Datenschutzmanagement nach der DSGVO „Wie organisiere ich den Datenschutz im Unternehmen“

Prof. KommR Hans-Jürgen Pollirer

anlässlich der Veranstaltung

„Datenschutz im Fokus
Das neue Datenschutzregime ab Mai 2018!“

Wien, 13. Oktober 2017

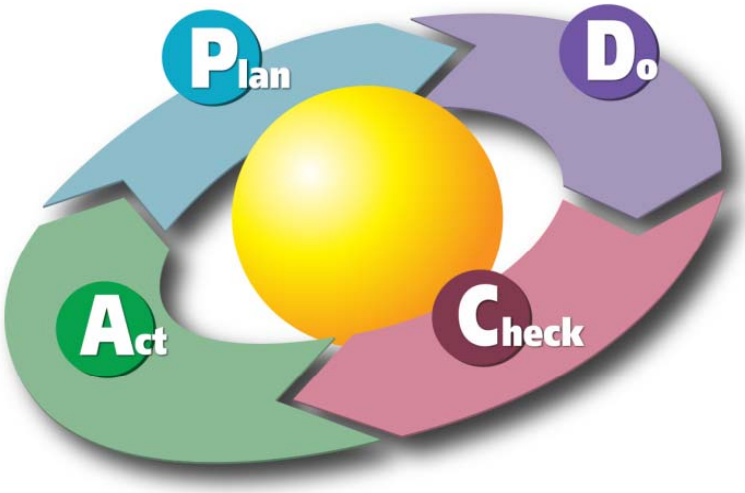
ÜBERSICHT

Art. 5 Abs. 2 DSGVO

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

FAZIT:

- Das Unternehmen muss den Nachweis erbringen können, dass es die Anforderungen der DSGVO umgesetzt hat.
- Lt. ErwGr 74 bezieht sich diese Nachweispflicht auch auf die Wirksamkeit der umgesetzten Maßnahmen
- Art. 24 Abs. 1 fordert die Berücksichtigung geeigneter technischer und organisatorischer Maßnahmen und den Nachweis, dass die Verarbeitung nach den Bestimmungen der DSGVO erfolgt ist sowie, dass diese Maßnahmen erforderlichenfalls überprüft und aktualisiert werden.
- Datenschutz ist somit kein Einmalereignis sondern eine kontinuierliche Verpflichtung zur Überwachung und Verbesserung der getroffenen Maßnahmen.
- In diesem Zusammenhang hat sich der Plan-Do-Check-Act-Zyklus (PDCA-Zyklus) bewährt.



Quelle: Karn G. Bulsuk (http://www.bulsuk.com)

2. Die Datenschutzleitlinie („Datenschutzpolitik“)

Datenschutzleitlinie =

- Selbstverpflichtung des Unternehmens zur Umsetzung des Datenschutzes
- Dokumentation der Datenschutzziele, Rollen und Verantwortlichkeiten (Governance-Struktur)
- Innen- und Außenwirkung

Inhalte:

- Einleitung
- Geltungsbereich
- Grundprinzipien des Datenschutzes
- Datenschutzziele des Unternehmens
- Verantwortlichkeiten
- Datenschutzbeauftragter
- Auditing
- Sanktionen bei Verstößen

3. Datenschutzmanagement-System (DSMS)

I. PLAN – Aufbau eines Managementsystems

In der Planungsphase werden zunächst die Ziele formuliert und die Anforderungen identifiziert. Es erfolgt darüber hinaus eine Bestandsaufnahme der im Unternehmen eingerichteten Prozesse und implementierten Datenanwendungen und Richtlinien. Erstellung eines Umsetzungsplanes und Realisierung der Anforderungen.

II. DO – Implementierung des Managementsystems

In dieser Phase werden die Ziele und Maßnahmen aus der Planungsphase implementiert und die Verantwortlichkeiten festgelegt. Besonders wichtig ist in dieser Phase die Schulung und Sensibilisierung der Mitarbeiter.

