emig
Datenverarbeitung GmbH

... wirtschaftliche IT-Lösungen

Datenschutzgrundverordnung - DSGVO

Was braucht ein Unternehmen,
um auf der (rechts-)sicheren Seite zu sein?

Haftungsausschluss

Die vorliegende Unterlage stellt lediglich einen Überblick über das vorgetragene Thema dar.

Sie erhebt keinen Anspruch auf Vollständigkeit, gibt teilweise die Meinung der Autoren wieder und kann keinesfalls die Beratung im Einzelfall und die Konsultation diverser Berater (Rechtsanwälte, Steuerberater, sonstige Berater) ersetzen.

Der Inhalt wurde unter größtmöglicher Sorgfalt erstellt, ist jedoch ohne Gewähr.

Eine Haftung aus der vorliegenden Unterlage ist ausgeschlossen.

Allgemeines

Warum Datenschutz?

- ✓ Man gebe mir sechs Zeilen, geschrieben von dem redlichsten Menschen, und ich werde darin etwas finden, um ihn aufhängen zu lassen ... (Kardinal Richelieu 1585-1642)

Wie hat sich die DSGVO entwickelt?

- ✓ 1995 - 1. Richtlinie -> 28 Datenschutzgesetze
- ✓ 2016 - 1. Verordnung -> 1 Datenschutzgesetz

Wie hat sich die DSGVO entwickelt?

- ✓ 04. Mai 2016 Amtsblatt der EU veröffentlicht
- ✓ 25. Mai 2016 DSGVO ist in Kraft getreten
- ✓ **25. Mai 2018** DSGVO ist anwendbar

Welche Daten sind erfasst?

- **Personenbezogene Daten natürlicher Personen**
  - Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
  - zB Name, Kontaktdaten, Kleidergröße, Einkommen, SV-Nr, Charaktereigenschaften etc

- **Sensible Daten**
  - Rassistische und ethnische Herkunft
  - Politische Meinungen
  - Religiöse oder weltenanschauliche Überzeugungen
  - Gewerkschaftszugehörigkeit
  - Genetische oder biometrische Daten
  - Gesundheitsdaten
  - Sexuelle Orientierung

Was ist Datenverarbeitung?

- ✓ Verarbeitung als weitgefasster Begriff
  - ✓ Erheben / Erfassen
  - ✓ Speicherung
  - ✓ Verwendung
  - ✓ Weitergabe / Verbreitung
  - ✓ Löschen / Vernichtung etc

  → zB Erstellung einer Kundendatei, Datenaufnahme zur Erstellung einer Rechnung, Mitarbeiterdatenbank

- ✓ Verarbeitung im Rahmen der Tätigkeit einer Niederlassung in der EU
- ✓ Verarbeitung findet **überall** statt (zB Cloud)

Rechtfertigungsgründe für Datenverarbeitung

- ✓ Erfüllung eines **Vertrages**
- ✓ **Gesetzliche** Verpflichtungen (BAO, etc…)
- ✓ **Berechtigte Interessen** des Verantwortlichen
- ✓ **Einwilligung**

Datenverarbeitung im Geschäftsleben
Beispiel Mitarbeiter

Natürliche oder juristische Person, die über Zwecke und Mittel der Datenverarbeitung entscheidet und für entstandene Schäden haftet

Verantwortlicher

Interesse an Informationen

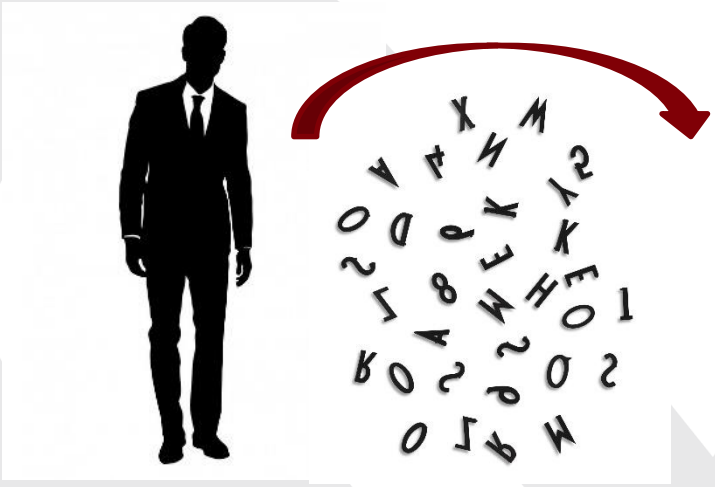
Natürliche Person, deren Daten verarbeitet werden

