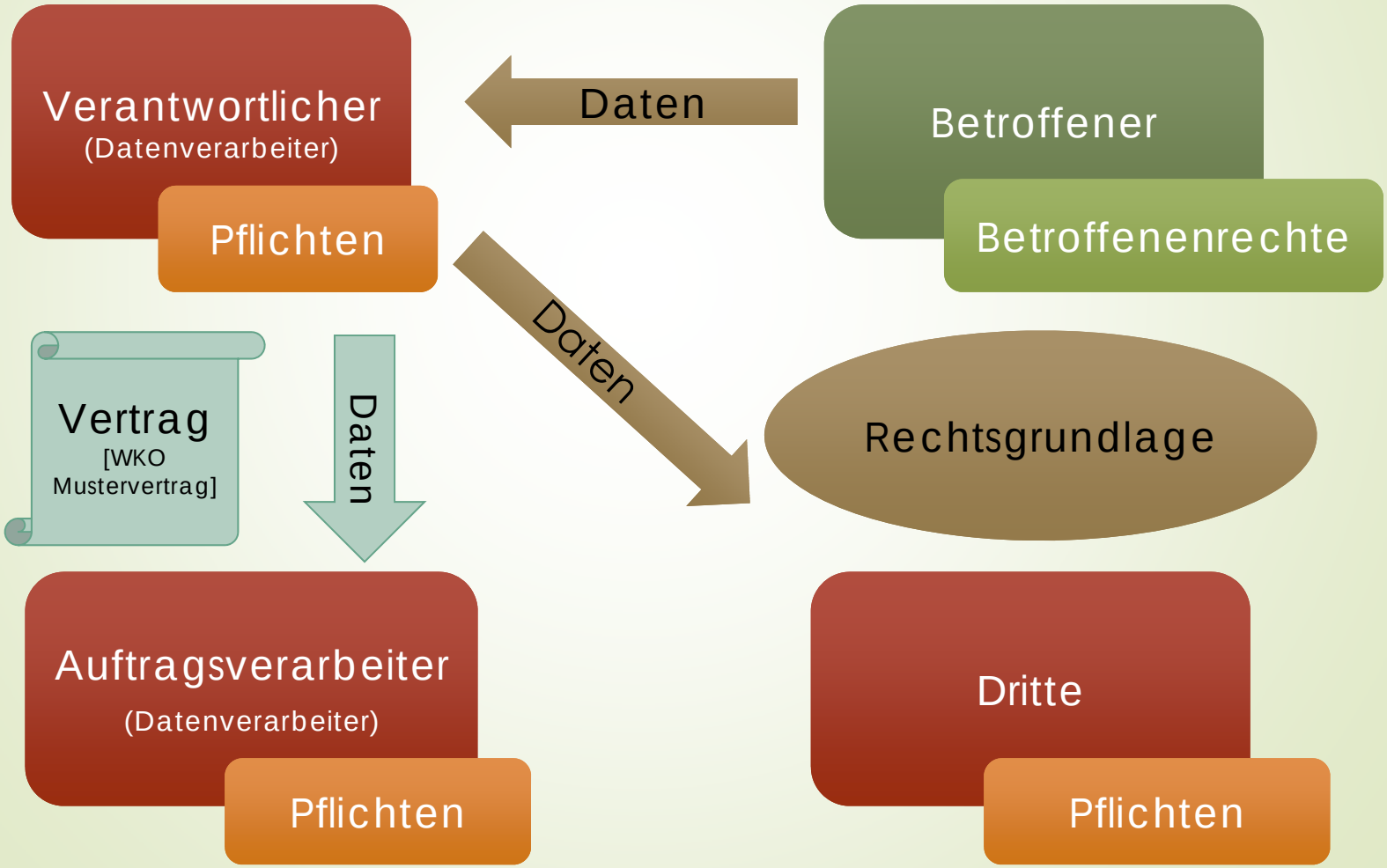
Datenschutz Grundverordnung (DSGVO)

- DATENSCHUTZ IST KEIN LUXUS, SONDERN PFLICHT

Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB17P0031
Valid:12/2020

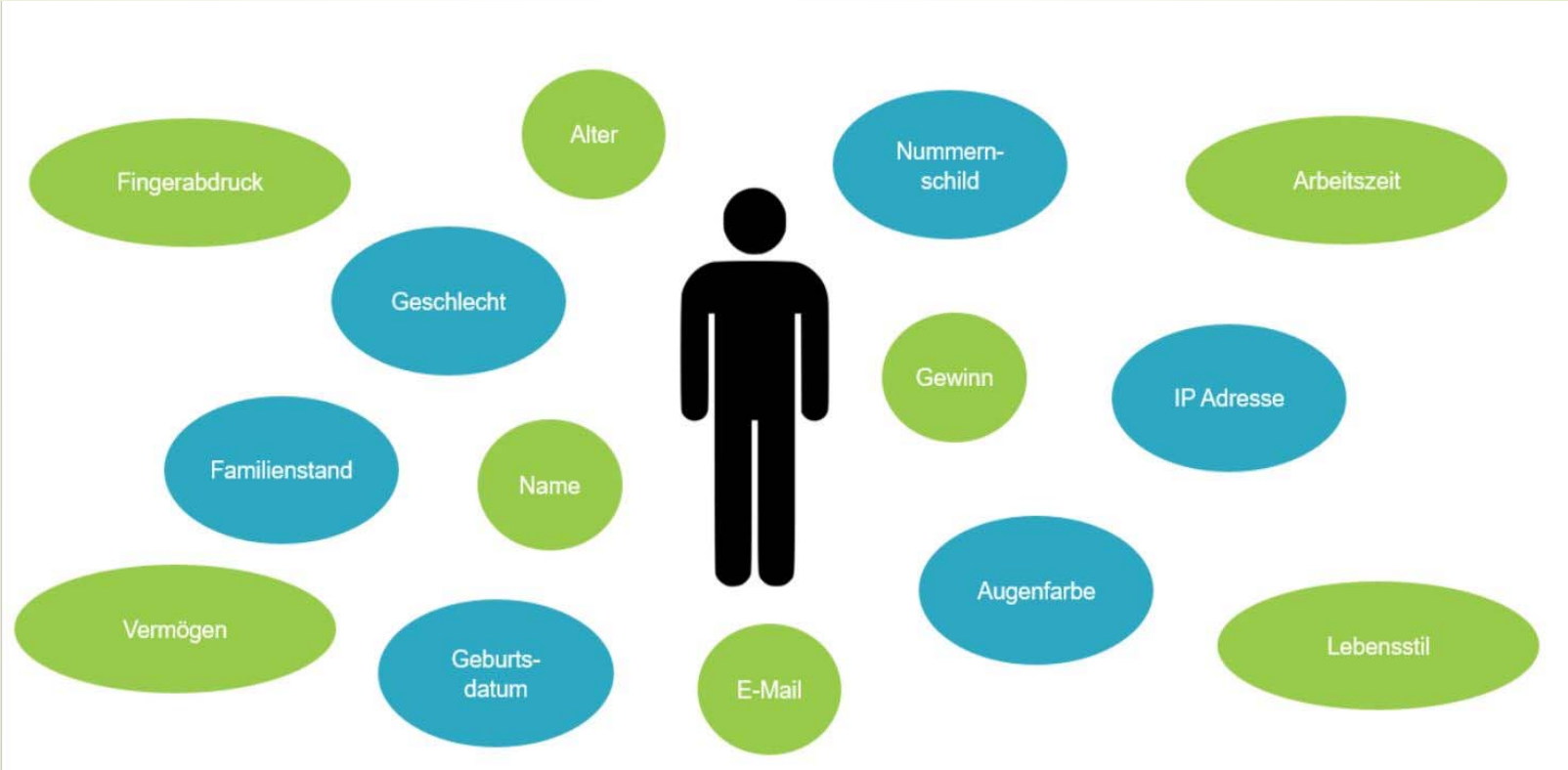
Pflichten des Verantwortlichen



Personenbezogene Daten

Definition

personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen;