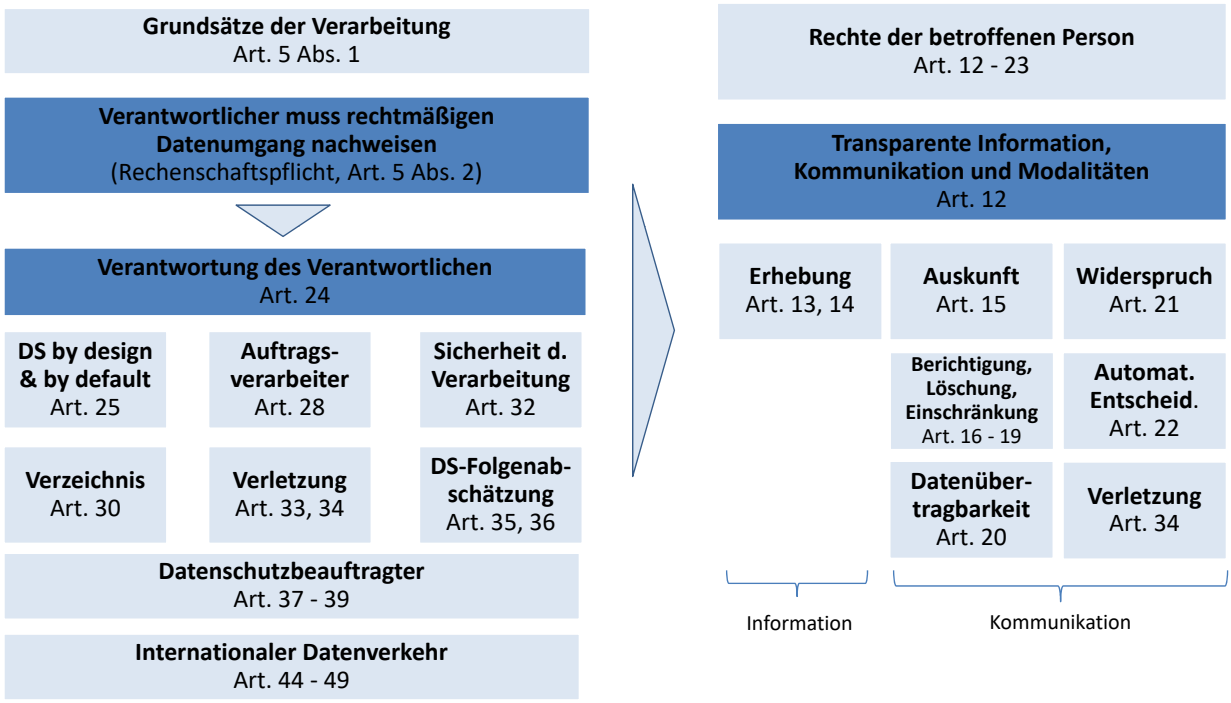
III. CHECK – Überprüfung durch ständige Überwachung

Die Wirksamkeit der Umsetzung muss überprüft werden (Audit). Das bedeutet, eine laufende Überwachung der umgesetzten Maßnahmen und Prozesse.

IV. ACT – Optimierung und Mängelbeseitigung

Der in Phase III durchgeführte Auditprozess kann die Notwendigkeit von Änderungen von Zielen, Maßnahmen und Richtlinien ergeben. Die Verbesserung bzw. Beseitigung von Mängeln findet in dieser Phase statt.

4. Die wesentlichen Datenvorschriften der DSGVO



Quelle: *Kranig/Sachs/Gierschmann*, Datenschutz-Compliance nach der DS-GVO, 2017, Bundesanzeiger Verlag

5. Die Datenschutz-Kernprozesse

- Verarbeitung
- Sicherstellung der Betroffenenrechte
- Vorgangsweise bei Datenschutzverletzungen (Data Breach)

5.1 Verarbeitung

Plan	Do	Check	Act
Einhaltung der Datenschutzgrundsätze	Umsetzung in den Betrieb	Monitoring	Maßnahmen zur Behebung der Schwachstellen
Rechtmäßigkeit der Verarbeitung	Festlegung der Zuständigkeiten und Verantwortlichkeiten	Internes Audit	Überprüfung der Wirksamkeit der Verbesserungs-maßnahmen
Einwilligungserklärungen	Schulung und Sensibilisierung der Mitarbeiter	Externes Audit	
Informationspflichten	Umsetzung der Löschfristen (Löschkonzept)		
Sicherheit			
Risikoanalysen			
Datenschutz-Folgenabschätzung			
Auftragsverarbeitung			
Dokumentation (sog. Verfahrensverzeichnis)			
Datenschutzbeauftragter			
Übermittlung in Drittländer			