Betroffener

Interesse an Datenschutz

Personen & Interessen im Geschäftsleben

Verantwortlicher: IT-DL



Auftragsverarbeiter

Betroffener: Kunde

Datenschutzrechtliche Grundsätze I

- **Rechtmäßigkeit**
  - Darf ich Daten überhaupt verarbeiten?
  - Einwilligung, Erfüllung einer vertraglichen Verpflichtung, Wahrung berechtigter Interessen des Verantwortlichen, Erfüllung einer Rechtsvorschrift?
- **Transparenz**
  - Kunde muss wissen, was mit seinen Daten passiert
- **Zweckbindung**
  - Aufnahme der Daten des Mitarbeiters im Dienstvertrag → wofür? (Vertragszweck!)
  - Weiterverarbeitung (Alumniveranstaltung?)

Datenschutzrechtliche Grundsätze II

- **Richtigkeit**
  - Sind die Daten des Kunden/Mitarbeiters richtig und aktuell?

- **Verhältnismäßigkeit**
  - Datenverarbeitung zur Verwirklichung eines legitimen Zwecks?
  - Datenverarbeitung als mildestes Mittel?
  - Interessenabwägung: Recht auf Information vs Recht auf Datenschutz

Datenschutzrechtliche Grundsätze III

- **Koppelungsverbot**
  - Kundenkarte für Prozente?
- **Datenminimierung**
  - Welche Daten brauche ich wirklich? (SV-Nr?!)
- **Speicherbegrenzung**
  - Wie lange darf ich Daten des Kunden/Mitarbeiters speichern?
  - Beschränkung auf das unbedingt erforderliche Mindestmaß
  - Generelle Speicherfrist von 7 Jahren (Aufbewahrungsfrist nach § 132 BAO)
  - Gewährleistung / Schadenersatz: 3 – maximal 30 Jahre

Datenschutzrechtliche Grundsätze IV

- ✓ **Integrität** und **Vertraulichkeit**
  - ✓ Wer kann intern auf die Daten zugreifen?
    - → Geeignete technische und organisatorische Maßnahmen

- ✓ **Rechenschaftspflicht**
  - ✓ Unternehmen muss Grundsätze einhalten und Nachweis darüber führen - Verfahrensverzeichnis

- ✓ Recht auf **"Vergessenwerden"**

Wer haftet?

Verantwortlicher

- Geschäftsführung?
- Vorstand ?

Auftragsverarbeiter

Keine Entlastung durch Bestellung eines Datenschutzbeauftragten

Haftung des IT-DL für datenschutzrechtliche Verfehlungen des Kunden

Verzeichnis von Verarbeitungstätigkeiten

- ✓ Das Verzeichnis von Verarbeitungstätigkeiten ersetzt ab 25.5.2018 die Meldepflicht iSd §§ 17ff DSG 2000 (https://dvr.dsb.gv.at/at.gv.bka.dvr.public/DVRRecherche.aspx)
- ✓ Die bis dato meldepflichtigen Informationen entsprechen zu einem Gutteil jenen Informationen, die auch im Verfahrensverzeichnis zu führen sind
- ✓ Die Verantwortliche (Ihr Unternehmen) und der Auftragsverarbeiter (zB etwaige Dienstleister) haben ein Verzeichnis der Verarbeitungstätigkeiten zu führen, die beinhaltet u.a.:
  - ✓ Beschreibung des Zwecks der Datenverarbeitung
  - ✓ Beschreibung der Betroffenen und der verwendeten Datenarten
  - ✓ Datenempfänger, Dienstleister und die vertragliche Grundlage sowie die Dokumentation der geeigneten Garantien (Standardvertragsklauseln)
  - ✓ Löschfristen und Speicherdauer
  - ✓ Getroffene Datensicherheitsmaßnahmen