Sensible Daten

Definition

- ✓ Rassische und ethnische Herkunft
- ✓ Politische Meinung
- ✓ Gewerkschaftszugehörigkeit
- ✓ Religiöse oder weltanschauliche Überzeugung
- ✓ Genetische und biometrische Daten
- ✓ Gesundheitsdaten zum Sexualleben oder der sexuellen Orientierung

Die wesentlichen Neuerungen

Pflichten des Verantwortlichen

Verzeichnis von Verarbeitungstätigkeiten

Das Verfahrensverzeichnis ist statt der DVR-Meldung

Export aus DVR ist bis Ende 2019 möglich

Risikobasierter Ansatz für TOM

Die **T**echnischen und/oder **O**rganisatorischen **M**aßnahmen zum Schutz der personenbezogenen Daten

Datenschutz-Folgenabschätzung

Wenn ein hohes Risiko für die Daten oder im hohem Maß sensible Daten oder Profiling Daten verarbeitet werden

Pflichten des Verantwortlichen

Koppelungsverbot

Für Einwilligungserklärung (Vorlage)

Datenschutzbeauftragten

wenn die Kerntätigkeit umfangreiche und systematische Überwachung Betroffener oder umfangreichen Verarbeitung sensibler Daten besteht

Datenschutz durch

Technik Privacy by Design und durch Voreinstellungen Privacy by Default

Datensicherungsmaßnahmen (technisch/organisatorisch)

Datensicherheit und Datenschutz

Informationspflicht

Bei Datenmissbrauch, Info an Betroffene und DSB binnen 72h (außer wenn keine Gefahr für Betroffene)

Pflichten des Verantwortlichen

Betroffenenrechte

Informationspflicht

- Auskunft binnen 1 Monat (**Neu**)
- Berichtigung
- Einschränkung/Löschung
- Widerspruch/Widerruf
- Datenübertragbarkeit (**Neu**)
- Beschwerdemöglichkeit (**Neu**)

Vereinbarung über eine Auftrags-verarbeitung

Vertragliche Vereinbarung mit Auftrags-Verarbeiter nach Art. 28 DSGVO

Vertrag
[WKO Mustervertrag]

Verarbeitungstätigkeit

(Verfahrensverzeichnis) gilt auch eingeschränkt für Auftragsverarbeiter

Pflichten des Verantwortlichen

WER	Name / Kontaktdaten (Inkl. Datenschutzbeauftragten)
WAS	Erhobene Daten nach Kategorien
WARUM	Vertragserfüllung, rechtliche Verpflichtung, berechtigtes Interesse
WOZU	Zweck Beschreibung
WOHIN	Übermittlungsempfänger nach Kategorien
WIE LANG	Speicherdauer (Kriterien)
TOM´s	Schutzmaßnahmen für die Datensicherheit

Technische **O**rganisatorische **M**aßnahmen

Pflichten des Verantwortlichen

Ein Verein PC ist kein Privat PC!!!

Absicherung von Server/Desktop/Laptop/Mobiles

Komplexität „*$MyPass4711!*“ der Passwörter für die Zugangsdaten zum System

Installation einer Virenschutz Software, regelmäßige Durchführung eines kompletten System und Daten Scan

Supportunterstütztes Betriebssystem und Regelmäßige Durchführung der Windows Update

Supportunterstützte Anwendersoftware und Regelmäßige Durchführung der Anwendersoftware Update