5.2 Sicherstellung der Betroffenenrechte

Plan	Do	Check	Act
Gestaltung der Verfahren und Prozesse zur Erfüllung der nachfolgenden Betroffenenrechte: - Auskunft - Richtigstellung - Löschung - Einschränkung - Mitteilungspflicht - Datenübertragbarkeit - Widerspruch - Widerruf - Automatisierte Einzelentscheidung	Festlegung der Zuständigkeiten und Verantwortlichkeiten	Analyse der Wahrnehmung von Betroffenenrechten (Anzahl, erledigt/offen etc.)	Festlegung von Maßnahmen zur Verbesserung der Prozesse
	Einrichtung eines Eskalationsprozesses	Identifikation von Verbesserungs-möglichkeiten	Überprüfung der Wirksamkeit der Verbesserungs-maßnahmen
	Terminverfolgung	Schwerpunkte der Anfragen	
	Dokumentation	Auditbericht	

5.3 Vorgangsweise bei Datenschutzverletzungen (Data Breach)

Plan	Do	Check	Act
Festlegung der Vorgangsweise bei einer Datenschutzverletzung nach folgenden Gesichtspunkten - Fristen - Bewertung - Inhalt der Meldungen an die DSB - Inhalt der Benachrichtigung an die betroffene Person - Maßnahmen - Dokumentation	Festlegung der Verantwortlichkeiten und Zuständigkeiten (Notfallsteam) Training	Verbesserung in Bezug auf die Vorgangsweise Verbesserung der technischen und organisatorischen Maßnahmen	Festlegung von Maßnahmen zur Behebung von Schwachstellen Systematische Nachverfolgung der Umsetzungsmaß-nahmen

6. Weitere Informationen zur EU Datenschutzgrundverordnung

Unter dem Link https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html finden Sie zielführende Informationen, wie Sie sich auf den 25. Mai 2018 vorbereiten können. Die abgelegten Informationen werden laufend erweitert.

Anhang I: Beispiel: Datenverarbeitungsverzeichnis nach Art. 30 Abs. 1 EU-Datenschutz-Grundverordnung (DSGVO) (Verantwortlicher)

Diskussion

Ich danke für Ihre Aufmerksamkeit

Besuchen Sie uns auch im Internet!
Sie finden uns unter **http://www.secur-data.at**

Meine E-Mail-Adresse lautet **hj.pollirer@secur-data.at**

WIRTSCHAFTSRECHT

WKO WIRTSCHAFTSKAMMERN ÖSTERREICHS

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

BEISPIEL

Datenverarbeitungsverzeichnis nach Art 30 Abs 1 EU-Datenschutz-Grundverordnung (DSGVO) (Verantwortlicher)

(HINWEIS: es wird darauf hingewiesen, dass es sich hier um ein fiktives Beispiel handelt. Bei der praktischen Umsetzung ist auf die konkreten Anwendungsfälle im Unternehmen abzustellen)

Inhalt

A. Stammdatenblatt

Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen

a. Name(n) und Anschrift(en):
Max Mustermann GmbH
Neuer Weg 1
ZZZZ Musterdorf

b. E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):
max@mustermann.at

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten[1]:
Franz Fachmann e.U.
Datenstraße 5
YYYY Datenstadt

d. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Vertreters des (der) Verantwortlichen:[2]
KEINER

[1] Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde.
HINWEIS: Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „*Datenschutzbeauftragter*“ genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (zB „*Datenschutzkoordinator*“). Dieser kann, muss aber nicht ins Verfahrensverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt „Datenschutzbeauftragter“.
[2] Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.

B. Datenverarbeitungen/Datenverarbeitungszwecke

1. **Zwecke und Beschreibung der Datenverarbeitung[3]:**
   1. **Rechnungswesen und Geschäftsabwicklung:** Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenzen oder Verträge) in diesen Angelegenheiten
   2. **Personalverwaltung: …….**
   3. **Marketing: ……**
   4. **Geschäftspartnerdatenbank: …….**
   5. **usw.**

2. **Wurde eine Datenschutz-Folgenabschätzung durchgeführt?[4]**

   Ja ☐ X Nein ☐

   Wenn Ja, wann?
   zuletzt vor 6 Monaten

   Wenn Nein, aus welchem Grund nicht?[5]

[3] Zum Begriff „Verarbeitung“ siehe das Merkblatt „Wichtige Begriffsbestimmungen“; sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren.
[4] Zur Datenschutz-Folgenabschätzung siehe das Merkblatt „Risiko-Folgenabschätzung“. Im Verarbeitungsverzeichnis sind zwar Angaben zur Datenschutz-Folgenabschätzung nicht zwingend vorgesehen. Aus Gründen der Rechenschaftspflicht empfehlen sich aber grundsätzliche Angaben darüber auch ins Verarbeitungsverzeichnis aufzunehmen.
[5] Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, wenn durch die Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte der Betroffenen besteht oder die Datenverarbeitungsart in der sogenannten „white list“ der Datenschutzbehörde gelistet ist (derzeit besteht noch keine „white list“); Näheres dazu siehe auch das Merkblatt „Risiko-Folgenabschätzung“.