Detailerhebung

Detailerhebung		
Angaben zur Verarbeitung		
Verarbeitung		
Lfd. Nr.		
Zweck der Verarbeitung		
Erhebungsdetails		
Auskunftspersonen	**Name der Auskunftspersonen im Inteview**	**Abteilung, Funktion**
Prüfung der Verarbeitung		
Datum der letzten Prüfung		
Datum der aktuellen Prüfung		
Datum der nächsten Prüfung		
Risikoabschätzung		
Datenschutz-Folgenabschätzung		
Risikoklassifikation		
Datenschutzklasse		
Verarbeitungsklasse		
Erlaubnistatbestände		
Rechtgrundlage der Verarbeitung		
besondere Kategorien personenbezogener Daten		
Zweckbindung		
Datenminimierung		
Richtigkeit		
Speicherbegrenzung		
Integrität und Vertraulichkeit		
Auftragsgebundenheit		
Zuständigkeiten, Verantwortung	**zuständige Rolle/Person/Abteilung**	**Name**
fachlich verantwortlich		
technisch zuständig		

Technische und Organisatorische Massnahmen - TOM

- ✓ Zutrittskontrollen: Schlüssel, Alarmanlage,…
- ✓ Zugangskontrolle: Kennwörter, Verschlüsselungen,…
- ✓ Zugriffskontrolle: Berechtigungen
- ✓ Weitergabekontrolle: Verschlüsselungen, …
- ✓ Eingabekontrolle: Protokolle,…
- ✓ Verfügbarkeitskontrolle: Virenschutz, Firewall,…
- ✓ Evaluierungsmassnahmen: Mitarbeiterschulungen, Datenschutzmanagement,….
- ✓ …

Data Breach – Was tun bei Datenpannen?

= *Verlust der vollständigen Kontrolle über die Daten und auch darüber, was mit diesen Daten passiert*

- ✓ Physischer, materieller oder immaterieller **Schaden** des Betroffenen
- ✓ Datenverlust durch **ungewollte** Panne oder grobe Fahrlässigkeit
  - ✓ zB aufgrund Softwarefehler sind Daten für andere Nutzer sichtbar; Versenden eines E-Mails mit Sichtbarkeit aller Empfänger; fehlender Passwortschutz; E-Mail aufgrund Namensähnlichkeit an falschen Empfänger
- ✓ **Vorsätzlich** herbeigeführte Datenpanne
  - ✓ zB Hacking, unzulässige Datenweitergabe

Was tun bei einer Datenpanne?

Sanktionen: Geldbuße

- ✓ Bis zu **€ 10 Mio** oder 2% des weltweiten Konzernjahresumsatzes
  - ✓ Unterlassene Datenschutzfolgenabschätzung
  - ✓ Keine Bestellung eines Datenschutzbeauftragten trotz Verpflichtung

- ✓ Bis zu **€ 20 Mio** oder 4% des weltweiten Konzernjahresumsatzes
  - ✓ Verstoß gegen Grundsätze der Verarbeitung
  - ✓ Verstoß gegen Voraussetzungen der Einwilligungserklärung
  - ✓ Verstoß gegen die Informationspflicht

Abschließende Tipps

- ✓ Erstellung datenschutzrelevanter **Richtlinien**
- ✓ Interne **Schulungen** und **Schulungen der Kunden**
- ✓ Durchführung von **Audits**
- ✓ **Schnelle Reaktion** auf Zwischenfälle
- ✓ **Bearbeitung von Anfragen** von Betroffenen
- ✓ **Weiterführende Unterlagen der WKO**
  - ✓ https://www.wko.at/branchen/handel/datenschutzgrundverordnung-in-handelsunternehmen.html

mesonic
mit sicherheit ein gewinn

Das neue Modul WinLine DSGVO

WinLine DSGVO

- ✓ Prozess- & Dokumentenmanagementsystem (PDMS)
  - ✓ Aufbau, Verwaltung und Revisionierung von Verarbeitungsverzeichnissen
- ✓ Einwilligungsverwaltung
  - ✓ Opt-in/Opt-out Verwaltung
- ✓ Auskunftstool
  - ✓ Automatische Zusammenfassung von Dateninformationen
- ✓ Anonymisierungstool
  - ✓ Zusammenfassung auf Sammelkonten

