

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
- Ersetzt die DSG2000
- Verschärfte Haftung bei Verstößen und Fahrlässigkeiten

DEFINITIONEN

PERSONENBEZOGENE DATEN

- Alle Informationen die sich auf eine natürliche Person beziehen
 - Name, Geburtsdatum, Geschlecht, Haarfarbe, Finanzinformationen, E-Mail, ...
- Und diese direkt oder indirekt identifizierbar machen

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
- Sobald signifikanter Teil der Verarbeitung sensible Daten umfasst: Datenschutzbeauftragter Pflicht!

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
- Jede Verarbeitung braucht einen Prozess, der im Verfahrensverzeichnis dokumentiert ist

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.

VERANTWORTLICHKEITEN & HAFTUNGEN

- Hauptverantwortlich: Geschäftsführer
- Kann Umsetzung delegieren
- Haftung kann nicht komplett abgegeben werden
- Strafen bis zu
 - 4% des Jahresumsatzes des Unternehmens
 - € 20 Mio.
 - Je nachdem was mehr ist!
- Tatsächliche Strafe im Ermessen der Datenschutzbehörde

VERANTWORTLICHKEITEN & HAFTUNGEN

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

AUFTRAGSVERARBEITUNG

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

RECHTE UND PFLICHTEN

RECHTE UND PFLICHTEN

- Recht auf Auskunft: jede Person kann jederzeit über jede Kontaktmöglichkeit Auskunft über ihre verarbeitete Daten verlangen
 - Innerhalb von 4 Wochen ab Eingang zu erledigen
 - In komplexen Fällen um 2 Monate verlängerbar, ist zu begründen

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, ist zu begründen

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, ist zu begründen

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
 - Ausnahme: Löschung aus rechtlichen Gründen nicht möglich

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

RECHTE UND PFLICHTEN

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

VERARBEITUNGSVER ZEICHNIS

VERARBEITUNGSVERZEICHNIS

- Aufzeichnung aller Verarbeitungsvorgänge
- Nicht unter 250 Mitarbeitern
- Ausnahme
 - Rechte oder Freiheiten der betroffenen Personen gefährdet
 - Wenn Daten nicht nur gelegentlich verarbeitet werden
- Im Zweifel ist es besser eines zu führen

BEISPIEL

Datenschutzbeauftragter	Weitere Verantwortliche
Name: Anschrift: Kontakt:	Name: Anschrift: Kontakt:

Schätz- schätzung	Basisdaten		Fristen			Weitergabe		Maßnahmen			
	Betroffene Personen	Rechtsgrundlage	Zugehörige Dokumente	Löschungsfristen	Aufbewahrungsfristen	Empfänger	Dokumentation	Vertraulichkeit	Integrität	Verfügbarkeit	Pseudonymisierung
notwendige Daten	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	Datenschutz-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*
- Hauptsächlich sensible Daten verarbeitet werden
- Aufgaben:
 - Führung des Verarbeitungsverzeichnisses
 - Kontrolle und Dokumentation der Verarbeitungsprozesse, schon bei der Konzeption
- nicht Weisungsgebunden
- Vor Gericht nicht Auskunftspflichtig

LINKS

LINKS

LINKS

- Präsentation:
<https://gitlab.usrspace.at/everyone/presentation-dsgvo>
- Verein /usr/space: <https://usrspace.at>
- Präsentation ist [CC-BY-SA 4.0](#)

FRAGEN?