C. Detailangaben zu (1) Rechnungswesen und Geschäftsabwicklung

1. Kategorien der betroffenen Personen

Lfd.Nr.	*Beschreibung der Kategorien betroffener Personen (zB Kunden, Mitarbeiter, Lieferanten usw.)*
1	Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten
2	Sachbearbeiter beim Verantwortlichen
3	An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten

2. Rechtsgrundlagen[6]

Art 6 Abs 1 lit a (*Einwilligung der Betroffenen*), b (*zur Vertragserfüllung erforderlich*), c (*gesetzliche Verpflichtungen nach der BAO und dem UGB*), f (*berechtigte Interessen des Verantwortlichen*) DSGVO
§ 132 BAO
§§ 190, 212 UGB

3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten[7]) sind abgelegt:[8] (freiwillig)

Unterlagen zu aufrechten Geschäftsabwicklungen in der Verkaufsabteilung, Rechnungen (auch) in der Finanzabteilung, erledigte Geschäftsfälle im Archiv. Verträge mit Auftragsverarbeitern sind, je nach Thematik, in der Rechtsabteilung, Finanzabteilung, Vertriebsabteilung oder IT-Abteilung abgelegt.

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[9]

a. Kategorien der verarbeiteten Daten und Ankreuzen, ob sie an Empfänger übermittelt werden

---

[6] Die Rechtsgrundlagen (zB rechtliche Verpflichtung, Einwilligung, Vertragserfüllung, lebenswichtige Interessen des Betroffenen, kein überwiegendes berechtigtes Interesse des Betroffenen) sind nach der DSGVO zwar nicht verpflichtend ins Verfahrensverzeichnis aufzunehmen. Allerdings unterliegt der verantwortliche Verarbeiter einer sogenannten Rechenschaftspflicht. Diese besagt eine Nachweispflicht bzgl. der Einhaltung der Pflichten nach der DSGVO. Dazu gehört unter anderem auch der Nachweis, dass die Datenverarbeitung nach den in der DSGVO normierten Rechtmäßigkeitsgrundlagen erfolgt. Siehe das Merkblatt „Grundsätze und Rechtmäßigkeit der Verarbeitung“.

[7] Siehe zu den Informationspflichten das Merkblatt „Informationspflichten“.

[8] Die Angabe, wo die Unterlagen innerhalb der Organisation abgelegt wurden, ist nicht verpflichtend im Verarbeitungsverzeichnis zu dokumentieren, erleichtert aber vor allem in größeren, arbeitsteilig organisierten Organisationen das Auffinden der entscheidenden Unterlagen (dient also lediglich der innerbetrieblichen Arbeitserleichterung).

[9] Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verfahrensverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (zB „nach Ablauf des Vertrages“).

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO[10], strafrechtlich relevant iSd Art 10 DSGVO[11]	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden Im Anlassfall	Inkassounternehmen Im Anlassfall	Fremdfinanzierer (zB Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)
1	1	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	X	X	X	X	X	X	X	X	X	X
	2	Anschrift	Nein	X	X	X	X	X	X	X	X	X	X
	3	Kontaktdaten (Tel., Mail,Fax)	Nein	X	X	X	X	X	X	X	X	X	X
	4	Firmenbuchdaten	Nein	X	X	X	X	X	X	X	X	X	X
	5	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		X		X						
	6	Bankverbindungen	Nein	X	X	X	X	X	X	X	X	X	
	7	Kreditkartennummern und -unternehmen	Nein	X	X	X	X						
	8	UID-Nummer	Nein	X	X	X	X	X	X	X	X	X	
	9	Namen der Kontaktpersonen	Nein	X	X	X	X	X	X	X	X	X	X
	10	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.)	Nein	X	X	X	X	X	X	X	X	X	X
	11	Vertragstexte und Geschäftskorrespondenzen		X	X	X	X	X	X	X		X	
2	12	Name	Nein	X	X	X	X	X	X	X	X	X	X
	13	Funktion des betroffenen Sachbearbeiters beim Verantwortlichen	Nein	X	X	X	X	X	X	X	X	X	X
	14	Vom betroffenen Sachbearbeiter bearbeitete Fälle	Nein	X	X	X	X	X	X	X	X	X	X
	15	Umfang der Vertretungsbefugnis	Nein	X	X	X	X	X	X	X	X	X	X
3	16	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	X	X	X	X	X	X	X	X	X	X
	17	Anschrift	Nein	X	X	X	X	X	X	X	X	X	X
	18	Kontaktdaten (Tel., Mail, Fax odgl.)	Nein	X	X	X	X	X	X	X	X	X	X
	19	Firmenbuchdaten	Nein	X	X	X	X	X	X	X	X	X	X
	20	Namen der Kontaktpersonen	Nein	X	X	X	X	X	X	X	X	X	X
	21	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.)	Nein	X	X	X	X	X	X	X	X	X	X
	22	UID-Nummer	Nein	X	X	X	X	X	X	X	X	X	X
	23	Bankverbindungen	Nein	X	X	X	X	X	X	X	X	X	
	24	Kreditkartennummern und -unternehmen	Nein	X	X	X	X						
	25	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		X	X	X						

