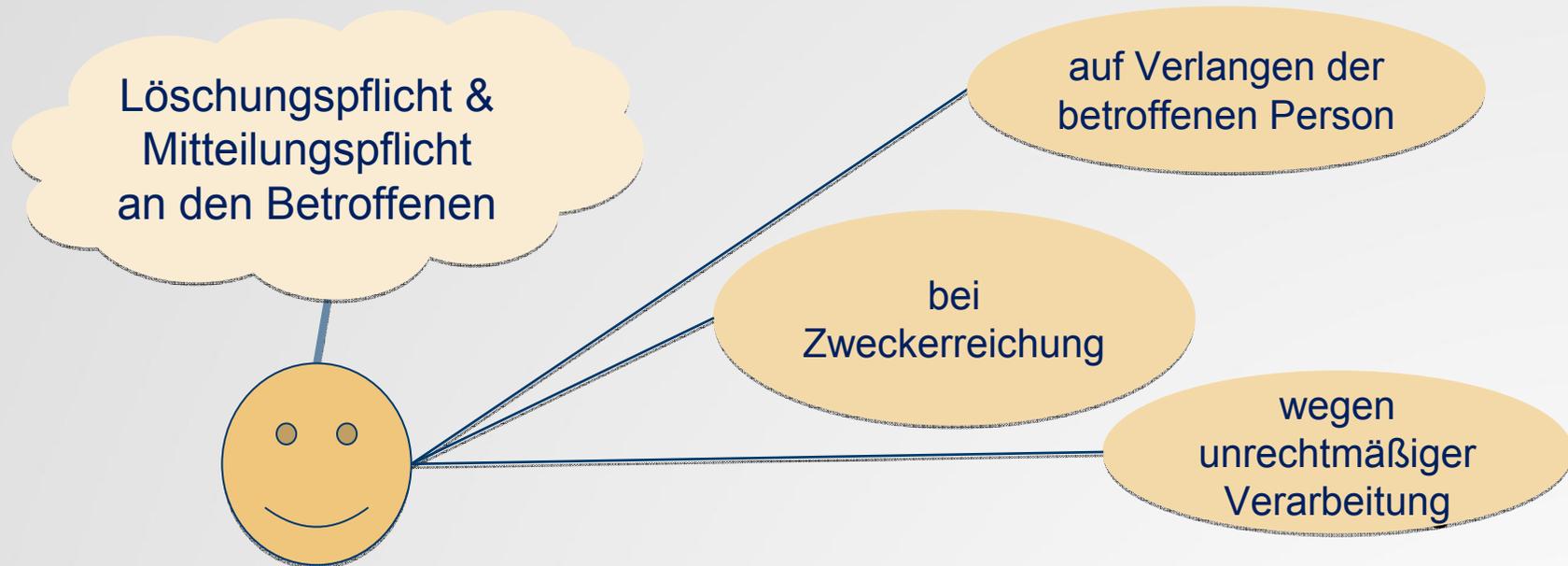
III. Rechte der Betroffenen



1. Auskunftsrechte



2. Recht auf Löschung / „Vergessenwerden“

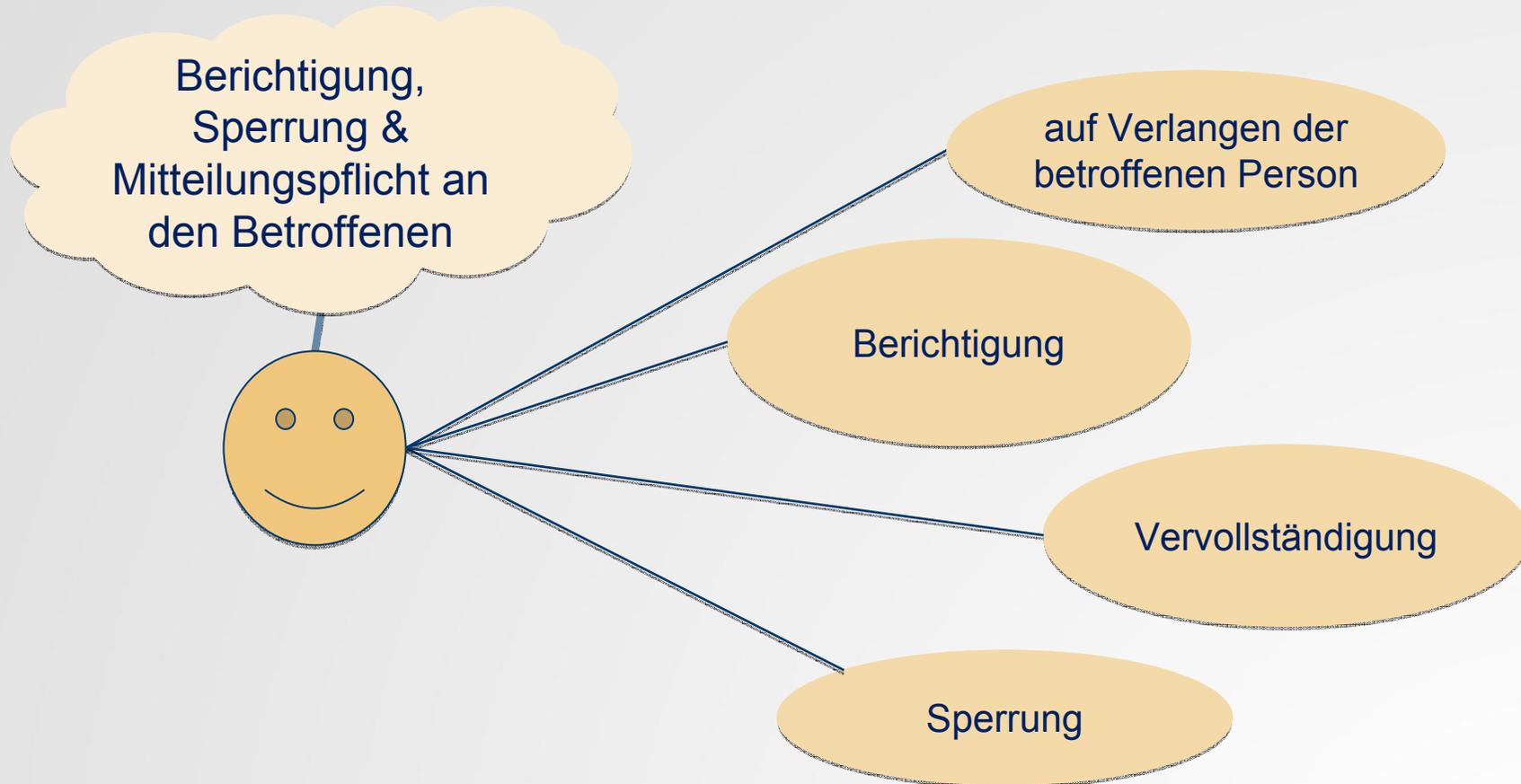


Beispielhafte Ausnahmen:

- Erfüllung einer rechtlichen Verpflichtung
- zur Wahrnehmung einer Aufgabe im öffentlichen Interesse
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen



3. Recht auf Berichtigung und Sperrung



VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Schneider + Partner GmbH
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft
Member of IGAL Intercontinental Grouping of
Accountants and Lawyers

Dresden
Lortzingstraße 37
01307 Dresden
Telefon 0351 34078-0
Fax 0351 34078-99
mail@sup-dresden.de

Chemnitz
Ludwigstraße 20
09113 Chemnitz
Telefon 0371 38195-0
Fax 0371 38195-50
mail@sup-chemnitz.de

München
Schackstraße 1
80539 München
Telefon 089 36049-00
Fax 089 360490-49
kontakt@sup-muenchen.de

www.schneider-wp.de