DATENSCHUTZ - GRUNDVERORDNUNG

BEDEUTUNG FÜR KLEINE UNTERNEHMEN

HAFTUNGSAUSSCHLUSS

- Wir sind keine Juristen
- Die hier präsentierten Informationen bieten nur einen Leitfaden
- Für die Umsetzung ist jedes Unternehmen selbst verantwortlich

INHALT

- Was ist die DSGVO
- Definitionen
  - Personenbezogene / Sensible Daten
- Verarbeitung
  - Umgang mit und Erfassung von personenbezogenen Daten
  - Verantwortlichkeiten & Haftungen
- Rechte und Pflichten
- Verarbeitungsverzeichnis
- Datenschutzbeauftragter
- Fragen?

WER SIND WIR?

- Verein `/usr/space`, besteht seit Mai 2015
- Wollen Menschen über Technik zusammenbringen & dafür begeistern

WAS IST DIE DSGVO

- Rechtlich Bindende Verordnung der EU
- Als Verordnung direkt in allen EU-Staaten rechtlich bindend
- Gültig ab 24. Mai 2016
- Bindend ab 25. Mai 2018
- Regelt die Prozesse, Verantwortungen & Strafen bei der Verarbeitung von personenbezogenen Daten

Speaker notes

- Erfassung = Verarbeitung
- Nicht nur elektronisch, auch strukturiert auf Papier
- Strukturiert = mit Index, als Formular z.B.
- DSG2000: Vieles bereits dort geregelt
- Unternehmen werden stärker in die Verantwortung genommen

DEFINITIONEN

PERSONENBEZOGENE DATEN

- Alle Informationen die sich auf eine natürliche Person beziehen
  - Name, Geburtsdatum, Geschlecht, Haarfarbe, Finanzinformationen, E-Mail, …

Speaker notes

Definiert in Art. 4 Absatz 1

Beispiel:

- Direkt: per Name + Geburtsdatum
- Indirekt: im Unternehmen 15 Männer, 2 Frauen, im Fragebogen M/W zur Auswahl

SENSIBLE DATEN

- Personenbezogene Daten, deren bekannt werden einen potentiellen Nachteil mit sich bringen können
  - Sexuelle Identität, Religiosität, politische Meinung, Gewerkschaftszugehörigkeit, Gesundheitsdaten, Fotos und Videos, …
- Mitarbeiterfotos sind biometrische Daten, also sensibel

Speaker notes

Besondere Kategorien: Art. 9 Absatz 1

- Signifikant: Streitpunkt, wird erst noch von DSB geregelt
- Fotos: Im Mitarbeiterverzeichnis, E-Mail ok, in Verbindung mit Gehaltsdaten unzulässig

VERARBEITUNG

UMGANG MIT PERSONENBEZOGENEN DATEN

- Zugriff darf nur bestimmten Personen gestattet sein
- Nur im Rahmen der Tätigkeit wenn begründet
- Keine Daten ausserhalb des unbedingt benötigten
- Absicherung nach Stand der Technik

Speaker notes

Artikel 5

- Für Verarbeitung von Gehaltsdaten ist kein Zugriff auf Geschlecht oder Alter notwendig.
- Ausnahmen bestätigen die Regel
- Details zu Verfahrensverzeichnis später

ERFASSUNG VON PERSONENBEZOGENEN DATEN

- Opt-In: nur erfassen, wenn Person dem zustimmt
- Informiertes Einverständnis: Person muss informiert werden, welche Daten zu welchem Zweck erfasst werden
- Minimale Erfassung: Anwendungen dürfen nur das unbedingt notwendige erfassen.

Speaker notes

Artikel 5

VERANTWORTLICHKEITEN & HAFTUNGEN

- Hauptverantwortlich: Geschäftsführer
- Kann Umsetzung delegieren
- Haftung kann nicht komplett abgegeben werden
- Strafen bis zu
  - 4% des Jahresumsatzes des Unternehmens
  - € 20 Mio.

Speaker notes

- Abgegebene Verantwortung kann nur soweit übernommen werden wie entsprechende Ausbildung vorhanden ist
- Strafen für vorsätzliches Fehlverhalten sicher höher als einfache Versäumnisse
  - Schlecht geführtes Verfahrensverzeichnis vs kein Verfahrensverzeichnis
  - Zu lasche Zugriffssicherung & Keine Zugriffssicherung

Verantwortung: Kapitel IV Strafen: Artikel 83

VERANTWORTLICHKEITEN & HAFTUNGEN

- Auskunftspflicht an Datenschutzbehörde
- Meldepflicht für neue Anwendungen entfällt
- Verarbeitungsverzeichnis ist Pflicht!

Speaker notes

DSG2000: Jede Verarbeitung muss vorher gemeldet werden. Entfällt bei DSGVO DSB kann jederzeit ohne Ankündigung Kontrollen durchführen

AUFTRAGSVERARBEITUNG

- Auftragsverarbeiter sind Dritte, an die Personendaten übermittelt werden
- Jede Weitergabe muss dokumentiert sein
- Darunter fallen auch Werbenetzwerke, Analysenetzwerke, …

Speaker notes

- Beispiel Auftragsverarbeiter: E-Mail-Anbieter, Webhoster, …

RECHTE UND PFLICHTEN

RECHTE UND PFLICHTEN

- Recht auf Auskunft: jede Person kann jederzeit über jede Kontaktmöglichkeit Auskunft über ihre verarbeitete Daten verlangen

Speaker notes

Auskunftsrecht: Art. 15

Fristen, etc.: Art 12

Jede! Kontaktmöglichkeit! Telefon, Fax, Email, Brief, …

Aber: Person muss ggf. genug Angaben für exakte Identifikation bekannt geben, und muss ggf. Identität nachweisen (Ausweiskopie, …)

Prozess muss ggf auch ins Verfahrensverzeichnis

Antwort muss bei sensiblen Daten gesichert sein: physisches Medium / verschlüsselt / verschlossener Brief

RECHTE UND PFLICHTEN

- Recht auf Berichtigung: jede Person kann jederzeit über jede Kontaktmöglichkeit die Berichtigung ihrer Daten verlangen
  - Innerhalb von 4 Wochen ab Eingang zu erledigen
  - In komplexen Fällen um 2 Monate verlängerbar

Speaker notes

Auskunftsrecht: Art. 16

Fristen, etc.: Art 12

Rechnungsdaten z.B. 7 Jahre aufzuheben Alles andere ist zu löschen!

Sonst gelten gleiche Bedingungen wie bei Auskunft

RECHTE UND PFLICHTEN

- Recht auf Einschränkung der Verarbeitung: jede Person kann jederzeit über jede Kontaktmöglichkeit die Verarbeitung ihrer Daten einschränken
  - Innerhalb von 4 Wochen ab Eingang zu erledigen
  - In komplexen Fällen um 2 Monate verlängerbar

Speaker notes

Auskunftsrecht: Art. 18

Fristen, etc.: Art 12

Rechnungsdaten z.B. 7 Jahre aufzuheben Alles andere ist zu löschen!

Sonst gelten gleiche Bedingungen wie bei Auskunft

RECHTE UND PFLICHTEN

- Recht auf Vergessen / Löschung: jede Person kann jederzeit über jede Kontaktmöglichkeit die Löschung ihrer Daten verlangen
  - Innerhalb von 4 Wochen ab Eingang zu erledigen
  - In komplexen Fällen um 2 Monate verlängerbar, ist zu begründen

Speaker notes

Auskunftsrecht: Art. 17

Fristen, etc.: Art 12

Rechnungsdaten z.B. 7 Jahre aufzuheben Alles andere ist zu löschen!

Sonst gelten gleiche Bedingungen wie bei Auskunft

RECHTE UND PFLICHTEN

- Recht auf Übertragung: jede Person kann jederzeit über jede Kontaktmöglichkeit die Ausfertigung ihrer Daten in einem maschinenlesbaren Format verlangen, zur Übertragung an ein anderes Unternehmen
  - Innerhalb von 4 Wochen ab Eingang zu erledigen
  - In komplexen Fällen um 2 Monate verlängerbar, ist zu begründen

Speaker notes

Gleiche Bedingungen wie bei Auskunft

RECHTE UND PFLICHTEN

- Informationspflicht:
  - bei Datenverlusten (Datendiebstahl) ist innerhalb von 72h ab bekannt werden die Daten-schutzbehörde zu informieren
  - bei sensiblen Daten auch die betroffenen Personen

VERARBEITUNGSVERZEICHNIS

VERARBEITUNGSVERZEICHNIS

- Aufzeichnung aller Verarbeitungsvorgänge
- Nicht unter 250 Mitarbeitern
- Ausnahme
  - Rechte oder Freiheiten der betroffenen Personen gefährdet
  - Wenn Daten nicht nur gelegentlich verarbeitet

Speaker notes

Artikel 30

- Rechte und Freiheiten: z.B. Gesundheitsdaten oder Finanzdaten als Hauptverarbeitung
- Nicht nur gelegentlich: Eine Buchhaltungsfirma, die typischerweise Gehaltsdaten verarbeitet, hat eines zu führen
- Z.B. bei Mitarbeiterdaten: Daten für Dienstzeugnis müssen 30 Jahre aufgehoben werden

BEISPIEL

	Datenschutzbeauftragter	Weitere Verantwortliche
dikovsky	Name:	Name:
se 8 obersdorf	Anschrift:	Anschrift:
d@usrspace.at	Kontakt:	Kontakt:

Basisdaten				Fristen		Weitergabe		Maßnahmen				
htz-schätzung	**Betroffene Personen**	**Rechtsgrundlage**	**Zugehörige Dokumente**	**Löschungsfristen**	**Aufbewahrungsfristen**	**Empfänger**	**Dokumentation**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Pseudonymisierung**	**E**
notwendige laten	Mitglieder des Vereins	Keine		Binnen 2 Wochen nach Beendigung der Mitgliedschaft	Dauer der Mitgliedschaft			Persönlich beschränkter Zugriff für Mitglieder des Vorstandes	Kryptographische Signatur	Regelmäßige Backups	Nicht anwendbar	
	Mitglieder des Vereins	§§ 131, 132 BAO		Binnen 1 Monat nach Ablauf der Aufbewahrungsfrist	Ende des Kalenderjahres des Austritts + 7 Jahre	BMF Kontoführende Bank		Persönlich beschränkter Zugriff für Mitglieder des Vorstandes Zugriff durch Rechnungsprüfer bei Bedarf	Kryptographische Signatur	Regelmäßige Backups	Nicht anwendbar	

BEISPIEL

Verantwortlicher		Datenschutzbeauftragter	Weitere Verantwortliche
Name:	Peter Ludikovsky	Name:	Name:
Anschrift:	Mühlgasse 8 2544 Leobersdorf	Anschrift:	Anschrift:
Kontakt:	vorstand@usrspace.at	Kontakt:	Kontakt:

BEISPIEL

Basisdaten				
Zweck und Beschreibung der Datenverarbeitung	**Datenschtz-Folgeabschätzung**	**Betroffene Personen**	**Rechtsgrundlage**	**Zugehörige Dokumente**
Mitgliederstammdaten: Name, E-Mail-Adresse	Nein, da notwendige Stammdaten	Mitglieder des Vereins	Keine	
Mitgliederdaten: Finanzdaten	Nein	Mitglieder des Vereins	§§ 131, 132 BAO	

BEISPIEL

Fristen

Löschungsfristen	**Aufbewahrungsfristen**
Binnen 2 Wochen nach Beendigung der Mitgliedschaft	Dauer der Mitgliedschaft
Binnen 1 Monat nach Ablauf der Aufbewahrungsfrist	Ende des Kalenderjahres des Austritts + 7 Jahre

BEISPIEL

Weitergabe

Empfänger	**Dokumentation**
BMF Kontoführende Bank	

BEISPIEL

Maßnahmen				
Vertraulichkeit	**Integrität**	**Verfügbarkeit**	**Pseudonymisierung**	**Evaluierungsmaßnahmen**
Persönlich beschränkter Zugriff für Mitglieder des Vorstandes	Kryptographische Signatur	Regelmäßige Backups	Nicht anwendbar	
Persönlich beschränkter Zugriff für Mitglieder des Vorstandes Zugriff durch Rechnungsprüfer bei Bedarf	Kryptographische Signatur	Regelmäßige Backups	Nicht anwendbar	

DATENSCHUTZBE-AUFTRAGTER

DATENSCHUTZBEAUFTRAGTER

- Pflicht für Firmen mit >250 MA *oder*
- 10 MA hauptsächlich mit der Verarbeitung beschäftigt sind *oder*
- Hauptsächtlich sensible Daten verarbeitet werden
- Aufgaben:
  - Führung des Verarbeitungsverzeichnisses
  - Kontrolle und Dokumentation der Verarbeitungsprozesse, schon bei der Konzeption
- nicht Weisungsgebunden

Speaker notes

Artikel 37 - 39

LINKS

LINKS

LINKS

- Präsentation: https://gitlab.usrspace.at/…
- Verein `/usr/space`: https://usrspace.at
- Präsentation ist CC-BY-SA 4.0

FRAGEN?