



Handbuch zur Umsetzung der Datenschutz-Grundverordnung

Branchenspezifika für Transport & Verkehr

Version 1.1, Sommer 2018

Dieses Handbuch mit Branchenspezifika wurde in Zusammenarbeit mit der Sparte “Transport & Verkehr” der Wirtschaftskammer Österreich erstellt.



Autor

Ing. Mag. Dr. Vincenz Leichtfried

Certified Data & IT-Security Expert

Certified Digital Consultant

Geprüfter Datenschutzexperte

VL@LV7.ms

*Fragen Sie nicht, was Sie für den Datenschutz tun können,
sondern was der Datenschutz für Sie tun kann.*

Datenschutz = IT-Sicherheit = Unternehmensstabilität

DISCLAIMER

Die Inhalte sollen einen einfachen und schnellen Überblick über die Datenschutz-Grundverordnung ermöglichen. Es wird kein Anspruch auf Vollständigkeit sowie korrekte Interpretation und Wiedergabe der aktuell vorliegenden Verordnung erhoben. Die Informationen ersetzen keine Beratung durch einen Unternehmensberater, Techniker oder Juristen. Diverse Auslegungen sowie finale Umsetzungen in nationale Gesetze sind noch nicht verfügbar. Es wird keine wie auch immer geartete Haftung übernommen.

Inhalte

Handlungsempfehlung zur Umsetzung der Datenschutz-Grundverordnung	9
Präambel	9
Ziele der Umsetzung	9
Funktional	9
Technisch-organisatorisch	9
Juristisch	10
10 Punkte-Programm zur Umsetzung	10
1. Sensibilisierung	11
Wer und was ist betroffen?	11
Protagonisten der Datenverarbeitung	11
Personenbezogene Daten	11
Anonyme Daten	12
Natürliche vs. juristische Personen	12
Digitale und analoge Daten	12
Arten von Daten - SENSIBLE DATEN	12
Private vs. institutionelle Verarbeitung von Daten	13
Auslöser	13
Typische Datenanwendungen	13
Strafraumen & 'Timeline'	14
Chancen erkennen	14
Grundregeln	15
Zweck	15
Minimal	15
Sicher	15
Risikobasiert	16
Plus: Personenbezogen vs. erlaubt vs. Aufklärung	16
Rechte der Betroffenen	16
Informationspflicht	16

Auskunftsrecht	17
Recht auf Berichtigung	17
Recht auf Löschung	17
Recht auf Einschränkung der Verarbeitung	17
Recht auf Datenübertragbarkeit	17
Widerspruchsrecht	17
Conclusio aus den Rechten der Betroffenen	18
Datenschutzvorfall	18
Weiterführende Informationen	18
Informationsservices der Wirtschaftskammer	18
Informationsveranstaltungen und Seminare	19
2. Projektmanagement	20
Wie umfangreich ist die Umsetzung?	20
Was sind die wichtigsten Protagonisten der Umsetzung?	20
Wer kann bei der Umsetzung unterstützen?	20
3. Analyse	21
Schritte für den Teilbereich der Analyse von Datenanwendungen	21
Hilfestellung: Identifikation von Datenanwendungen	22
Hilfestellung: Struktur von Datenanwendungen	22
Individuell pro Organisation	24
Verfahrensverzeichnis	24
Gesetzliche Verpflichtung	24
Inhalte eines Verfahrensverzeichnisses	24
Praktische Umsetzung	25
Muster für Verfahrensverzeichnisse	25
4. Auswirkungen evaluieren	25
Informationen zu Datenpartnern	26
...zur Erfüllung der Auflagen der DSGVO	26
...im Falle eines Wechsels	26
Notwendigkeit eines Datenschutzbeauftragten	26

Notwendigkeit einer Datenschutz-Folgenabschätzung	26
Erweiterte Informationen zur Einstufung	27
5. Juristisch	28
Zweck, Rechtsgrundlage und Aufbewahrungspflichten	28
Zwecke und Rechtsgrundlagen	28
Löschfristen bzw. Aufbewahrungspflichten	28
Einwilligungen	29
Informationspflichten / Datenschutzerklärung	29
Rechenschaftspflicht	29
Internationaler Datenverkehr	30
Datenpartner	30
6. Data & IT Security	31
Evaluierung des Risikos - CIA	31
Beispiele für technisch-organisatorische Maßnahmen	31
Datenmanagement: Fit für DSGVO - privacy by design / default	32
Datenschutz-Folgenabschätzung	32
7. Funktional	33
Prozesse und Datenschutz Policy	33
Umsetzung der Rechte der Betroffenen	33
Schulungen	34
8. Technisch	35
9. Vorbereitung Datenschutzvorfall	35
10. Dokumentation, laufende Adaptierung und Audits	35
Spezifika Fahrschulen	36
Ärztliches Gutachten (Gesundheitsbefund)	36
Erläuterung zur Notwendigkeit eines Datenschutzbeauftragten	36
Rechtsgrundlage	36
Spezifika Mitarbeiter	36
Arbeitnehmerdatenschutz im Allgemeinen	36
Verpflichtung zum Datengeheimnis	36

Privatnutzung	37
Datenschutzerklärung für Mitarbeiter	37
Checklisten	38
Checkliste: Ergebnisse aus 10 Punkte-Programm	38
Checkliste: Teil-Schritte der Analyse von Datenanwendungen	38
Checkliste: Erweiterte Informationen zur Einstufung von Datenanwendungen	39
Checkliste: Informationen zu einem Datenpartner	39
...für Start, Beendigung oder Wechsel	40
...plus allgemein	40
Checkliste: Umsetzung der Rechte der betroffenen Personen	40
Checkliste: Vorbereitung auf einen Datenschutzvorfall	41

Handlungsempfehlung zur Umsetzung der Datenschutz-Grundverordnung

Präambel

Das Ziel des vorliegenden Kompendiums ist eine praxisbezogene Zusammenfassung einer komplexen Thematik in möglichst verständlicher Form. Der Schwerpunkt wurde daher auf die Vorgehensweise gelegt, für theoretische Erläuterungen wird an den jeweiligen Stellen auf das umfassende Angebot von wko.at/datenschutz verlinkt.

Die Umsetzung der Datenschutz-Grundverordnung sollte immer unter dem Grundprinzip eines **risikobasierten Ansatzes** erfolgen. Ein 100%iger Schutz kann nie gewährleistet werden.¹ Ein besonderes Augenmerk sollte daher vor allem auf jene Datenanwendungen gerichtet werden, die ein besonderes Risiko für die Rechte und Freiheiten der Betroffenen darstellen.

Ziele der Umsetzung

Als oberste Ziele der Umsetzung sind die Vermeidung von Datenschutzvorfällen und die Rechtmäßigkeit der Verarbeitung (inkludiert auch die Speicherung von Daten) zu sehen. Die **tatsächliche Umsetzung ist sehr vielschichtig**. Ein paar Punkte sollen **besonders hervorgehoben** werden:

Funktional

- **Verfahrensverzeichnis** - Ist-Analyse und Protokollierung der Datenanwendungen einer Organisation zur Erfüllung der Dokumentationspflichten und als Ausgangslage für die weitere Umsetzung ('Verzeichnis der Verarbeitungstätigkeiten')
- **Rechte der Betroffenen** - Gewährleistung einer fristgerechten Umsetzung (siehe auch [Rechte der Betroffenen](#))

Technisch-organisatorisch

'Gelebter Datenschutz' - zur aktiven und passiven Sicherheit - Maßnahmen um einem Datenschutzvorfall entgegenzuwirken und um einen rechtmäßigen Umgang mit Informationen zu gewährleisten:

- **Technische Rahmenbedingungen** (z.B. Zugriffsbeschränkungen, Pseudonymisierung, datenschutzfreundliche Voreinstellungen...)
- **Praktischer Umgang** - vor allem um der 'Schwachstelle Mensch' entgegenzuwirken (z.B. durch Schulung, Betriebsunterweisung, Definition von Prozessen im Umgang mit Informationen...)

¹ Wieso? - 1. Technische Schwachstellen: Ständiger Wettlauf zwischen IT-Sicherheit und Hackern; 2. Menschliches Versagen: Fehler können passieren. Aber: Es muss immer nachweisbar dokumentiert sein, dass entsprechende 'technisch-organisatorische Maßnahmen nach aktuellem Stand der Technik, Aufwand und Risiko' getroffen wurden.

Juristisch

- **Rechtsgrundlage** - passend zum Zweck der Verarbeitung (Was ist erlaubt?)
- **Informationspflicht** - nicht zu verwechseln mit der Rechtsgrundlage (Datenschutzerklärung für Kunden, Mitarbeiter...)
- **Verträge mit Datenpartnern** - Festlegung der gegenseitigen Rechte und Pflichten (**insbesondere mit Auftragsverarbeitern**)

10 Punkte-Programm zur Umsetzung

Das Programm unterteilt sich in mehrere Phasen.

- *Start* -

1. Sensibilisierung (Wissensvermittlung, Teilnahme an Workshops)
2. Projektmanagement

- *Evaluierung* -

3. Analyse (IST-Stand, Verzeichnisse, kritische Unternehmensprozesse)
4. Auswirkungen evaluieren (GAP-Analyse für Konzeption und Ausführung, Notwendigkeit eines Datenschutzbeauftragten, einer -Folgenabschätzung...)

- *Konzeption* -

5. Juristisch (Verträge, Datenschutzerklärung, Rechtsgrundlagen, Löschfristen...)
6. Data & IT Security (Evaluierung technisch-organisatorischer Maßnahmen, Datenschutz-Folgenabschätzung...)