WinLine PDMS

WinLine PDMS

- ✓ Dokumentation technisch-organisatorischer Maßnahmen
- ✓ Aufbau, Verwaltung und Revisionierung von Verarbeitungsverzeichnissen
- ✓ Automatische Verteilung von Mitarbeiteranweisungen
- ✓ Dokumentation und Nachvollziehbarkeit der unternehmensinternen Verteilung
- ✓ Einfache Nachweismöglichkeit gegenüber Behörden

WinLine PDMS

- ✓ Winline DSGVO – Prozess und Dokumentenmanagementsystem (PDMS) inkl. WinLine mobile light Benutzer

WinLine PDMS

- ✓ Wie können Sie dieses Modul über die DSGVO hinaus in ihrem Unternehmen nutzen?

WinLine PDMS

- ✓ Arbeitsplatzevaluierung
- ✓ Arbeitsanweisungen
- ✓ Brandschutzmaßnahmen
- ✓ Mitarbeiter Handbücher
- ✓ Ö-NORMen
- ✓ ISO-Zertifizierung
- ✓ etc.

Einwilligungsverwaltung

Einwilligungsverwaltung

- ✓ Verwaltung von Einwilligungserklärungen zur Verarbeitung personenbezogener Daten, insbesondere im Bereich des E-Mail Marketings
  - ✓ Personenkonten
  - ✓ Interessenten
  - ✓ Kontakte
- ✓ Einwilligungs-, Änderungs- und Widerrufsverwaltung (Opt-in/Opt-out)
- ✓ Protokollierung der Einwilligungsart
- ✓ Historie der Einwilligungserteilung

Einwilligungsverwaltung

- ✓ WinLine DSGVO – Einwilligungsverwaltung

Auskunftstool

Auskunftstool

- ✓ Automatische Zusammenfassung von Dateninformationen
- ✓ Ausgabe der gesammelten Informationen im PDF-Format auf Knopfdruck
- ✓ Erfüllung der Auskunftspflicht gegenüber Betroffenen

Auskunftstool

- ✓ WinLine DSGVO – Auskunftstool

Anonymisierungstool

Anonymisierungstool

- ✓ Anonymisierung personenbezogener Daten (unterbundener Personenbezug)
- ✓ Rekonstruktion der Ursprungsdaten ausgeschlossen
- ✓ Bewegungsdaten für statistische Auswertungen weiterhin auch ohne Personenbezug verfügbar
- ✓ Umsetzung des Rechts auf Datenminimierung/-löschung

Anonymisierungstool

- ✓ WinLine DSGVO – Anonymisierungstool

Das neue Modul WinLine - DSGVO

Wir können Ihnen damit die Arbeit und Verantwortung zu diesem Thema zwar nicht abnehmen, aber enorm erleichtern.

WinLine DSGVO

Die 4 Säulen des neuen Moduls

- ✓ Einwilligungsverwaltung
  - ✓ Opt-in/Opt-out Verwaltung mit Historie
- ✓ Auskunftstool
  - ✓ Automatische Zusammenfassung von Dateninformationen
- ✓ Anonymisierungstool
  - ✓ Zusammenfassung auf Sammelkonten
- ✓ Prozess-& Dokumentenmanagementsystem (PDMS)
  - ✓ Aufbau, Verwaltung und Revisionierung von Verarbeitungsverzeichnissen

WinLine DSGVO – PDMS inkl. UKP

- ✓ Dokumentation technisch-organisatorischer Maßnahmen
- ✓ Aufbau, Verwaltung und Revisionierung von Verarbeitungsverzeichnissen
- ✓ Automatische Verteilung von Mitarbeiteranweisungen
- ✓ Dokumentation und Nachvollziehbarkeit der unternehmensinternen Verteilung
- ✓ Einfache Nachweismöglichkeit gegenüber Behörden