[10] Daten nach Art 9 DSGVO sind besondere Datenkategorien („sensible Daten): rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

[11] Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln unter behördlicher Aufsicht.

b. Löschungs- und Aufbewahrungsfristen (wenn möglich)

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-4; 6-24; 26;	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
5; 25;	Bis zur Beendigung der Geschäftsbeziehungen

5. Kategorien von Empfängern[12], an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern[14]

a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)

Empfängerkategorien (aus 4.a.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
Banken		
Rechtsvertreter im Geschäftsfall		
Wirtschaftstreuhänder		
Gerichte		
Verwaltungsbehörden		
Inkassounternehmen		
Fremdfinanzierer (zB Leasing)		
mitwirkende Vertrags- und Geschäftspartner	Kanada	
Versicherungen um Anlassfall		
Provider (IT-Dienstleister)		

b. Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt)**:**[13]

Für Kanada gibt es einen Angemessenheitsbeschluss der Europäischen Kommission.

[12] Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren.
[13] Siehe dazu das Merkblatt „Internationaler Datenverkehr“.

C. Detailangaben zu (2) Personalverwaltung

usw.

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

(HINWEIS: die hier angeführten Maßnahmen verstehen sich als beispielhafte Auflistung; es ist je nach Einzelfall und Risikobehaftung der Datenverarbeitung zu entscheiden, welche konkreten Maßnahmen zu treffen sind und welche im Einzelfall auch zumutbar sind)

a. Vertraulichkeit:

i. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, zB: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;

ii. Zugangskontrolle: Schutz vor unbefugter Systembenutzung, zB: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

iii. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, zB: Protokollierung von Zugriffen; oder: Zugriff nur für Unternehmensinhaber, Mitarbeiter der Abteilung Rechnungswesen und Mitarbeiter, die an der Geschäftsabwicklung beteiligt sind

b. Integrität:

i. Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, zB: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

ii. Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, zB: Protokollierung, Dokumentenmanagement;

c. Verfügbarkeit und Belastbarkeit:

i. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, zB: Backup-Strategie, Virenschutz, Firewall;

d. Pseudonymisierung und Verschlüsselung:

i. Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

ii. Verschlüsselung: sofern für die jeweilige Datenverarbeitung möglich, werden folgende Verschlüsselungstechnologien eingesetzt: ….

e. Evaluierungsmaßnahmen:

i. Datenschutz-Management (zB Risikoanalyse, Datenschutz-Folgenabschätzung), einschließlich regelmäßiger Mitarbeiter-Schulungen;

Stand: August 2017

Dieses Merkblatt ist ein **Produkt der Zusammenarbeit aller Wirtschaftskammern**.
Bei Fragen wenden Sie sich bitte an die Wirtschaftskammer Ihres Bundeslandes:
Burgenland, Tel. Nr.: 05 90907, Kärnten, Tel. Nr.: 05 90904, Niederösterreich Tel. Nr.: (02742) 851-0,
Oberösterreich, Tel. Nr.: 05 90909, Salzburg, Tel. Nr.: (0662) 8888-0, Steiermark, Tel. Nr.: (0316) 601-0,
Tirol, Tel. Nr.: 05 90905-1111, Vorarlberg, Tel. Nr.: (05522) 305-0, Wien, Tel. Nr.: (01) 51450-1615,
Hinweis! Diese Information finden Sie auch im Internet unter http://wko.at/datenschutz. Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr. Eine Haftung der Wirtschaftskammern Österreichs ist ausgeschlossen. Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter!