leitnerleitner

leitnerleitner
wirtschaftsprüfer steuerberater

WKO DER HANDEL

D_04a WKO Verfahrensverzeichnis

Im Rahmen der DSGVO wird der Unternehmer verpflichtet ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Eine Verarbeitungstätigkeit kann als ein Sammelsurium von Verarbeitungsprozessen gesehen werden.

Art 30 DSGVO

Es folgt eine Übersicht von wesentlichen Verfahrenstätigkeiten einfach strukturierter Einzelhändler, wobei jene Tätigkeiten ohne farblicher Hinterlegung als optional gesehen werden können und die Beurteilung der Relevanz der Tätigkeiten im Einzelfall zu erfolgen hat. Die optional angeführten Tätigkeiten stellen jedenfalls keine abschließende Auflistung dar.

Im Rahmen der einzelnen Tätigkeiten wurden bereits einzelne Verarbeitungsprozesse definiert, welche jedenfalls einer individuellen Ergänzung bedürfen.

Rechnungswesen und Geschäftsführung
VT01 (SA001)
- Buchhaltung bzw Einnahmen-Ausgaben-Rechnung
- Verarbeitungen im Rahmen des Steuerrechts bzw Übermittlungen an Steuerberater und Finanzamt
- UVAs
- Kostenrechnung
- Verwaltung der Bankkonten bei Kreditinstituten (Zahlungsverkehr)
- Auflagen iZm Registrierkassen
- Ausgangs- und Eingangsrechnungen (Einkauf / Verkauf)
- Miet- und Leasingverträge
- Versicherungen
- Lagerverwaltung (incl Inventurunterlagen)
- ....

Personalverwaltung
VT02 (SA002)
- Personalverwaltung von bestehenden Dienstverhältnissen
- Verwaltung von Bewerbungen bzw Stellenausschreibungen
- Zeiterfassungssysteme
- Zutrittssysteme (Schlüssel- u Chipsysteme)
- Krankmeldungen
- Kündigungen
- An/Abmeldung Krankenkasse
- Personalverrechnung incl Pfändung
- Gehaltszahlungen
- Dienstverträge
- Stellenausschreibungen
- Arbeitsplatzbeschreibungen
- ....

Marketing
VT03 (SA022)
- Außenauftritt
- Werbung
- Newsletter Systene
- Homepages
- Gewinnspiele und Preisausschreiben

Akten- und Datenverwaltung (IT)
VT04
- Nur bei größeren (Papier)Archiven und/oder etwaiger komplexerer IT-Strukturen notwendig. Ansonten kann diese Verarbeitungstätigkeit "aufgelöst" und die einzelnen Vorgänge anderen Bereichen zugeordnet werden.
- Papierarchiv
- Redundante RAID-Systeme (Server)
- Sicherungssysteme
- Ausfall- und Backupsysteme

Videoüberwachung
VT05
- Separat aufgrund hohem Risiko

Userverwaltung
VT06 (SA007)
- Elektronische Userverwaltung - nur relevant sofern mehere Systemzugänge (bzw Logindaten) mehrerer Personen verwaltet werden (Active Directory, USP, Finanzonline,...)

mögliche weitere Tätigkeiten
...

Verantwortliche Person:
Im Rahmen der einzelnen Verfahrenstätigkeiten bedarf es der Bestimmung eines Verantwortlichen je Tätigkeit. Aus Gründen der Praktikabilität kann dies jedoch gesammelt für alle Tätigkeiten erfolgen:

Art 30 lit a DSGVO

Max Mustermann
Musterstraße 30
4020 Musterhausen
Tel +43 7233 xxxx
Email max.mustermann@mustermann.at

Zur Info: "Warum finde ich keinen Prozess zum Thema Emails?"
Emails werden nicht als eigener Prozess geführt, da es sich dabei um ein Kommunikationsmedium handelt, welches als Hilfsmittel zur Durchführung der einzelnen Prozesse zu sehen ist.

Technische und organisatorische Maßnahmen:
Siehe entsprechende Beilage.

Änderungsprotokoll:
Das Verzeichnis bedarf einer regelmäßigen Aktualisierung. Eine entsprechende Dokumentation der Änderungen ist notwendig.

leitnerleitner
leitnerleitner
wirtschaftsprüfer steuerberater

WKO DER HANDEL

WKO Risiko und Folgenabschätzung

Für **jede** Verfahrenstätigkeit ist abzuschätzen, ob diese ein Risiko für die Rechte anderer bergen könnte. Sollte man in Zuge dieser Abschätzung zu einem hohen Risiko gelangen, so ist eine weitergehende Beurteilung im Sinne einer Folgenabschätzung notwendig. Achten sie dabei unbedingt auf eine ausreichende Dokumentation (Etwaige Ergänzungen dieses Dokuments). Sofern Auftragsverarbeiter einbezogen werden, sind diese in die Beurteilung entsprechend einzubeziehen.