Technische Organisatorische Maßnahmen

Pflichten des Verantwortlichen

Absicherung der Daten

E-Mail Kommunikation über eine gesicherte Verbindung und komplexen Passwörtern

Verwenden von Spamfiltern und Antivirus für E-Mail

Zugriffskonzept, wer hat wo Zugriff

WLAN Verbindungen nur über eine gesicherte Verbindung

Absicherung des Local Netzwerkes durch eine Firewall

Einsatz einer Festplattenverschlüsselung

Verbindungen zu Internet Portalen nur über eine gesicherte Verbindung

Firmenfremde Hardware im eigenem Firmennetzwerk verbieten

Firmennetzwerk und privates Netzwerk trennen

Technische Organisatorische Maßnahmen

Pflichten des Verantwortlichen

Daten Sicherung

Die Anlage von mindestens zwei Sicherungen im regelmäßigen Abstand auf physikalisch unabhängigen Datenträgern (Intern/Extern)

Regelmäßige Überprüfung der Sicherung auf

- Erfolgreicher Durchführung
  - System Sicherung
  - Exchange Sicherung
  - Datenbank Sicherung
  - File Sicherung
- Rücksicherungstest

Technische Organisatorische Maßnahmen

Pflichten des Verantwortlichen

Webseite

Sicherstellung der Daten im EU Raum (Auftragsverarbeiter Vereinbarung)

Sicherstellung einer Sicherung bei nicht statischen Webseiten

Sicherstellung einer regelmäßigen Wartung, nach Abhängigkeit der Webseite

Verwendung eines SSL Zertifikat, wenn personenbezogene Daten verarbeitet werden

Rechtskonformität des Impressum

Rechtskonformität des Newsletters

<u>Offenlegungspflicht nach dem Mediengesetz</u>

Eine „große Website“ liegt vor, wenn der Informationsinhalt über die Präsentation
des Unternehmens hinausgeht und geeignet ist, die Meinungsbildung zu beeinflussen.
Alle anderen Websites sind „kleine Websites“.

Technische Organisatorische Maßnahmen

Pflichten des Verantwortlichen

E-Mail

- Verwenden einer digitalen Signatur
- Verwenden einer Verschlüsselung von Daten
- Schutz der Daten bei Übermittlung
- Sicherstellung der Sicherung der Daten
- Regelung der Zugriffsberechtigung
- Schutz der Daten bei Mobilgeräten

Technische Organisatorische Maßnahmen

Pflichten des Verantwortlichen

Veranstaltung

Anmeldung in schriftlicher Form

Informationspflicht

- Verwendungszweck
- Weitergabe der Daten
- Speicherdauer
- Rechtsgrundlage

Technische **O**rganisatorische **M**aßnahmen

Pflichten des Verantwortlichen

Organe im Verein

Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen!!!

Kurzum

Dokumentationspflicht:

Erstellung eines zentralen Verfahrensverzeichnis, in dem alle verarbeiteten Daten nach diversen Parametern laufend gepflegt und aktualisiert werden.

Informationspflicht:

Betroffene (also Besitzer der Daten) haben das Recht auf Einsicht ihrer Daten bzw. zur Einschränkung der Datenverarbeitung und Datenweitergabe.

Prüfung des Datenschutz:

Durch die Datenschutzfolgeabschätzung sollen die Risiken beim Datenschutz aufgezeigt und davon passende Maßnahmen abgeleitet werden.

Auskunftspflicht:

Um die Rechte der betroffenen Personen zu wahren, schreibt die DSGVO eine erweiterte Auskunftspflicht über alle personenbezogenen Daten des Betroffenen vor und auch gegenüber der Aufsichtsbehörde.

Geldstrafen

Die Verletzung der Dokumentationspflicht ist mit bis zu EUR 10 Mio. oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

Relevante Artikel der DSGVO: Art 30-31
Relevante Erwägungsgründe: 13, 75, 76, 82, 89

Vielen Dank für Ihre Aufmerksamkeit

Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB17P0031
Valid:12/2020

Thomas Amon GmbH | Franz Gilly Gasse 7 | 3712 Maissau | Austria
dsgvo@at-edv.at | www.at-edv.at
Tel: +43 2958 20200 | Fax: +432958 20200 29