- *Ausführung* -

7. Funktional (Datenschutz Policy, Rechte der Betroffenen, Schulung...)
8. Technisch (Technisch-organisatorische Maßnahmen (TOM), privacy-by-, Datenmanagement optimieren...)
9. Vorbereitung Data Breach

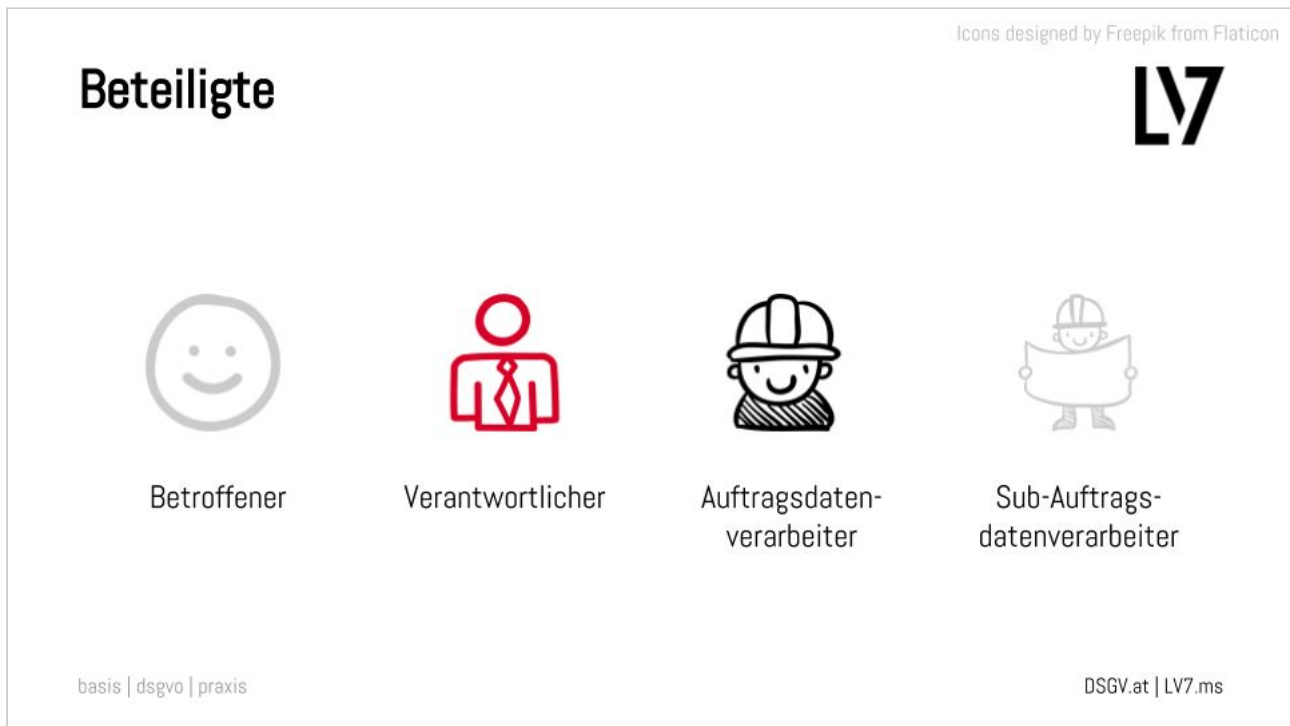
- *Dokumentation und Audits* -

10. Dokumentation, laufende Adaptierung und Audits

1. Sensibilisierung

Wer und was ist betroffen?

Protagonisten der Datenverarbeitung



Die Abbildung zeigt die Protagonisten einer Datenverarbeitung:

- **Betroffener** - Beteiligter, von dem personenbezogene Daten gespeichert werden (z.B. Kunde, Mitarbeiter, Ansprechpartner bei einem Geschäftspartner...)
- **Verantwortlicher** - Beteiligter, der personenbezogene Daten (über private Zwecke hinaus) speichert oder verarbeitet (z.B. Unternehmer, Verein, NGO...)
- **Auftragsverarbeiter** - Beteiligter, der ein Service oder eine Dienstleistung für den Verantwortlichen anbietet, bei dem er in Kontakt mit personenbezogenen Daten des Betroffenen kommt (z.B. Buchhalter, Druckerei für Adresstiketten, IT-Dienstleister...)
- **Sub-Auftragsverarbeiter** - Beteiligter, der ein Service oder eine Dienstleistung für den Auftragsverarbeiter anbietet, bei dem er in Kontakt mit personenbezogenen Daten des Betroffenen kommt (z.B. externer Dienstleister, Serveranbieter...)

Die EU-Datenschutz-Grundverordnung findet Anwendung, sobald einer der Beteiligten in der Europäischen Union ansässig ist.

Personenbezogene Daten

Die EU Datenschutz-Grundverordnung regelt die Verarbeitung von personenbezogenen Daten. Darunter versteht man jede Information, die **von Ihnen** (als Verantwortlicher) **oder einem Dritten** 'unter angemessenem Aufwand' einer Person zugeordnet werden kann. Leicht verständlich ist dies, sobald ein Name neben dem Datensatz steht. Anstelle eines Namens reicht aber beispielsweise auch eine ID oder Nummer, mit denen Sie oder jemand anderer (z.B. Geschäftspartner, Auftraggeber, Dienstleister, etc.) den Personenbezug herstellen kann.

Anonyme Daten

Anonyme Daten fallen **nicht in den Anwendungsbereich** der EU Datenschutz-Grundverordnung. Das sind beispielsweise Statistiken mit ausreichender Stichprobenanzahl, die **absolut keine Rückschlüsse auf einzelne Personen** erlauben. Eine rückführbare Verschlüsselung stellt keine Anonymisierung dar.

Natürliche vs. juristische Personen

Die EU Datenschutz-Grundverordnung bezieht sich auf **natürliche Personen** (also auf Menschen).² Dabei ist es wichtig, folgendes zu verstehen:

- **Auch im reinen Business-to-Business**-Bereich werden im Normalfall Daten von Ansprechpartnern, Mitarbeitern usw. verarbeitet (also von natürlichen Personen)
- **Auch ein Firmenname kann** den Namen einer natürlichen Person enthalten (oder entsprechende Rückschlüsse zulassen)

...daher gilt auch in diesen Bereichen die DSGVO.

Digitale und analoge Daten

In den Anwendungsbereich fallen:

- die 'automatisierte Verarbeitung' von Daten. Darunter ist **alles** zu verstehen, **was in irgendeiner Form digital verarbeitet oder** auch nur **gespeichert** wird
- **analoge Daten, die strukturiert aufbewahrt** werden (z.B. Papierakten)

In der Praxis bedeutet dies: jede Textdatei, Datentabelle, E-Mail ebenso wie jeder Aktenordner.

Arten von Daten - SENSIBLE DATEN

Der Begriff sensible Daten kommt aus dem DSG2000. In der EU-DSGVO spricht man von **besonderen Datenkategorien**. Ähnliche Auswirkungen haben auch **strafrechtlich relevante Daten**. **Im Folgenden** wird der Einfachheit halber **der Terminus "sensible Daten"** verwendet. Bitte aber **nicht verwechseln**:

- **sensible Daten im Sinne des Datenschutzes mit**

² Im österreichischen Anpassungsgesetz aus Mitte 2017 nimmt man jedoch auch auf juristische Personen Bezug. Hierzu gibt es verschiedenste Erläuterungen, wie dies zu deuten ist und ebenso zahlreiche Spekulationen ob dieser Passus von der neuen Regierung noch zeitnah modifiziert wird.

- **kritischen** Daten(anwendungen) im Sinne der Unternehmensstabilität (z.B. Produktion)
- **vertraulichen** Daten(anwendungen) (z.B. Geschäftsgeheimnisse)
- **ständig verfügbaren** Daten(anwendungen) (z.B. Kassensystem)

Unter besondere Datenkategorien fallen:

- Gesundheitsdaten (auch Sozialversicherungsnummer)
- Genetische und biometrische Informationen (z.B. Fingerabdruck)
- Sexualleben und sexuelle Orientierung
- Politische, religiöse, weltanschauliche Daten (auch Gewerkschaftszugehörigkeit)
- Rassistische und ethnische Herkunft

Private vs. institutionelle Verarbeitung von Daten

Die rein private Verarbeitung von Daten (z.B. Urlaubsfotos, Kontaktdaten von Freunden oder Bekannten) fällt nicht unter die DSGVO. Abseits dessen jedoch alles Andere - egal, ob die Verarbeitung von einer Einzelperson oder Institution durchgeführt wird. Ebenso ist es unerheblich, ob die Datenverarbeitung mit oder ohne Gewinnabsicht durchgeführt wird (gilt also auch für NGOs, Vereine...).

Die Verarbeitung der personenbezogenen Daten von Verstorbenen fällt ebenso nicht in den Anwendungsbereich - jedoch die Daten der Hinterbliebenen.

Auslöser

Es sollte nicht mit den ressourcen-technischen Möglichkeiten der Datenschutzbehörde spekuliert werden. Unabhängig von einer aktiven Prüfung kann es andere Auslöser geben, bei denen die Behörde aktiv wird:

- **Rechte der Betroffenen** (Fehler im Umgang)
- Verbandsklagen
- **Datenschutzvorfall** (egal ob Hackerangriff, menschliches Versagen oder andere Auslöser...)
- **Wettbewerb** (Beschwerde durch Wettbewerbsverzerrung bei Nichteinhaltung)

Typische Datenanwendungen

Bei genauer Betrachtung gibt es kaum eine Datenanwendung ohne personenbezogene Daten. Ausnahmen können jedoch je nach Gegebenheit Informationen wie Produktdatenbanken sein.

DATENANWENDUNGEN

Kunden Lieferanten Personal (Bewerbungen - Urlaube - Krankenstände)
E-Mails Termine Videoüberwachung Telefonanlagen
Zulieferer Partnerfirmen Fuhrparkmanagement Log-Dateien
Website-Analytics Zeiterfassung Buchhaltung Vertrieb
Auftragsabwicklung Rechnungen

Die Abbildung zeigt Beispiele von Datenanwendungen mit personenbezogenen Daten.

Strafraahmen & 'Timeline'

Der Strafraahmen von bis zu 20 Mio oder 4 % des weltweiten Konzernumsatzes (je nachdem was höher wiegt) soll alle Institutionen dazu bewegen, Datenschutz ernst zu nehmen.³

Wichtig: Vorbereitung und die dazugehörige Dokumentation sind entscheidend!

Plus: Zusätzlich zur Verwaltungsstrafe können Schadenersatzforderungen der Betroffenen schlagend werden.

Die EU-DSGVO wurde bereits 2016 beschlossen. Die Übergangsfrist (= 'Schonfrist') endet am 25. 5. 2018. Auch wenn bisweilen das Bewusstsein zur Thematik in vielen Institutionen nicht vorhanden war - viele Auflagen waren bereits durch das vorangegangene Datenschutzgesetz gegeben.

Chancen erkennen

Die Umsetzung der EU-Datenschutz-Grundverordnung sollte nicht nur als Bürde betrachtet werden. Ganz im Gegenteil sollte sie eher als Auslöser gesehen werden, um dem Umgang mit Informationen die nötige Aufmerksamkeit und Bedeutung beizumessen. "Fragen Sie nicht, was Sie für den Datenschutz tun können, sondern was der Datenschutz für Sie tun kann." Daten werden oft als 'das neue Öl' bezeichnet. Dementsprechend gilt auch die Gleichung 'Datenschutz = IT-Sicherheit = Unternehmensstabilität'. Überlegen Sie sich, was passieren würde, wenn:

- 5 Tage lang Ihre Dienstleistung / Ihre Produktion / Ihr Service ausfallen würde
- Ihre Kundendaten verändert wären

³ EU-Datenschutz-Grundverordnung (DSGVO): Rechtsdurchsetzung und Strafen
wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung-Rechtsdurchsetzung..

- Ihre Geschäftsgeheimnisse oder Finanzsituation öffentlich zugänglich wären

Datenschutz soll nicht nur der ungewollten Offenlegung von Informationen entgegenwirken, sondern auch die Integrität von Daten und die Stabilität von Datenanwendungen sicherstellen. Tatsächlich gelebter Datenschutz hilft daher auf mehreren Ebenen:

- Wettbewerbsfaktor
- Unternehmensprozesse (Evaluierung)
- Data & IT Management (Evaluierung)
- Cybercrime (Evaluierung)
- ...

Grundregeln

Um die Umsetzung der Datenschutz-Grundverordnung sinnvoll angehen zu können, ist das Bewusstsein einiger Grundregeln essentiell⁴.

Zweck

Die **Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten** (= 'Verbotsgesetz'). Für jeden Zweck der Datenverarbeitung **bedarf** es daher auch **einer entsprechenden Rechtsgrundlage**, darunter fallen:

- Gesetzliche Verpflichtung (z.B. Buchhaltungspflicht)
- Vertrag / vorvertraglich (z.B. Angebotserstellung)
- Einwilligung (z.B. Newsletterversand - Achtung: entsprechend dokumentieren!)
- Berechtigtes Interesse (sofern nicht Schutz überwiegt [spez. Kinder])
- Lebenswichtig
- Öffentlich / behördlich

Details siehe 'Grundsätze und Rechtmäßigkeit der Verarbeitung'⁵ und [Rechtsgrundlage](#).

Minimal

Das Prinzip des Datenminimalismus gilt auf zweierlei Arten. Es dürfen:

- **nur** die **Daten verarbeitet** werden, **die zur Zweckerfüllung benötigt** werden
- die Daten **nur solange** verarbeitet / gespeichert werden, **wie** diese zur Zweckerfüllung **benötigt** werden

Es gilt daher zu unterscheiden, welche Daten für welchen Zweck benötigt werden.

Sicher

⁴ Bei den beschriebenen Grundregeln handelt es sich um eine zusammenfassende Darstellung des Autors. Diese sollte nicht mit den Grundsätzen für die Verarbeitung personenbezogener Daten lt. Art. 5 der DSGVO verwechselt werden.

⁵ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsätze-und-Rechtsmaes.html

Der Verantwortliche ist dafür zuständig, dass die Daten bei **im eigenen Unternehmen und auch bei Auftragsverarbeitern** sicher verarbeitet werden.

Risikobasiert

Wie in der Präambel erwähnt. Die Umsetzung der Datenschutz-Grundverordnung sollte immer unter dem Grundprinzip eines **risikobasierten Ansatzes** erfolgen. Ein 100%iger Schutz von Daten kann nie gewährleistet werden. Ein besonderes Augenmerk sollte daher vor allem auf jene Datenanwendungen gerichtet werden, die ein **besonderes Risiko für die Rechte und Freiheiten der Betroffenen** darstellen. **Parallel** sollte ein **Augenmerk auf die Unternehmensstabilität** gelegt werden. Dabei gilt es abzuwägen, welche Abläufe für das Unternehmen besonders wichtig sind.

Plus: Personenbezogen vs. erlaubt vs. Aufklärung

Erfahrungsgemäß tendieren Unternehmer bei der Evaluierung von Datenanwendungen dazu, verschiedene Themenbereiche zu vermischen. Daher sollte klar sein:

- eine Datenanwendung fällt immer in den Anwendungsbereich der Datenschutz-Grundverordnung, **sobald ein Bezug zu einer Person herstellbar** ist (auch über eine ID, Notiz, etc...)
- eine Datenanwendung ist **erlaubt, sofern eine Rechtsgrundlage gegeben** ist
- über die Datenanwendung **muss entsprechend informiert** werden

Abseits dessen gibt es noch andere Grundsätze (wie Richtigkeit, Integrität, Vertraulichkeit, Verarbeitung nach Treu und Glauben, etc...), die bei entsprechender Abstraktion und Umsetzung der Thematik als logische Schlussfolgerung angesehen werden können.

Rechte der Betroffenen

Der richtige Umgang mit den Rechten der Betroffenen ist entscheidender Faktor im alltäglichen Umgang eines Unternehmers mit Daten. Klassisch fällt darunter alles, was mit Kunden, Mitarbeitern oder Lieferanten bzw. deren Ansprechpartnern zu tun hat. Jede Institution muss sich daher **überlegen, welche Protagonisten dies** im jeweiligen Umfeld **sein können** und sich entsprechend darauf ausrichten. Einen Großteil dieser Rechte hatte der Betroffene in Österreich auch bisher schon.

Informationspflicht

Der Verantwortliche muss den Betroffenen darüber informieren:

- **Wer** der Verantwortliche ist
- **Was** der Betroffene für Rechte hat (Aufklärung über seine Rechte)
- **Welche** Daten über ihn verarbeitet werden
- **Wann** bzw. wie lange die Daten verarbeitet werden
- **Wo** die Daten verarbeitet werden (falls diese ins EU-Ausland transferiert werden)
- **Wie** die Daten verarbeitet werden, im Falle von Profiling bzw. falls spezielle Algorithmen zur Entscheidungsfindung eingesetzt werden

- **Wieso** die Daten verarbeitet werden - also zu welchem Zweck

Im Detail ergeben sich Variationen je nachdem, ob die Daten beim Betroffenen selbst erhoben werden oder nicht - ebenso daraus, wie die Daten verarbeitet werden. Im Allgemeinen müssen aber all diese Informationen bekannt sein, was vor allem auch bedeutet, dass der Verantwortliche sich mit diesen Fragestellungen auseinandersetzen muss. Die praktische Umsetzung der Informationspflichten findet sich in der Datenschutzerklärung.

Auskunftsrecht

Vereinfacht ausgedrückt: 'Auskunftsrecht = Informationspflicht + Kopie der Daten'

Der Betroffene hat das Recht zu erfahren, welche Daten über ihn verarbeitet werden (bzw. gespeichert sind).

Recht auf Berichtigung

Falsche Daten können zu falschen Ergebnissen führen, daher das Recht auf Berichtigung.

Recht auf Löschung

Das Recht auf Löschung besteht immer dann, wenn keine andere Rechtsgrundlage mehr gegeben ist (z.B. gesetzliche Verpflichtung oder zur Vertragserfüllung). Natürlich kann es zu einem Betroffenen auch Datenanwendungen mit unterschiedlichen Rechtsgrundlagen geben. Ein gutes Beispiel hierfür ist die Differenzierung zwischen Daten zur Buchhaltung und reinen Nutzungsdaten. Für Ersteres gilt die gesetzliche Aufbewahrungspflicht. Zweiteres wäre zu löschen.

Recht auf Einschränkung der Verarbeitung

In manchen Szenarien kann es sein, dass Daten nicht einfach gelöscht, sondern deren Verarbeitung einfach nur ausgesetzt werden muss (z.B. für die Dauer einer Überprüfung, bei Rechtsanspruch, wenn nur eine Einschränkung verlangt wird...).

Recht auf Datenübertragbarkeit

Bei Wechsel eines Anbieters hat der Betroffene das Recht, dass seine Daten vom alten Anbieter 'direkt in automatisierter / maschinenlesbarer Form' an den neuen Anbieter übertragen werden. Dies gilt vor allem für die Daten, die der Betroffene selbst beigesteuert hat. Beispielsweise wäre das sein Einkaufsverhalten (also alle gespeicherten gekauften Produkte), aber nicht das vom Verantwortlichen berechnete Profil (z.B. Junggeselle, Mutter...).

Widerspruchsrecht

Das Widerspruchsrecht gilt unter anderem im Falle von 'besonderen Situationen' sowie bei 'Direktmarketing'.

Conclusio aus den Rechten der Betroffenen

Die Rechte der Betroffenen schaffen auch entsprechende Anforderungen an das Datenmanagement und deren Anwendungen. Gleiches gilt für alle Arten von Datenpartnern. Es muss die Möglichkeit geben, **informieren** / **beauskunften** / **korrigieren** / **löschen** / **deaktivieren** / **exportieren** zu können.

Siehe auch Betroffenenrechte⁶ und [Umsetzung der Rechte der betroffenen Personen](#)

Datenschutzvorfall

Unter einem Datenschutzvorfall versteht man **jedes Vorkommnis bei dem Informationen ‘ungewollt’ offengelegt, verändert oder verloren gehen**. Darunter fallen beispielsweise: der Verlust oder Diebstahl von Geräten, Bildschirmansicht oder auch Fehler im Versand von E-Mails.

Einer der häufigsten Auslöser ist menschliches Versagen. Im Umkehrschluss bedeutet dies, dass durch entsprechende Schulungsmaßnahmen sowie technisch-organisatorische Maßnahmen, die Eintrittswahrscheinlichkeit minimiert und deren negative Folgen beschränkt werden können. Siehe dazu auch [Beispiele für technisch-organisatorische Maßnahmen](#).

Andere Ursachen können jedoch auch Computerviren (bzw. Krypto-Trojaner) oder bewußtes ‘Social Engineering’ durch Hacker sein. Bei letzterem werden den Opfern durch geschickte Fragestellungen Informationen entlockt. Hinter einem Hackerangriff stecken also nicht immer nur ‘Computer-Nerds’. Telefonanrufe oder klug formulierte Mails bedürfen keiner IT-Kenntnisse.

Alle Datenschutzvorfälle müssen protokolliert und im Falle eines Risikos auch gemeldet werden. Siehe dazu Vorbereitung auf Datenschutzvorfälle. Siehe [9. Vorbereitung Datenschutzvorfall](#).

Weiterführende Informationen

Informationsservices der Wirtschaftskammer

Ausführliche Detailinformationen zu den aufgeführten Punkten bietet die Wirtschaftskammer unter wko.at/datenschutz⁷

Einen guten Einstieg bieten hier auch Checkliste⁸ und Begriffsbestimmungen⁹.

⁶ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Betroffenenrechte.html

⁷ wko.at/datenschutz

⁸ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html

⁹ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Wichtige-Begriffsbestimmu.html

Informationsveranstaltungen und Seminare

Interessensvertretungen wie die Wirtschaftskammer bieten zahlreiche Informationsveranstaltungen rund um die EU Datenschutz-Grundverordnung an. Einen bequemen Einstieg in diese komplexe Thematik bieten Abendveranstaltungen und andere Kurzvorträge. Für die tiefergehende Wissensvermittlung ist die Teilnahme an Tagesveranstaltungen zu empfehlen.

2. Projektmanagement

Wie umfangreich ist die Umsetzung?

Dauer und Umfang des Projektes stehen immer in Abhängigkeit mehrerer Faktoren (Branche, aktuelle Struktur und Sicherheit der Datenanwendungen, Kenntnisse rund um die Informationsverarbeitung der Projektbeteiligten, bisheriger Umgang mit Rechtsgrundlagen und Verträgen in der Organisation...). Auch wenn wie eingangs erwähnt ein 100%iger Schutz nie möglich sein wird, macht es einen Unterschied, ob bei 20 oder 93% gestartet wird. Pauschale Aussagen über den Umfang sind daher vorab schwer zu treffen.

Was sind die wichtigsten Protagonisten der Umsetzung?

In die Umsetzung müssen immer mehrere Beteiligte einbezogen werden.

- Unternehmensleitung (Endverantwortung - muss Zeit & Budget freigeben)
- Abteilungsverantwortliche (Wissen über jeweilige Datenanwendungen, Zwecke...)
- Personalabteilung (viele personenbezogene Daten, Schulungen...)
- IT-Abteilung (Wissen über IT-Infrastruktur, technische Sicherheitsmaßnahmen...)
- Datenpartner des Unternehmens (Auftragsverarbeiter / Dienstleister, Geschäftspartner...)

Wer kann bei der Umsetzung unterstützen?

Die Umsetzung erfolgt in mehreren Disziplinen:

- **Funktional** (Verständnis über Abläufe im Unternehmen, Funktion und Zweck von Datenanwendungen, Implementierung organisatorischer Sicherheitsmaßnahmen, Schulungen...)
- **Juristisch** (Klärung der Rechtsgrundlage, Anpassung von Verträgen, Datenschutzerklärungen...)
- **Technisch** (Evaluierung der IT-Infrastruktur, Implementierung technischer Sicherheitsmaßnahmen...)

Im Gesamtprojekt sind alle Bereiche abzudecken. Mit Datenschutz ist es ähnlich wie beispielsweise beim Finanzwesen (Buchhaltung / Rechnungswesen / Lohnverrechnung...). Man kann es entweder selbst machen, oder sich von externen Dienstleistern unterstützen lassen. Die Intensität der Begleitung erfolgt in gemeinsamer Absprache. Idealerweise führt ein Datenschutzexperte (z.B. speziell ausgerichteter Unternehmensberater) durch das Projekt. Zusätzlich sollten je nach Bedarf Dritte mit einbezogen werden (z.B. bestehende oder externe IT-Dienstleister und Juristen). Geprüfte Datenschutzexperten sowie Certified Data & IT-Security Experts können unter anderem über die Qualitätsakademie der WKO gefunden werden (www.incite.at)

3. Analyse

Schritte für den Teilbereich der Analyse von Datenanwendungen

Die in den Checklisten aufgeführten Punkte¹⁰ dienen dem **allgemeinen Grundwissen, das über die eigenen bzw. in Auftrag gegebene Datenverarbeitungen vorhanden sein sollte** - unabhängig davon, ob Sie dieses **Wissen für** die Erstellung des **Verfahrensverzeichnisses**, die Umsetzung der **Rechte der Betroffenen**, **Vertragserstellung mit Datenpartnern** oder die **Aufrechterhaltung kritischer Unternehmensanwendungen** benötigen.

*Anmerkung: Beispielsweise mag es für das Verfahrensverzeichnis nicht unbedingt notwendig sein, den genauen Speicherort anzugeben, allerdings können zugriffsberechtigte Personen (Empfängerkategorien) sowie technisch-organisatorische Sicherheitsmaßnahmen oder die Auswirkungen bei einem Datenschutzvorfall (z.B. Verlust eines Notebooks) nur dann evaluiert werden, wenn diese Informationen bekannt sind. Abseits der rechtlichen Thematik ist dieses **Wissen unerlässlich für tatsächlich gelebte Datensicherheit** - egal, ob im Sinne des **Datenschutzes**, der Wahrung von **Geschäftsgeheimnissen** oder zur **Stabilität des Unternehmens**).*

Die Thematik der Datenschutz-Grundverordnung ist komplex und deren Gesamtforderung vielschichtig. Die angeführten Punkte¹¹ mögen **umfangreich** sein, sollen aber dafür **Schritt-für-Schritt** durch die Umsetzung führen.

*Anmerkung: Im Folgenden wird nicht zwischen Auftragsverarbeiter oder parallelen Verantwortlichen unterschieden und daher der **Terminus Datenpartner** verwendet.*

Was ist in der Analyse unter einer Datenanwendung zu verstehen?

Um die Auswirkungen einer Datenanwendung separiert analysieren zu können, wird in der hier beschriebenen Methodik unter einer **Anwendung ein Kompendium an Zwecken, Protagonisten, Datenkategorien und technisch-organisatorischen Maßnahmen** verstanden.

Dies können beispielsweise sein:

- Papierformular (Anmeldeformular, Feedbackbogen...)
- Excel-Sheet (Ein-Ausgaben-Rechnung, Rechnungsliste...)
- Software-Teil (Terminverwaltung, Adressbuch, E-Mail Dienst...)

Unter diesem Verständnis enthalten E-Mail Programme zumeist verschiedene 'Sub-'Anwendungen (z.B. E-Mail Anwendung, Kontaktverwaltung, Kalenderanwendung), wobei jede 'Sub-'Anwendung andere Zwecke erfüllt und andere Datenkategorien beinhaltet. Das 'Verfahren' einer Website kann oftmals die 'Anwendungen' Analytics, Kontaktformular und Newsletter-Anmeldung beinhalten.

Natürlich **kann** es **Sinn machen, einzelne Anwendungen** im Verzeichnis der Verarbeitungstätigkeiten **als ein gemeinsames Verfahren auszuweisen** (z.B. als Buchhaltung).

¹⁰ siehe im Anhang unter [Checklisten](#)

¹¹ siehe unten, sowie im Anhang unter [Teil-Schritte der Analyse von Datenanwendungen](#)

Hilfestellung: Identifikation von Datenanwendungen

Die Herangehensweise aus verschiedenen Blickwinkeln fördert die Vollständigkeit der Auflistung.

I. Via Geräte

- Welche Geräte(kategorien) gibt es im Unternehmen(z.B. Notebook Kategorie Außendienstmitarbeiter, NAS-Server)?
- Welche Software ist auf diesen Geräten installiert?

II. Via Ablage

- Welche Speicherorte gibt es in meinem Unternehmen?
- Fragestellungen:
 - Wo werden Informationen abgelegt?
 - Wie erfolgen Backups?
 - Wie werden Daten übermittelt?

III. Via Prozess

- Welche Tätigkeiten (Prozesse) gibt es in meinem Unternehmen?
Allgemeine Kommunikation und Korrespondenz, Buchhaltung, Newsletter...
- Nach Situation
Tagesablauf, wöchentliche oder monatliche Routinen
- Bestehende Dokumentationen
DVR-Nummern, empfohlene Abläufe und Protokolle

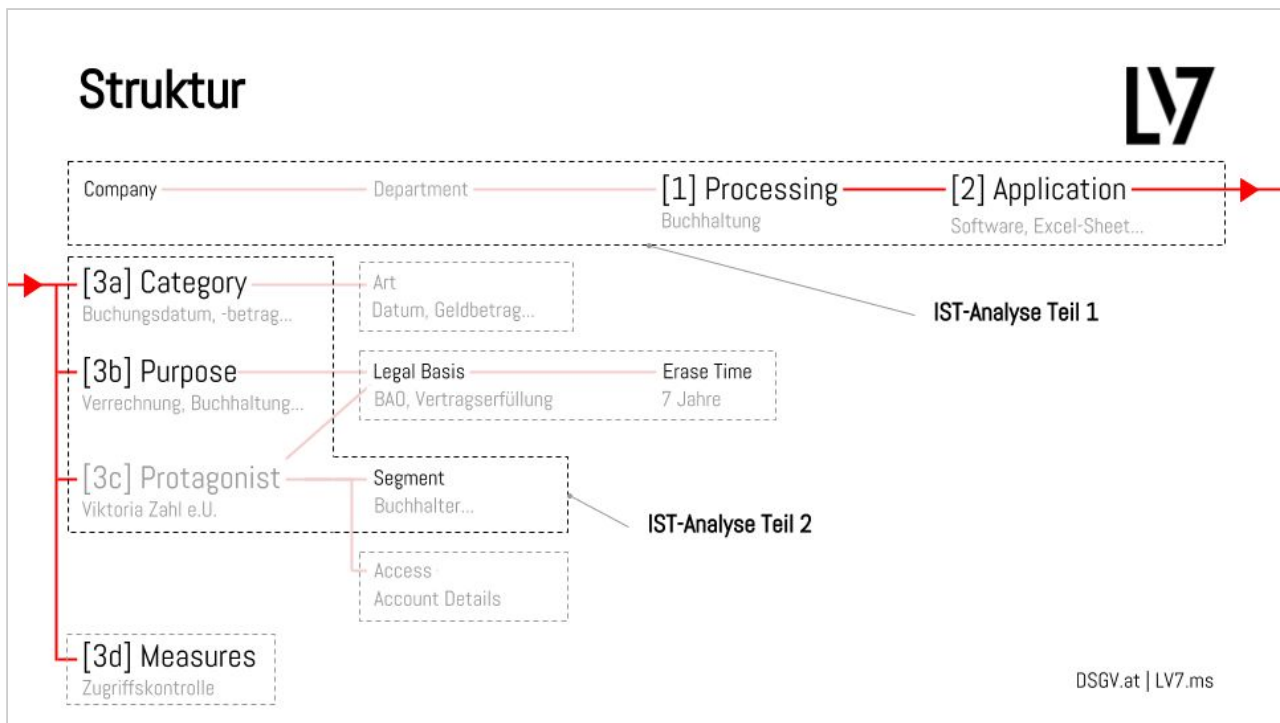
Ergebnis:

- **Verfahren und deren Datenanwendungen** (grobe Auflistung)
- Abteilungen
- Ansprechpartner / Verantwortlichkeiten
- Datenpartner (Auftragsverarbeiter / Dienstleister, Geschäftspartner...)

Hilfestellung: Struktur von Datenanwendungen

Im Allgemeinen gibt es keine Formvorschrift, wie ein Verzeichnis der Verarbeitungstätigkeiten auszusehen hat. Die dargestellte Struktur hat folgende Vorteile:

- klares Abbild des IST-Stands
- Trennung unterschiedlicher Disziplinen (funktional, juristisch, technisch)
- leichte Wartbarkeit, da ein Überblick über veraltete, veränderte und neu hinzugekommene Anwendungen gegeben ist
- Darstellung von Abhängigkeiten (z.B. jeder Zweck benötigt eine Rechtsgrundlage)



Die Abbildung zeigt die Struktur der Vorgehensweise. Nach Teil 1 erfolgt eine Priorisierung der Verfahren mit Fokus auf Risikorelevanz im Sinne von Datenschutz und Unternehmensstabilität. In Teil 2 erfolgt eine tiefere Analyse inklusive Metadaten auf Basis von Reihung und Zeitkontingenz.

- **Abteilung** (= sinnvolle Segmentierung - unabhängig der realen Struktur)
 - Kerntätigkeit A (z.B. Personalvermittlung, Immobilienmakler...)
 - Kerntätigkeit B (z.B. Arztpraxis, Entwicklungsabteilung...)
 - Backoffice (mit Verfahren: Rechnungswesen, Mitarbeiter, Marketing...)
 - IT-Inventory (mit Verfahren: Website, Rechner Gsf, Rechner Mitarbeiter..)
- **Verfahren** (= sinnvolle Gruppierung von Applikationen)
 - Buchhaltung (mit Anwendung: Software, Excel-Sheet...)
 - Website (mit Anwendung: Kontaktformular, Analytics, Newsletteranmeldung...)
- **Anwendung** (= Kompendium an Zwecken, Protagonisten, Datenkategorien...)

z.B. jedes...

 - Papierformular (Anmeldeformular, Feedbackbogen...)
 - Excel-Sheet (Ein-Ausgaben-Rechnung, Rechnungsliste...)
 - Software-Teil (Terminverwaltung, Adressbuch, E-Mail Dienst...)
- **Protagonist**
 - Betroffener
 - Empfänger
 - Ablage- / Speicherort
 - Quelle
- **Maßnahme** (= Maßnahmenpaket)
 - Risiko
 - Abhilfemaßnahme (Technisch-organisatorische Einzelmaßnahme)

Individuell pro Organisation

Natürlich gibt es Verfahren, die in vielen Organisationen ähnlich sind. Trotzdem gibt es individuell große Unterschiede (z.B. tatsächlich verarbeitete Datenkategorien, technisch-organisatorische Maßnahmen, zugriffsberechtigte Personen...).

Verfahrensverzeichnis

Das sogenannte **‘Verfahrensverzeichnis’** oder **‘Verzeichnis der Verarbeitungstätigkeiten’** ist so etwas wie ‘die Buchhaltung der Datenanwendungen’ einer Institution. Es muss ebenso immer aktuell gehalten werden. Um Missverständnissen vorzubeugen: Es müssen nicht alle Datensätze, sondern lediglich die Datenanwendungen selbst angeführt werden.

Gesetzliche Verpflichtung

Die gesetzliche Verpflichtung zur Führung eines Verfahrensverzeichnisses mag für den Laien in der Verordnung etwas undurchsichtig formuliert sein.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Im Ergebnis ist beinahe jede Institution verpflichtet, dieses Verzeichnis zu führen. Unabhängig, ob es sich um ein Ein-Personen-Unternehmen, einen Industriebetrieb, eine Non-Profit-Organisation oder einen Verein handelt.

Inhalte eines Verfahrensverzeichnisses

Zur Führung des Verfahrensverzeichnisses gibt es keine besonderen Formvorschriften. Es ist jedoch schriftlich zu führen (z.B. elektronisch) und muss folgende Informationen beinhalten:

- **Namen** und **Kontaktdaten** von Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- **Zwecke** der Verarbeitung
- **Kategorien** personenbezogener **Daten**
- Kategorien **betroffener Personen**
- Kategorien von **Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
- vorgesehene **Fristen** für die **Löschung**
- Beschreibung der **technischen und organisatorischen Datensicherheitsmaßnahmen** (nach Möglichkeit)

Praktische Umsetzung

Dies sind die Minimalanforderungen an die Inhalte. Wie bereits erwähnt, macht es jedoch Sinn, weitere Inhalte zu erheben, um auch den anderen Anforderungen gerecht werden zu können (z.B. Rechtsgrundlage, Speicherort...). Siehe auch 'Dokumentationspflicht - Verzeichnis von Verarbeitungstätigkeiten'¹².

Im Falle einer Unterstützung durch einen Berater sollten gemeinsam ein paar exemplarische Beispiele erarbeitet werden. Je nach Abmachung kann ein Dienstleister zwar weiterführend unterstützen, im Endeffekt müssen die Informationen jedoch von der jeweiligen Organisation selbst kommen.

Muster für Verfahrensverzeichnisse

Siehe parallel publizierte Branchenmuster.

Anmerkung: Der Detailgrad in den Branchenmustern wurde bewusst gewählt, um aufzuzeigen, wie die Einträge zustande gekommen sind.

Achtung: Bei der **Nutzung von Mustern** gilt ebenso wie bei **Vorlagen von Softwareanbietern**, dass deren Einsatz **je nach Unternehmen individuell** analysiert werden muss. Im Normalfall sind zusätzlich zu allgemeinen Branchenlösungen immer noch **unternehmensspezifische Anwendungen** in Verwendung. Speziell gilt dies bei analoger Datenverarbeitung, da diese von keinem Branchenmuster eins-zu-eins abgedeckt werden kann.

In Hinblick auf die **Minderung der wahrscheinlichsten Auslöser 'Umsetzung der Rechte der Betroffenen'** oder bei **'Datenschutzvorfall'**, die in Verbindung mit einem Fehlverhalten und damit verbunden Strafen stehen, **helfen Muster nur** dann, **wenn** deren **Umsetzung** des Datenschutzes auch **tatsächlich gelebt wird**.

4. Auswirkungen evaluieren

Auf Basis der Metadaten im Verfahrensverzeichnis können die Auswirkungen auf weitere Anforderungen in der Umsetzung der Datenschutz-Grundverordnung evaluiert werden.

4. Auswirkungen evaluieren (GAP-Analyse für Konzeption und Ausführung, Notwendigkeit eines Datenschutzbeauftragten, einer -Folgenabschätzung...)
 - Rechtlich (Verträge mit Datenpartnern vorhanden, Datenschutzerklärungen vorhanden, Rechtsgrundlagen bekannt, Aufbewahrungspflichten bekannt...)
 - Technisch-organisatorische Maßnahmen (vorhanden, dokumentiert...)
 - Informationen zu Datenpartnern (bekannt / unbekannt)
 - Notwendigkeit eines Datenschutzbeauftragten (ja / nein und Begründung)
 - Notwendigkeit einer Datenschutz-Folgenabschätzung (ja / nein und Begründung)

¹² wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html

Informationen zu Datenpartnern

...zur Erfüllung der Auflagen der DSGVO

Um Informationspflichten und anderen Auflagen rund um die DSGVO nachkommen zu können, werden von Datenpartnern letztendlich **ähnliche Informationen benötigt wie bei den eigenen Datenanwendungen** (siehe **Teil-Schritte der Analyse von Datenanwendungen ab 3.5**) - allerdings in anderem Detailgrad. Was genau, ist je nach Konstellation der Beziehung und Art der Anwendungen individuell abzuwägen. Es kann sinnvoll sein, auch direkt auf die Information eines Vertragspartners zu verweisen. Letzteres ändert jedoch selten etwas an der Konstellation Betroffener-Verantwortlicher-Auftragsverarbeiter, sowie den damit einhergehenden Rechten und Pflichten.

Selbstverständlich müssen auch allen anderen Schritte der Umsetzung (z.B. Abwicklung der Rechte der Betroffenen) mit den jeweiligen Datenpartnern bewältigbar sein!

...im Falle eines Wechsels

Der Wechsel eines Datenpartners (Auftragsverarbeiters / Geschäftspartner... z.B. des Website Anbieters) kann aus verschiedenen Gründen nötig sein:

- Änderung bei Subauftragsverarbeitern (z.B. nicht DSGVO-konform)
- Ausfall bzw. Nichterfüllung gegenseitiger Anforderungen
- Zerwürfnisse

Selbstverständlich ist es sinnvoll, diese Informationen schon vorab zu kennen (siehe [Checkliste: Informationen zu einem Datenpartner](#)).

Notwendigkeit eines Datenschutzbeauftragten

Die Notwendigkeit zur Bestellung eines Datenschutzbeauftragten wird in verschiedensten Publikationen dargestellt¹³ und erläutert¹⁴. Da nach allgemeiner Meinung davon auszugehen ist, dass die Notwendigkeit der Bestellung auf einen Großteil der österreichischen Unternehmen nicht zutreffen wird, wird auf eine praxisbezogene Erläuterung an dieser Stelle bewusst verzichtet. Dafür wird **ungeachtet der Bestellung eines Datenschutzbeauftragten** darauf hingewiesen: **Gelebter Datenschutz benötigt ausreichendes Know-how**. Egal ob dieses in der Institution intern vorhanden ist oder durch externe Leistungen ergänzt wird.

¹³ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Der-Datenschutzbeauftragte.html

¹⁴

dsb.gv.at/documents/22758/112500/Leitlinien_in_Bezug_auf_Datenschutzbeauftragte.pdf/d241f0fd-6908-44fd-a12a-0f861e7a1dfb

Notwendigkeit einer Datenschutz-Folgenabschätzung

Das bisherige österreichische System des Datenverarbeitungsregisters mit den dazugehörigen DVR-Nummern wird durch die DSGVO abgelöst. In Zukunft wird vor allem auf Selbstevaluierung des Risikos von Datenanwendungen gesetzt.

Grundsätzlich sind **für alle** Datenanwendungen **passende technisch-organisatorische Maßnahmen** nach **‘aktuellem Stand der Technik, Aufwand und Risiko’** zu setzen. **Bei hohem Risiko** sowie in definierten Fällen ist **zusätzlich eine Datenschutz-Folgenabschätzung**¹⁵ durchzuführen.

Erweiterte Informationen zur Einstufung

Um diese Notwendigkeiten evaluieren zu können, kann das Verzeichnisse um die entsprechenden Informationen ergänzt werden (siehe [Erweiterte Informationen zur Einstufung](#)).

¹⁵ wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html

5. Juristisch

Auf Basis der **Zwecke und Rechtsgrundlagen** aus der Analyse gilt es zu definieren, ob das Betreiben der jeweiligen Datenanwendungen rechtmäßig ist.

Für die einzelnen Protagonisten muss überprüft werden, ob entsprechende Vereinbarungen vorhanden sind, in denen die Rechte und Pflichten der Vertragspartner definiert werden. Es gilt also, **Verträge und Einwilligungen mit Betroffenen, Auftragsverarbeitern sowie anderen Verantwortlichen** zu evaluieren. Ebenso sind die **Einhaltung von Informationspflichten** sowie von optionalen weiteren Rechtstexten zu überprüfen.

Anmerkung: Ein Berater (sofern kein Rechtsanwalt) kann lediglich überprüfen, ob ein Vertrag bzw. eine Rechtsgrundlage vorhanden ist. Er kann keine finale Aussage über Inhalt und Gültigkeit evaluieren. Dies gilt auch für die Zuordnung der daraus resultierenden Löschrfrist.

Zweck, Rechtsgrundlage und Aufbewahrungspflichten

Zwecke und Rechtsgrundlagen

Siehe auch [Zweck](#). Einen Eindruck für Zwecke der Datenverarbeitung liefern auch die bisherigen Standard- und Musterverordnungen aus dem bisherigen Datenschutzgesetz (DSG2000).

Tipp: Die Zuordnung der Zwecke sollte nicht nur nach Mustern erfolgen. Vielmehr macht es innerhalb einer Organisation Sinn zu überlegen, wofür einzelne Datenanwendungen (also Dateien, Formulare, etc...) tatsächlich benötigt werden. In der Praxis ergeben sich daraus vielfach 'Aha-Effekte', aus denen notwendige Schlüsse zur Optimierung von Datenmanagement und Unternehmensstabilität gezogen werden können.

Löschfristen bzw. Aufbewahrungspflichten

Das Prinzip der Datenminimierung bedeutet auch, dass personenbezogene Daten nur solange aufbewahrt werden dürfen, wie diese zur Erfüllung auch benötigt werden.

Sind Aufbewahrungspflichten in Gesetzen die Rechtsgrundlage einer Datenanwendung, so fallen hier die minimale und maximale Dauer der Datenverarbeitung zusammen. Dies bedeutet, dass Informationen für eine bestimmte Zeit verarbeitet werden müssen und danach zu löschen sind. Diese Aufbewahrungspflichten stehen nicht in der Datenschutz-Grundverordnung selbst, sondern ergeben sich aus den jeweiligen nationalen oder internationalen Gesetzen.

Die WKÖ hat als Service die wichtigsten Speicher- und Aufbewahrungspflichten zusammengefasst¹⁶.

¹⁶ <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html>

Auch das Auseinandersetzen mit den Aufbewahrungspflichten dient nicht nur der Umsetzung der Datenschutz-Grundverordnung, sondern hilft auch zu evaluieren, inwiefern andere gesetzliche Anforderungen im Informationsmanagement einer Institution bisher bedacht wurden.

Einwilligungen

Werden Einwilligungen als Rechtsgrundlage herangezogen, so sollten ein paar wichtige Regeln bedacht werden:

- **Freiwilligkeit und Kopplungsverbot** - eine Einwilligung muss immer so gestaltet sein, dass der Betroffene nicht dazu gezwungen wird oder mit anderen Einwilligungen bzw. Auswirkungen einhergeht
- **Widerrufbarkeit** - der Verantwortliche muss bedenken, was es für Auswirkungen hat, wenn der Betroffene seine Einwilligung zurückzieht. Auf die Möglichkeit des Widerrufs muss der Betroffene auch hingewiesen werden.
- **Aktive Einwilligung** - Einwilligung muss aktiv erfolgen, d.h. eine Zustimmung darf auf Formularen nicht vorausgefüllt sein. Auch ein stillschweigendes Hinnehmen einer Situation gilt nicht als Zustimmung (z.B. nur wenn jemand sich 10 mal nicht beschwert hat, dass seine Daten verarbeitet werden, bedeutet dies nicht, dass er es auch noch ein 11. Mal möchte)
- **Nachweisbarkeit** - es sollte (wie auch bei anderen Vertragsverhältnissen, die etwa mündlich abgeschlossen werden) immer die Problematik der Beweisbarkeit bedacht werden

Details dazu auf wko.at: 'Einwilligungserklärung'¹⁷. Beispiele finden sich auch beim Themenbereich 'Datenverarbeitung im Webshop und auf der Website'¹⁸.

Informationspflichten / Datenschutzerklärung

Der Betroffene muss entsprechend aufgeklärt werden. Details dazu auf wko.at: 'Informationspflichten'¹⁹

Zur leichteren Umsetzung wird außerdem mit einem online Ratgeber unterstützt²⁰.

Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung der beschriebenen Grundsätze für die Datenverarbeitung verantwortlich und muss ihre Einhaltung nachweisen können.

Anmerkung: es sind keine zusätzlichen Verzeichnisse zu führen, sondern es ist schriftlich zu vermerken, dass alles getan wird, was datenschutzrechtlich geboten ist. Es geht hier um die Beweislast bzw. Beweisbarkeit von rechtskonformen Verhalten. So ist zum Beispiel ein

¹⁷ [wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html)

¹⁸ [wko.at/service/wirtschaftsrecht-gewerberecht/datenverarbeitung-webshop-website.html](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/datenverarbeitung-webshop-website.html)

¹⁹ [wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Informationspflichten.html](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Informationspflichten.html)

²⁰ [dsgvo-informationsverpflichtungen.wkoratgeber.at/](https://www.dsgvo-informationsverpflichtungen.wkoratgeber.at/)

Aktenvermerk sinnvoll, dass innerhalb der gesetzlichen Frist Auskunft erteilt wurde, oder eine Einwilligungserklärung vorliegt.

Internationaler Datenverkehr

Die Übermittlung von Daten in das EU-Ausland ist nur in bestimmten Fällen zulässig.

Details siehe wko.at ²¹.

Datenpartner

Alle aus der Datenschutz-Grundverordnung resultierenden Auflagen und Pflichten gelten natürlich auch im Umgang mit Partnern. Speziell dann, wenn Daten an Dritte weitergegeben werden oder diese auf sonstige Weise Zugriff erhalten (z.B. externe Buchhaltung, Cloud-Anbieter, IT-Dienstleister). Eine spezielle Kombination ist gegeben, wenn dadurch Daten ins EU-Ausland gelangen. Der Verantwortliche hat dafür Sorge zu tragen seine Auftragsverarbeiter entsprechend auszuwählen und sicherzustellen, dass die DSGVO entsprechend eingehalten wird. Siehe dazu auf wko.at: 'Pflichten des Auftragsverarbeiters'²² und [Checkliste: Informationen zu einem Datenpartner](#).

²¹ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html

²² wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Pflichten-des-Auftragsver.html

6. Data & IT Security

Evaluierung des Risikos - CIA

Unabhängig von der Notwendigkeit einer Datenschutz-Folgenabschätzung gilt es, **zumindest die wichtigsten Quick-Wins für Data & IT-Security** zu evaluieren. Diese sind später unter Punkt 8 umzusetzen (technisch).

Das Risiko von Datenanwendungen sollte aus zwei Blickwinkel heraus evaluiert werden:

- **Risiko für die Rechte und Freiheiten der Betroffenen**
- **im Sinne der Unternehmensstabilität**

Siehe dazu auch [Risikobasiert](#).

Dabei gilt es wiederum verschiedene Ebenen zu betrachten:

- **C** (Confidentiality / **Vertraulichkeit**) - zielt darauf ab, dass Dritte Einsicht erhalten
- **I** (Integrity / **Integrität**) - zielt darauf ab, dass Daten verändert werden
- **A** (Accessibility / **Verfügbarkeit**) - zielt auf die Belastbarkeit von Systemen oder den Verlust von Daten ab (z.B. Backup)

Es gilt also zu evaluieren, wie groß der Schaden wäre, wenn beispielsweise:

- Akten öffentlich einsehbar und dadurch **Geschäftsgeheimnisse oder Daten von Betroffenen offengelegt** wären
- Daten in der Buchhaltung verändert und dadurch **Transaktionen falsch durchgeführt** würden
- Produktionssysteme oder Kommunikationsdienste ausfallen und dadurch **ein Unternehmen einen Serviceausfall** erleiden würde

...und einzuschätzen, ob die aktuellen Sicherheitsmaßnahmen ausreichend sind oder um zusätzliche technisch-organisatorische Maßnahmen erweitert werden müssen.

Hilfestellung bei der Evaluierung bietet die WKO mit [it-safe.at](#)²³.

Beispiele für technisch-organisatorische Maßnahmen

Die Datenschutz-Grundverordnung sieht vor, dass **technisch-organisatorische Maßnahmen (TOM)** nach aktuellem Stand / Aufwand / Risiko umzusetzen sind. Darunter können fallen:

- Zutrittskontrolle (Alarmanlage, Pförtner)
- Zugangskontrolle (Passwortverfahren, Verschlüsselung)
- Zugriffskontrolle (Berechtigungskonzepte, Protokollierung)
- Weitergabekontrolle (Verschlüsselung, VPN)
- Eingabekontrolle (Protokollierung, Protokollauswertungssysteme)
- Auftragskontrolle (Vertragsgestaltung bei ADV, Kontrollen)
- Verfügbarkeitskontrolle (Datensicherung/Backup, Firewall/Virenschutz)

²³ [it-safe.at](#)

- Trennungsgebot (Mandanten, Trennung der Systeme)

Die umgesetzten TOM sind wiederum im Verzeichnis festzuhalten.

Datenmanagement: Fit für DSGVO - privacy by design / default

Im Rahmen der DSGVO versteht man unter **privacy-by-design** bzw. **privacy-by-default**, dass Anwendungen und Prozesse so konzipiert werden, dass diese Informationen so **datenschutzfreundlich wie möglich** verarbeiten und auch **Voreinstellungen** (z.B. in Konfigurationseinstellungen oder bei Einwilligungen) von vornherein so gesetzt sind.

Egal ob Daten analog oder digital verarbeitet oder gespeichert werden. Es ist darauf zu achten, dass:

- so **wenig Daten wie möglich** bzw. nur so viel wie unbedingt notwendig verarbeitet werden
- Datenanwendungen **löschen / aussetzen / kopieren / übertragen können**, damit die Rechte der Betroffenen umgesetzt werden können
- **Voreinstellungen richtig gesetzt** werden

Datenschutz-Folgenabschätzung

Sollte eine Datenschutz-Folgenabschätzung notwendig sein (als Resultat aus Punkt 4), ist diese durch einen geeigneten Experten (z.B. Certified Data & IT-Expert) durchzuführen. Auf wko.at findet sich ein 'Ablaufplan für die Datenschutz-Folgenabschätzung'²⁴.

Die Datenschutzbehörde kann ein Black- bzw. White-Listening für Datenanwendungen veröffentlichen, für die jedenfalls eine Datenschutz-Folgenabschätzung vorgenommen werden muss bzw. die davon ausgenommen sind.²⁵

²⁴ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Ablaufplan-Datenschutz-Fo.html

²⁵ Aktueller Stand in Österreich zum Zeitpunkt im Mai 2018 siehe https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.pdf#sig

7. Funktional

Prozesse und Datenschutz Policy

Gelebter Datenschutz (und damit auch die Risikominimierung, um mit Strafen in Berührung zu kommen) erfordert klare Vorgehensweisen, die auch innerhalb der Organisation entsprechend kommuniziert werden, beispielsweise:

- welche Dateien sollen auf welchen Verzeichnissen mit unterschiedlichen Zugriffsberechtigungen abgelegt werden
- wo und wie werden Kundendaten abgelegt und verwaltet
- wie werden Projekte dokumentiert
- wie wird mit abgelehnten Bewerbungen umgegangen
- was wird im E-Mail Ordner gespeichert oder sollte besser gleich verschoben werden
- welche Daten sollten überhaupt per E-Mail versandt werden oder besser über einen sicheren Cloud-Link
-

Umsetzung der Rechte der Betroffenen

Definition der Prozesse, um zumindest die Rechte der Betroffenen innerhalb der Frist (1 Monat)²⁶ abwickeln zu können:

- Anfrage entgegennehmen (z.B. Bekanntgabe einer E-Mail in der Datenschutzerklärung: datenschutz@firmenname.at)
- Identitätsfeststellung (wie kann die Identität des Betroffenen verifiziert PLUS wie können die Datensätze zugeordnet werden)
- Zuständigkeiten (Ansprechpartner innerhalb der Organisation und ggf. bei Datenpartnern)
- Abfrage / Sperrung / Löschung (wie durchzuführen und auch separiert von anderen Betroffenen durchgeführt werden)
- Output Kontrolle (Überprüfung der Qualität)
- Rückmeldung (Formulierung und Art)
- Timeline (wie lange benötigen die einzelnen Schritte und kann die Frist auch eingehalten werden - auch wenn ein Ansprechpartner nicht verfügbar sein sollte [z.B. Urlaub, Krankenstand...])
- Controlling (Ablaufkontrolle, dass die Umsetzung innerhalb der Frist erfolgt)

Siehe auch auf wko.at: 'Auskunftspflicht des Verantwortlichen'²⁷ und 'Musterschreiben zur Auskunftserteilung'²⁸.

²⁶ in Ausnahmesituationen auch länger siehe

wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Betroffenenrechte.html

²⁷ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Auskunftspflicht-des-Vera.html

²⁸ wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-musterschreiben-auskunftserteilung.html

Schulungen

Ursache für den Großteil an Datenschutzvorfällen ist menschliches Versagen. Durch Schulungsmaßnahmen kann dem entsprechend entgegengewirkt werden. Ebenso schaffen fix definierte Prozesse (z.B. bei Zahlungsanweisungen) Abhilfe gegen Angriffe (z.B. gegen 'CEO-Fraud'²⁹).

²⁹ de.wikipedia.org/wiki/CEO_Fraud

8. Technisch

Die vorab definierten Auswirkungen sind auch technisch umzusetzen. Hier kann ein Certified Data & IT-Security Expert unterstützen. Zu beachten ist, dass gerade dieser Punkt die längste Umsetzungszeit benötigen könnte.

9. Vorbereitung Datenschutzvorfall

Allgemeines zu Datenschutzvorfällen siehe [Datenschutzvorfall](#).

Auf Basis der Analyse-Ergebnisse (aus Punkt 3) gilt es, Vorkehrungen für einen Datenschutzvorfall zu treffen - siehe [Checkliste: Vorbereitung auf einen Datenschutzvorfall](#).

Datenschutzvorfälle sind grundsätzlich zu dokumentieren und je nach Risiko für die Rechte und Freiheiten der Betroffenen zu melden - siehe auf wko.at:

- 'Meldung von Datenschutzverletzungen (Data Breach Notification)'³⁰
- 'Mustermeldung Behörde'³¹
- 'Muster Benachrichtigung der betroffenen Person'³²

10. Dokumentation, laufende Adaptierung und Audits

Die Dokumentation ist wesentlich, da alle gesetzten Maßnahmen entsprechend nachzuweisen sind. Darunter fallen:

- Verfahrensverzeichnis
- Rechenschaftspflicht (Art 5)
- Datenschutz-Folgenabschätzung
- Data-Breach (Datenschutzverletzungen...)
- Juristisch (Informationspflicht, Einwilligungen, Verträge, Auftrag, EU-Ausland)
- Abwicklung der Rechte der Betroffenen
- Datensicherungsmaßnahmen (Datenschutz-Handbuch / Schulungsmaßnahmen, TOM)
- ...

Der tatsächliche Dokumentationsumfang ist abhängig von den individuellen Gegebenheiten der Organisation.

Keinesfalls ist die Umsetzung der DSGVO eine einmalige Sache. Vielmehr gilt es bei Änderungen in den Datenanwendungen entsprechenden Anpassungen durchzuführen sowie die Einhaltung der Maßnahmen zur Datensicherheit laufend zu auditieren.

³⁰ wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Meldung-von-Datenschutzve.html

³¹ wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.html

³² wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-betroffene.html

Spezifika Fahrschulen

Ärztliches Gutachten (Gesundheitsbefund)³³

Vor der Erteilung einer Lenkberechtigung hat der Antragsteller (Fahrschüler) der Behörde ein ärztliches Gutachten vorzulegen, dass er zum Lenken von Fahrzeugen geeignet ist (§ 8 FSG). Das Prozedere der Weiterleitung ist je nach Fahrschule und Bundesland unterschiedlich (direkte Übergabe an einen der Prüfer, Versand per E-Mail, Versand per Fax).

Erläuterung zur Notwendigkeit eines Datenschutzbeauftragten

Kerntätigkeit: Wenn die Fahrschule so wie bisher im Kulanzweg das Dokument im Kuvert einsammelt und an die Behörde weiterleitet, ist das eine zu vernachlässigende Serviceleistung, da dies keine Haupttätigkeit der Fahrschule darstellt. Die Übermittlung des Dokuments ist eine reine Zusatzleistung der Fahrschule, die nicht im Rahmen der Kerntätigkeit (Ausbildungsauftrag) der Fahrschule statt findet.

Umfang: Auch die Anzahl der Dokumente ist als nicht umfangreich einzustufen (immer nur wenige gleichzeitig, kurze Aufbewahrungsdauer etc).

Daraus ist abzuleiten, dass kein Datenschutzbeauftragter benötigt wird.

Rechtsgrundlage

Einwilligung des Schülers einholen, dass er das Zusatzservice wie folgt in Anspruch nehmen möchte:

- Offline Übergabe bei Bedarf in einem verschlossenen Kuvert
- Online Vorweg-Übermittlung in einer unverschlüsselten E-Mail

Spezifika Mitarbeiter

Arbeitnehmerdatenschutz im Allgemeinen

- Überprüfung von Dienstverträgen, Betriebsvereinbarungen, Dienstordnungen, etc
- Rechtzeitige Kommunikation mit dem Betriebsrat

³³ Quelle Fachverband für Fahrschulen und Allgemeiner Verkehr WKÖ

Verpflichtung zum Datengeheimnis

siehe [Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen](#)³⁴

Privatnutzung³⁵

Grundsätzlich empfiehlt es sich die private Nutzung zu untersagen. Sollte dennoch die private Nutzung zugelassen werden:

Mobile Device Management-Lösung einsetzen: Mit einer MDM-Lösung verfügt man über eine entsprechende Kontrolle über die Gerätenutzung. Im Falle von BYOD von Tablet und Smartphone ist die Zustimmung des Mitarbeiters notwendig. Softwarelösung zur Verschlüsselung sowie Trennung zwischen privatem und geschäftlichen Teil nützen.

E-Mail: Wenn Folgendes geregelt ist, darf man auf den Mail-Account eines Mitarbeiters zugreifen:

- Der Zugriff ist aus betrieblichen Gründen notwendig,
- Den Mitarbeitern wurde die Privatnutzung des beruflichen Mail-Accounts verboten (Achtung: mögliche sensible Daten vorhanden – Kommunikation mit Arzt, usw.)
- Die Mitarbeiter wurden über die Möglichkeit eines Zugriffs informiert, bzw. in Betrieben mit Betriebsrat gibt es eine Betriebsvereinbarung darüber

Verarbeitung nicht-sensibler Daten bei Einsichtnahme in den Mail-Account des Mitarbeiters stützt sich auf die Rechtsgrundlage des überwiegend berechtigten Interesses (Art 6 Abs 1 lit f DSGVO).

Die Pflicht Mitarbeiter über einen etwaigen Zugriff zu informieren, resultiert aus der Pflicht den Betroffenen immer über den Zweck der Verarbeitung seiner Daten zu informieren (Art 13 Abs 1 lit c, Art 14 Abs 1 lit c – DSGVO).

Datenschutzerklärung für Mitarbeiter

siehe [EU-Datenschutz-Grundverordnung \(DSGVO\): Datenschutzerklärung für Mitarbeiter](#)

³⁶Anmerkung: Die Datenschutzerklärung ist auf die individuellen Anwendungen im Unternehmen anzupassen (inkl. Besonderheiten wie GPS, Maut, etc...). Tipp: Gleichen Sie die Informationen dieser Datenschutzerklärung mit Ihrem Verarbeitungsverzeichnis ab!

³⁴

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtungserklaerung-datengeheimnis.html>

³⁵ Quelle Fachverband für das Güterbeförderungsgewerbe WKÖ

³⁶ <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/dsgvo-muster-datenschutzerklaerung-mitarbeiter.html>

Checklisten

Checkliste: Ergebnisse aus 10 Punkte-Programm

Nach Abwicklung des 10 Punkte-Programms sollten Sie sich unter anderem mit folgenden Bereichen beschäftigt haben:

- Verfahrensverzeichnis
- Rechtsgrundlagen, Verträge und Informationspflichten
- Datenübermittlung ins Ausland
- Datenschutz-Folgenabschätzung
- Datenschutzbeauftragter
- Privacy by design / default
- Datensicherheitsmaßnahmen / Technisch-organisatorische Maßnahmen
- Prozesse für Rechte der Betroffenen
- Vorbereitung Data Breach
- Compliance intern & extern (Dokumentation, laufende Adaptierung und Audits)

Checkliste: Teil-Schritte der Analyse von Datenanwendungen

Die **IST-Analyse ist der Kern der Umsetzung der Vorgaben der DSGVO**. Das **Ziel ist eine Übersicht über die wichtigsten Datenanwendungen im Unternehmen**. Dabei wird empfohlen, mehrstufig vorzugehen. Stufe 3.1 und 3.2 dienen der **Identifikation** der Datenanwendung. In Stufe 3.3 und 3.4. erfolgt eine **Segmentierung und Priorisierung**. Ab Stufe 3.5 erfolgt die eigentliche **Erstellung des Verfahrensverzeichnisses** sowie die Erhebung von **Metadaten**, die zur weiteren Umsetzung der DSGVO benötigt werden:

3. Analyse (IST-Stand, Verfahrensverzeichnis, kritische Unternehmensprozesse)

- *Identifikation von Datenanwendungen* -

- 3.1. Grob-Auflistung (zwecks Überblick) aller
 - a. Gerätetypen (Notebook Typ Geschäftsführung, Vertriebsmitarbeiter...)
 - b. Speicherorte
 - c. Datenpartner (Auftragsverarbeiter / Dienstleister, Geschäftspartner...)
- 3.2. Detail-Auflistung aller Anwendungen in
 - a. Software
 - b. Cloud Applikationen und Services (Zusätzlich zu 1c)
 - c. Dateien (Excel Sheets, Access Datenbanken...)

- *Segmentierung und Priorisierung von Datenanwendungen* -

- 3.3. Gruppierung nach:
 - a. Abteilung (z.B. Kerntätigkeit A, Kerntätigkeit B, Backoffice, IT-Infrastruktur - inkl. Ansprechpartner bzw. individueller Verantwortlichkeiten pro Anwendung)
 - b. Verfahren (Buchhaltung, CRM...)
- 3.4. Priorisierung der Verfahren bzw. Anwendungen nach:

- a. Relevanz für Umsetzung der DSGVO
- b. Relevanz für IT-Sicherheit und Unternehmensstabilität (zeigt einen anderen Blickwinkel und ist dadurch natürlich auch für DSGVO Compliance von Relevanz)

- Informationen pro Datenanwendung -

- 3.5. Erhebung der **Datenkategorien** (inkl. Einstufung z.B. sensibel)
- 3.6. Metadaten I - **Rechtlich**
 - a. Zwecke (Verwaltung von Kundendaten, Buchhaltung...)
 - b. Rechtsgrundlagen (Vertragserfüllung, Einwilligung... auch für sensible Daten)
 - c. Löschrfrist (bzw. Aufbewahrungspflichten)
- 3.7. Metadaten II - **Protagonisten**
 - a. Betroffene (Kunden, Lieferanten...) - Daten von **Kindern** (ja/nein)
 - b. Empfängerkategorien (inkl. Auftragsdatenverarbeiter und Informationen über Sub-Auftragsverarbeiter, Zugriffsberechtigte Personen, Datenübermittlung ins EU-Ausland)
 - c. Herkunft / Datenquelle (auch Drittquellen, die direkt von einem Auftragsverarbeiter ergänzt werden bzw. Informationen, die der Anreicherung dienen)
 - d. Aufbewahrungs- und Speicherorte (Aktenschrank, Abteilungsverzeichnis, Cloudspeicher, Festplatten...)
 - e. TOM (Technisch Organisatorische Maßnahmen soweit vorhanden - siehe auch unten)

Checkliste: Erweiterte Informationen zur Einstufung von Datenanwendungen

Um die Auswirkungen auf die Anforderungen des Datenschutzes evaluieren zu können, sollten die Informationen zu den Datenanwendungen noch entsprechend ergänzt werden.

- 3.8. Metadaten III - **Risiko und Maßnahmen**
 - a. Art der Datenübertragung (z.B. Mail, SFTP, Cloud Speicher)
 - b. Risikoabschätzung
- 3.9. Metadaten IV - **Einstufung** (zur Priorisierung und Evaluierung der Notwendigkeit eines Datenschutzbeauftragten, einer -Folgenabschätzung)
 - a. Sensibilität (im Sinne des Datenschutzes)
 - b. Kritikalität (im Sinne der Unternehmensstabilität)
 - c. Häufigkeit
 - d. Kernaktivität (ja / nein)
 - e. Umfang
 - f. Systematische Beobachtung (ja / nein)
 - g. Automatische Entscheidungsfindung oder Profiling (inkl. Beschreibung von Logik und Auswirkung)

Checkliste: Informationen zu einem Datenpartner

Die angeführten Fragestellungen können aus verschiedenen Gründen in unterschiedlichen

Ausprägungen benötigt werden (siehe [Informationen zu Datenpartnern](#)):

...für Start, Beendigung oder Wechsel

- Funktional (Funktion, Umfang und Zweck der Datenverarbeitung plus optional Kategorien der Betroffenen)³⁷
- Welche Datenkategorien werden benötigt bzw. verarbeitet?³⁸
- In welchem Format werden die Daten gegenseitig zur Verfügung gestellt?
- Wie werden die Daten zugänglich gemacht (z.B. Download)?
- Prozessbeschreibung: Wie kann ein Wechsel möglichst einfach erfolgen (z.B. wenn Subauftragsverarbeiter ohne Zustimmung gewechselt wird oder der Auftragsverarbeiter ausfällt)?
- Was ist zur Wiederinbetriebnahme bei einem anderen Partner notwendig? (Schritte, Kenntnisse, Systemanforderungen, Tools, Zeit / Kosten)
- Wie erfolgt die Löschung beim Partner (nach Beendigung des Auftrags bzw. bei Wegfall der Rechtsgrundlage)?

...plus allgemein

- Gegenstand des Vertrags
- Dauer des Vertrags
- Technisch-organisatorische Maßnahmen (zu C-Vertraulichkeit, I-Integrität, A-Verfügbarkeit - und wie erfolgen Audits)
- Regelungen zum Datengeheimnis (Vertraulichkeitspflichten) der Mitarbeiter des Datenpartners
- Regelungen zur Zulässigkeit von Subauftragsverhältnissen
 - Gibt es eine Regelung, wie ein Subauftragnehmer zu beauftragen ist?
 - Gibt es eine Regelung zur Genehmigung von Subauftragsverhältnissen (z.B. wenn Subauftragsverarbeiter ohne Zustimmung gewechselt wird oder der Auftragsverarbeiter ausfällt)?
- Regelungen zur Unterstützung bei der Umsetzung der Rechte von Betroffenen³⁹
- Regelungen zur Vorgehensweise bei einem Datenschutzvorfall⁴⁰
- Regelungen zu Kontrollrechten des Datenpartners bzw. deren Subauftragnehmern

Checkliste: Umsetzung der Rechte der betroffenen Personen

Wie können *Informationspflicht, Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung, Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit, Widerspruchsrecht* umgesetzt werden (siehe auch [Umsetzung der Rechte der Betroffenen](#))?

³⁷ siehe auch Informationen pro Datenanwendungen bei [Checkliste: Teil-Schritte der Analyse von Datenanwendungen](#)

³⁸ siehe auch Informationen pro Datenanwendungen bei [Checkliste: Teil-Schritte der Analyse von Datenanwendungen](#)

³⁹ siehe auch [Checkliste: Umsetzung der Rechte der betroffenen Personen](#)

⁴⁰ siehe auch [Checkliste: Vorbereitung auf einen Datenschutzvorfall](#)

- Technische und funktionale Umsetzbarkeit - kann ausreichend informiert, beauskunftet, exportiert, gelöscht oder deaktiviert werden? (ohne die Rechte von anderen Personen zu verletzen)
- Identitätsfeststellung und Zuordnungsbarkeit von Personen und Daten (wie kann festgestellt werden, ob es sich bei einer Anfrage beispielsweise wirklich um Franz Meyer handelt - und - gehört der Datensatz Franz Meyer auch zur Person Franz Meyer oder gibt es mehrere Franz Meyer in meiner Datenbank)
- Ansprechpartner, Verantwortlichkeiten und Zuständigkeiten
- Geschätzte Dauer zur Erfüllung
- Ablauf und Protokollierung

Checkliste: Vorbereitung auf einen Datenschutzvorfall

Um im Falle eines Datenschutzvorfalls (siehe [9. Vorbereitung Datenschutzvorfall](#)) schnell und richtig agieren zu können, sollte vorab das Bewusstsein für verschiedene Szenarien geschaffen werden:

A. Szenarien

- mögliche Arten von Datenschutzvorfällen bedenken
 - Art: (C - Vertraulichkeit / I - Veränderung / A - Verfügbarkeit)
 - z.B. C - Einsicht / I - Manipulation / A - Löschen - durch Verlust, Einbruch, Diebstahl, Auftreten von Sicherheitslücken und Bugs
- Feststellung: Alerts / Intrusion Detection

B. Auswirkungen

- Folgen für Betroffene
- Erkennung

C. Kommunikation

- Wie wird Verantwortlicher in Kenntnis gesetzt?
- Wie werden andere Stakeholder in Kenntnis gesetzt?
- Wer soll davon erfahren?
- Wer soll NICHT davon erfahren (kein Ausplaudern, bevor Schutz hergestellt werden konnte z.B. bei Sicherheitslücken / Bugs)?
- Wie können Betroffene bei Bedarf informiert werden?
 - Zielgerichtet (also nur an jeweilige Person: Identitätsfeststellung)
 - Vertraulich (über sicheren Kommunikationskanal)

D. Vorgehensweise

- Ansprechpartner (Kontaktdaten und Kontaktzeiten)
- Maßnahmen
 - Maßnahmen zur Abmilderung der Auswirkungen der Verletzung (Stecker ziehen vs. Abschottung)
- Kommunikation und Beschreibung
 - Protokollierung von Datum und Uhrzeit des Vorfalls
 - Beschreibung der Art der Verletzung
 - Kategorien und Zahl an Betroffenen
 - Kategorien und Zahl an Daten

- Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung
- Begründung, falls die Meldung länger als 72h nachdem der Vorfall dem Verantwortlichen bekannt wurde, erfolgte