Zur Info:
Grundsätzlich sollte die Behörde sogenannte "White" und "Black"-Listen veröffentlichen, welche verschiedene Tätigkeiten von der Folgenabschätzung ausschließt bzw eine verpflichtende Folgenabschätzung anordnet. Aktuell liegen diese jedoch noch nicht auf.

Im Rahmen der vordefinierten wesentlichen (farblich hinterlegten) Tätigkeiten kann bei einem gewissen Maß an ordentlicher Sorgfalt ein tendenziell eher niedriges Risiko angenommen werden, wobei jedenfalls eine Beurteilung im Einzelfall zu erfolgen hat.

Welche Indikatoren können dabei zur Beurteilung herangezogen werden, ob ein Risiko vorliegt:

	ja	nein
¬ Einsatz von Cloud Services		
¬ Einsatz von individuellen Softwarelösungen		
¬ Werden Daten in hohem Umfang verarbeitet		
¬ Verarbeitung von Daten schutzbedürftiger Personen (zB Kinder)		
¬ Entsteht die Gefahr von Identitätsdiebstahl oder -betrug		
¬ Existieren keine wirksamen Schutzmechanismen vor unbefugtem Zugriff (Verschließbare Räume, Firewalls, Passwortschutz, …)		
¬ Drohen erhebliche Schäden durch Verlust der Vertraulichkeit		
¬ Besitzen zugriffsberechtigte Personen keine angemessenen Kenntnisse im Bereich des Datenschutzes		
¬ …		

Sollten Sie die überwiegende Anzahl der Fragen mit "Ja" beantwortet haben, **könnte** für die entsprechende Verarbeitungstätigkeit eine **Folgenabschätzung notwendig sein.**

Bei den folgenden Verarbeitungstätigkeiten ist man **jedenfalls** zu einer Folgenabschätzung verpflichtet:

	ja	nein
¬ Automatisierte Analyse und Bewertung persönlicher Aspekte von Personen		
¬ Verarbeitung von Daten mit strafrechtlichem Bezug (in erhöhtem Umfang)		
¬ Umfangreiche Verarbeitung Daten besonderer Kategorie		
¬ Überwachung von öffentlichen Bereichen (Videokameras, …)		

Art 35 DSGVO

Eine Folgenabschätzung sowie eine Abschätzung der Notwendigkeit im Zweifelsfall bedarf tiefergehender Kenntnisse im Bereich des Datenschutzes und sollte daher jedenfalls in Abstimmung mit fachkundigen Dritten erfolgen.

Die oben durchgeführten Einschätzungen beziehen sich auf folgende Verarbeitungstätigkeiten und ergaben die Notwendigkeit einer Folgenabschätzung:

		ja	nein
¬ VT01 (SA001)	Rechnungswesen und Geschäftsführung		
¬ VT02 (SA002)	Personalverwaltung		
¬ VT03 (SA022)	Marketing		

Rechnungswesen und Geschäftsführung
VT01 (SA001)
- Buchhaltung bzw Einnahmen-Ausgaben-Rechnung
- Verarbeitungen im Rahmen des Steuerrechts bzw Übermittlungen an Steuerberater und Finanzamt
- UVAs
- Kostenrechnung
- Verwaltung der Bankkonten bei Kreditinstituten (Zahlungsverkehr)
- Auflagen iZm Registrierkassen
- Ausgangs- und Eingangsrechnungen (Einkauf / Verkauf)
- Miet- und Leasingverträge
- Versicherungen
- Lagerverwaltung (incl Inventurunterlagen)
- ....

Zweck:
- ¬ Verarbeitung von Daten im Rahmen der unternehmens- und steuerrechtlichen Dokumentationspflichten
- ¬ Vertragsverwaltung (Bestandsverträge, Einkauf / Verkauf)
- ¬ Durchführung des Zahlungsverkehrs
- ¬ Führen des täglichen Geschäftsverkehrs

Löschfrist/Höchstdauer:
Bis zur Beendigung der Geschäftsbeziehung oder bis zum Ablauf der für den Auftraggeber geltenden Garantie-, Gewährleistungs-, Verjährungs- und gesetzlichen Aufbewahrungsfristen; darüber hinaus bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden.

Übermittlungsempfänger:
1 Banken zur Abwicklung des Zahlungsverkehrs
2 Rechtsvertreter im Geschäftsfall
3 Wirtschaftsprüfer und Steuerberater
4 Gerichte
5 Zuständige Verwaltungsbehörden, insb. Finanzbehörden
6 Inkassounternehmen zur Schuldeneintreibung (ins Ausland daher nur, soweit die Schuld im Ausland eingetrieben werden muss)
7 Fremdfinanzierer wie Leasing- oder Factoringunternehmen und Zessionare, sofern die Lieferung oder Leistung auf diese Weise fremdfinanziert ist
8 Vertrags- oder Geschäftspartner, die an der Lieferung oder Leistung mitwirken bzw. mitwirken sollen
9 Versicherungen aus Anlass des Abschlusses eines Versicherungsvertrages über die Lieferung/Leistung oder des Eintritts des Versicherungsfalles
10 Bundesanstalt „Statistik Österreich“ für die Erstellung der gesetzlich vorgeschriebenen (amtlichen) Statistiken
11 Konzernleitung des Auftraggebers, bei Lieferanten sowie gewerblichen Kunden und Großkunden
12 Kunden (Empfänger von Leistungen)

Übermittlung in Drittländer (Nicht-EU-Länder) | ja | nein |
Wenn ja, welche:

Kategorien betroffener Personen:
1 Kunden
2 Lieferanten
3 Mitarbeiter
4 An der Geschäftsabwicklung mitwirkende Dritte

Kategorien personenbezogener Daten:
1 Stamm- und Kontaktdaten (Ordnungsnummer, Name, Anrede/Geschlecht/Titel, Geburtsdaten, Staatsbürgerschaft,…)
2 Vertragsdaten (Ausweiskopie, Zahlungs- und Leistungsverhalten, Ursprungsland, UID, Vertretungsbefugnisse und Kontaktpersonen,…)
3 Verrechnungs- und Zahlungsdaten (Bankverbindung , Zahlungsbedingungen, Bonität, Sperrkennzeichen, Kreditinformationen,…)
4 Registerauszüge (Firmenbuch, Wirtschaftliches Eigentümerregister, Erhebungen Geldwäsche,…)
5 Korrespondenz

Anwendung Profiling | ja | nein |
Bewerten, Analysieren bzw Vorhersagen von personenbezogenen Daten (zb personalisierte Onlinewerbung)

Zur Info:
Sollten sie weitere Datenkategorien im Rahmen Ihres Unternehmen identifizieren, bedarf es einer entsprechenden Ergänzung. Außerdem sollte besonderer Augenmerk auf Daten besonderer Kategorie (wie Religionsdaten, Gesundheitsdaten, Gewerkschafts- bzw politische Zugehörigkeit, Rassische oder ethnische Herkunft, Genetische oder biometrische Daten, Sexuelle Orientierung) gelegt werden, da für diese ein besonders strenger Rahmen gilt.

Art 9 DSGVO

Personalverwaltung
VT02 (SA002)

- Personalverwaltung von bestehenden Dienstverhältnissen
- Verwaltung von Bewerbungen bzw Stellenausschreibungen
- Zeiterfassungssysteme
- Zutrittssysteme (Schlüssel- u Chipsysteme)
- Krankmeldungen
- Kündigungen
- An/Abmeldung Krankenkasse
- Personalverrechnung incl Pfändung
- Gehaltszahlungen
- Dienstverträge
- Stellenausschreibungen
- Arbeitsplatzbeschreibungen

Zweck:
- ¬ Personalverrechnung und Erfüllung von gesetzlichen Dokumentations- und Melde bzw Auskunftspflichten
- ¬ Personalverwaltung (insb hinsichtlich Bereitschaft, Dienstpläne und Vertragsverwaltung)
- ¬ Bewerbermanagement von laufenden Bewerbungen und in Abstimmung mit dem Bewerber in Evidenz gehaltene Bewerbungen

Löschfrist/Höchstdauer:
Bis zur Beendigung der Beziehung mit dem Betroffenen und darüber hinaus solange als gesetzliche Aufbewahrungsfristen bestehen oder solange Rechtsansprüche aus dem Arbeitsverhältnis gegenüber dem Arbeitgeber geltend gemacht werden können.

Übermittlungsempfänger:
1 Banken
2 Rechtsverkehr im Geschäftsfall
3 Wirtschaftsprüfer und Steuerberater
4 Gerichte
5 Verwaltungs- und Finanzbehörden
6 Inkassounternehmen
7 Vertrags- oder Geschäftspartner sofern direkte Mitwirkung
8 Versicherungen
9 Externe Veranstalter für Events und Fortbildungen
10 Vorsorge- und Krankenkassen
11 AMS
12 gesetzliche Interessensvertretung

Übermittlung in Drittländer (Nicht-EU-Länder) — ja / nein
Wenn ja, welche:

Kategorien betroffener Personen:
1 Mitarbeiter (Unabhängig von der Art der Anstellung: freier DN, Angestellter, Arbeiter, …)
2 Bewerber und Interessenten
3 Kunden und Lieferanten
4 An der Geschäftsabwicklung mitwirkende Dritte (zb Personalvermittler)

Kategorien personenbezogener Daten:
1 Stamm- und Kontaktdaten (Ordnungsnummer, Name, Anrede/Geschlecht/Titel, Geburtsdaten, Staatsbürgerschaft,…)
2 Vertragsdaten (Personalnummer, Ausweiskopie, Notfallkontaktperson, Sozialversicherungsnummer, Informationen zum Thema Schwangerschaft,…)
3 Verrechnungs- und Zahlungsdaten (Bankverbindung, Lohnpfändungen, Arbeitnehmerveranlagung, Krankenstände,…)
4 Bewerberdaten (siehe Info, im Rahmen der Bewerbung übermittelte Informationen wie Zeugnisse, …)
5 Korrespondenz

Anwendung Profiling — ja / nein
Bewerten, Analysieren bzw Vorhersagen von personenbezogenen Daten (zb personalisierte Onlinewerbung)

Zur Info:
Sollten sie weitere Datenkategorien im Rahmen Ihres Unternehmen identifizieren, bedarf es einer entsprechenden Ergänzung. Außerdem sollte besonderer Augenmerk auf Daten besonderer Kategorie (wie Religionsdaten, Gesundheitsdaten, Gewerkschafts- bzw politische Zugehörigkeit, Rassische oder ethnische Herkunft, Genetische oder biometrische Daten, Sexuelle Orientierung) gelegt werden, da für diese ein besonders strenger Rahmen gilt. Art 9 DSGVO
Insbesondere im Bereich der Bewerberdaten kommt es regelmäßig zur Übermittlung von Religiösen Bekenntnissen oder Gesundheitsdaten. Hier kann man sich die Frage stellen, ob man hier im Sinne der Datenminimierung nicht auf eine entsprechende Verarbeitung verzichten kann.

Marketing
VT03 (SA022)

- Außenauftritt
- Werbung
- Newsletter Systene
- Homepages
- Gewinnspiele und Preisausschreiben

Zweck:

¬ Verwendung von Kunden- und Interessentendaten für die Geschäftsanbahnung im Rahmen der eigenen Geschäftstätigkeiten

Löschfrist/Höchstdauer:

Bis Ablauf der im Rahmen der Erhebung definierten Frist bzw bis Widerruf durch den Betroffenen.

Übermittlungsempfänger:

1 Werbeunternehmen
2 Online-Tracking-Anbieter
3 Event-Veranstalter
4 Hoster für Onlineplattformen (Homepage, Webshop,…)

Übermittlung in Drittländer (Nicht-EU-Länder)

ja	nein

Wenn ja, welche:

Kategorien betroffener Personen:

1 Interessenten (Dritte)
2 Kunden und Lieferanten
3 Besucher von Website bzw Webshop

Kategorien personenbezogener Daten:

1 Stamm- und Kontaktdaten (Ordnungsnummer, Name, Anrede/Geschlecht/Titel, Geburtsdaten,…)
2 Nutzungsdaten Online-Angebot (IP, Verweildauer, Klick-Statistiken, Herkunft IP, Browserinformationen,…)
3 Korrespondenz

Anwendung Profiling

ja	nein

Bewerten, Analysieren bzw Vorhersagen von personenbezogenen Daten (zb personalisierte Onlinewerbung)

Zur Info:

Sollten sie weitere Datenkategorien im Rahmen Ihres Unternehmen identifizieren, bedarf es einer entsprechenden Ergänzung. Außerdem sollte besonderer Augenmerk auf Daten besonderer Kategorie (wie Religionsdaten, Gesundheitsdaten, Gewerkschafts- bzw politische Zugehörigkeit, Rassische oder ethnische Herkunft, Genetische oder biometrische Daten, Sexuelle Orientierung) gelegt werden, da für diese ein besonders strenger Rahmen gilt. Art 9 DSGVO

Im Rahmen der Verwendung von Tracking-Tools wie zB Google Analytics sollte man in Abstimmung mit dem Anbieter den Tatbestand des Profilings näher beleuchten.