WinLine DSGVO – PDMS inkl. UKP

- ✓ Anwendungsmöglichkeiten des PDMS inkl. UKP
  - ✓ DSGVO – Verarbeitungsverzeichnisse
  - ✓ Arbeitsplatzevaluierung (Dokumentation)
  - ✓ Arbeitsanweisungen – Prozessbeschreibungen
  - ✓ Schulungsunterlagen
  - ✓ Interne Mitteilungen
  - ✓ ISO Zertifizierung
  - ✓ Verträge
  - ✓ …

WinLine DSGVO – PDMS inkl. UKP

- ✓ Anwendungsmöglichkeiten des WinLine mobile light Benutzers
  - ✓ Leseberechtigung und Lesebestätigung im PDMS
  - ✓ WinLine Share - Kommunikation
  - ✓ Urlaubsanträge
  - ✓ Krankmeldungen
  - ✓ Beschaffungsanträge
  - ✓ Zeiterfassung (Kommt/Geht)
  - ✓ …

WinLine DSGVO – Zielgruppe/Benefits

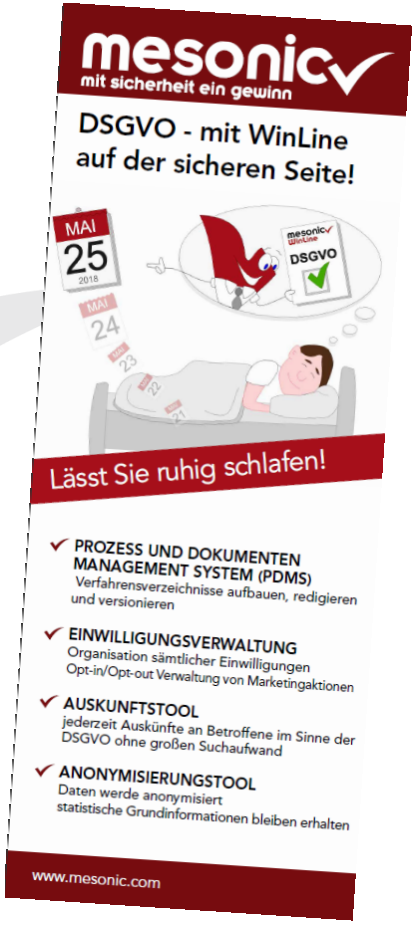
- ✓ Für Unternehmen jeder Größe
- ✓ Freie Wahl der Paketgröße
- ✓ Integration aller Mitarbeiter eines Unternehmens (PDMS, definierte Startschritte für Urlaub, Beschaffung, Zeiterfassung) – WinLine mobile light Benutzer
- ✓ PDMS deutlich weiter verwendbar als „nur" für die DSGVO
- ✓ Neben den must haves – enorme Administrationsvereinfachung durch PDMS und UKP
- ✓ Saubere und einfache Dokumentation gegenüber Behörde
- ✓ …

WinLine DSGVO - Preise

- ✓ Ab 990 Euro und 25 Euro monatlich
- ✓ Staffelung nach Arbeitnehmeranzahl
- ✓ Abwicklungstechnisch Kauf plus WV
  - ✓ Jährlich kündbar
  - ✓ Upgrade auf die nächst höhere Stufe möglich
- ✓ Nutzungsanteil des WinLine mobile light User ist in dem WV (monatl. Kosten)integriert
- ✓ 1 CRM User im WinLine DSGVO inkludiert
- ✓ Vollwertige CRM mobile User können PDMS inkl. UKP selbstverständlich nutzen

WinLine DSGVO

- ✓ Ab 990 Euro und 25 Euro monatlich
- ✓ Skalierbar
- ✓ DSGVO fit innerhalb der WinLine
- ✓ Weiterführende Funktionalitäten



- ✓ Weiterführende Unterlagen von der WKO

WinLine DSGVO - Preise

Staffelung nach Arbeitnehmern	Modul	WV inkl. Nutzung WinLine mobile light Benutzer pro Monat
bis 5 AN	990,00	25
bis 10 AN	1.500,00	39
bis 25 AN	2.100,00	60
bis 50 AN	2.900,00	95
bis 100 AN	3.800,00	139
bis 250 AN	4.850,00	199

mesonic
mit sicherheit ein gewinn

Vielen Dank!

Bis zum nächsten Mal!

info@mesonic.com **www.mesonic.com**