BEEKEEPER

White Paper

30-FRAGEN-ASSESSMENT FÜR DIE NEUE DATENSCHUTZ-GRUNDVERORDNUNG DER EU

EINFÜHRUNG

Die neue Datenschutz-Grundverordnung (GDPR) der EU vereinheitlicht die Regeln für die Verarbeitung personenbezogener Daten durch private und öffentliche Unternehmen. Die Verordnung soll insbesondere den Schutz von personenbezogenen Daten innerhalb der Europäischen Union sicherstellen. Das zugrundeliegende Gesetz wurde am 14. April 2016 angenommen und tritt per 25. Mai 2018 in Kraft. Ab dann kann die EU denjenigen Unternehmen, die sich nicht an die Bestimmungen halten, Bussgelder in Höhe von entweder 4 % des jährlichen Umsatzes oder 20 Millionen Euro verhängen, sowie weitere Sanktionen auferlegen. Hiervon betroffen sind nicht nur Unternehmen innerhalb der EU, sondern auch jene, die Mitarbeiter aus der EU beschäftigen. Die Regelungen des neuen Datenschutzrechtes schliessen also nicht nur Deutschland und Österreich, sondern auch die Schweiz ein. Setzen Sie sich deshalb früh mit den neuen Bestimmungen auseinander und sensibilisieren Sie Ihr Management.
Überprüfen Sie jetzt, welche Anforderungen der Datenschutz-Grundverordnung Ihr Unternehmen bereits erfüllt und welche zusätzlichen Massnahmen Sie für die Erfüllung des Reglements noch treffen müssen.

FRAGENKATALOG ZUR NEUEN DATENSCHUTZ-GRUNDVERORDNUNG (GDPR)

Folgende 30 Fragen unterstützen Sie in der Beurteilung, inwiefern Sie von der neuen Verordnung betroffen sind. Persönliche Daten und personenbezogene Daten werden synonym verwendet und beziehen sich auf jegliche Informationen, die die Identifizierung einer Person ermöglichen; dazu gehören technische, kulturelle, wirtschaftliche und soziale Informationen, sowie Erbgutinformationen und Informationen zur mentalen Gesundheit.

1. Verarbeitet Ihr Unternehmen persönliche Daten in EU-Ländern oder von EU-Bürgern? ☐

2. Setzt Ihr Unternehmen Technologien ein, mittels denen es Verstösse gegen die Datenschutzbestimmungen ermitteln kann (IDS / HIDS)? ☐

3. Hat Ihr Unternehmen ein Inventar aller verarbeiteten persönlichen Daten? ☐

4. Hat Ihr Unternehmen all seine Kanäle identifiziert, mittels denen es persönliche Daten verarbeitet? ☐

5. Verfügt Ihr Unternehmen über alle wichtigen technischen Mittel, mittels denen es die persönlichen Daten einer Person permanent löschen kann? ☐

6. Wird das Konzept des “eingebauten Datenschutzes” in Ihrem Unternehmen in Bezug auf die Datenverarbeitung bei Produkten und Dienstleistungen bereits berücksichtigt?

7. Analysieren und bewerten Sie während Ihres Produkt- oder Servicelebenszyklus allfällige Auswirkungen auf den Datenschutz? ☐

8. Entspricht das permanente Löschen persönlicher Daten den Standardbestimmungen gemäss der Internationalen Organisation für Normung (ISO) oder anderen Institutionen? ☐

9. Hat Ihr Unternehmen direkten Zugriff auf alle Systeme, mittels denen personenbezogene Daten verarbeitet werden? ☐

10. Besitzt Ihr Unternehmen das Recht, alle Systeme eigenhändig zu überprüfen, mittels denen persönliche Daten verarbeitet werden? ☐

11. Unterzeichnet Ihr Unternehmen eine Datenschutzvereinbarung mit dritten Parteien, bevor es persönliche Daten mit ihnen teilt? ☐

12. Ist Ihr Unternehmen nur so lange im Besitz von personenbezogenen Daten, wie es sie benötigt? ☐

13. Werden persönliche Daten verschlüsselt oder anonymisiert, bevor sie langfristig (z.B. als Backup) gespeichert werden? ☐

14. Ist der Zugriff auf personenbezogene Daten lediglich dann möglich, wenn er benötigt wird? ☐

15. Werden persönliche Daten sowohl unternehmensweit als auch von Dritten, die darauf Zugriff haben, gleich gut geschützt? ☐

16. Ist der Zugriff auf persönliche Daten durch sichere Authentifizierungstechnologien geschützt? ☐

17. Bleibt der gesamte Lebenszyklus von persönlichen Daten in Ihrem Unternehmen nachvollziehbar und überprüfbar? ☐

18. Verzichtet Ihr Unternehmen auf ein auf persönlichen Daten basierendes Profiling mittels Analyse von Arbeitsleistung, wirtschaftlicher Situation, Gesundheit, persönlichen Vorlieben, Interessen, Zuverlässigkeit, Verhalten und Aufenthaltsorte? ☐

19. Treffen in Ihrem Unternehmen folgende Faktoren zu, wenn Sie die Zustimmung einer Person in Bezug auf die Verarbeitung deren persönlicher Daten einholen: ☐

a. Der Grund, weshalb eine Zustimmung notwendig ist, wird klar und transparent kommuniziert.

b. Die Zustimmung zur Verarbeitung persönlicher Daten basiert nicht auf Schweigen, Inaktivität oder vorausgewählten Kästchen; die Person muss Ihre Wahl stets frei treffen können.

c. Der Prozess für das Einholen einer Zustimmung ist klar geregelt und nachvollziehbar.

d. Die Zustimmung kann mühelos widerrufen werden.

20. Verfügt Ihr Unternehmen über einen Prozess, mittels dem es Verstösse gegen die Datenschutzbestimmungen ermitteln kann und entspricht dieser den Anforderungen der Artikel 33 und 34 der neuen Datenschutz-Grundverordnung? ☐

21. Hat Ihr Unternehmen eine Strategie zur Datensparsamkeit? ☐

22. Vermeidet Ihr Unternehmen das manuelle Verarbeiten von persönlichen Daten? ☐

23. Erzeugt Ihr Unternehmen aggregierte Daten, die von sämtlichen persönlichen Daten gesäubert sind? ☐

24. Verarbeitet Ihr Unternehmen persönliche Daten auch in Ländern mit anderer Rechtsordnung? Falls ja, trifft hierbei Folgendes zu:
a. ie andere Rechtsordnung verfügt über angemessene Datenschutzbestimmungen.
b. er Transfer persönlicher Daten entspricht adäquaten technischen Sicherheitsmassnahmen.
c. Zwischen Sender und Empfänger der persönlichen Daten besteht eine vertragliche Vereinbarung.

25. Hat Ihr Unternehmen einen Datenschutzbeauftragten bestimmt?

26. Verwendet Ihr Unternehmen persönliche Daten zu einem anderen Zweck als für denjenigen, der mit dem Datensubjekt ausgemacht wurde? Hierzu zählen allgemeine Tests, die Weitergabe der Daten an eine Tochter- oder Partnerfirma mit einem Zweck, der vom ursprünglichen abweicht oder Marketingabsichten, denen das Datensubjekt nicht explizit zugestimmt hat.

27. Sind Ihre Datenschutzrichtlinien transparent und klar bezüglich der Verarbeitung persönlicher Daten?

28. Bietet Ihr Unternehmen denjenigen Mitarbeitenden, die mit persönlichen Daten zu tun haben, regelmässig Schulungen an?

29. Ist Ihr Unternehmen mit dem Sensitivity Rating vertraut, das sich auf Datensubjekte bis 16 Jahre bezieht?

30. Führen Sie eine Liste mit allen Dritten, die durch Ihr Unternehmen Zugriff auf persönliche Daten erhalten, sei dies auf direktem oder indirektem Wege?

Disclaimer: Die hier enthaltenen Fragen wurden nicht von der EU sanktioniert, sondern im Rahmen des internen GDPR Compliance-Assessments von unserem Chief Information Security Officer als essentiell beurteilt. Eine komplette Liste aller Anforderungen bezüglich GDPR finden Sie hier:

Official EU Documentation:
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1499864717744&uri=LEGISSUM:310401_2

Online Dokumentation:
https://dsgvo-gesetz.de/

Offizielles Archiv:
http://ec.europa.eu/justice/data-protection/

Inoffiziell:
http://www.eugdpr.org/eugdpr.org.html

BEEKEEPER

Beekeeper ist eine mehrfach ausgezeichnete Mitarbeiter-App, die dabei hilft, den Arbeitsplatz von gewerblichen Mitarbeitern zu digitalisieren. Unsere Mission besteht darin, diejenigen Menschen zu verbinden, die zuvor von der internen Kommunikation im Unternehmen weitgehend ausgeschlossen waren. Beekeeper macht Mitarbeiter über Standorte und Abteilungen hinweg in Echtzeit erreichbar und integriert bestehende IT-Systeme und Kommunikationskanäle auf einer sicheren Plattform. Unser smartes Dashboard hilft dabei, bessere Entscheidungen zu treffen und Prozesse zu optimieren. Beekeeper ist bei Mitarbeitern in mehr als 130 Ländern als mobile Kommunikationsplattform im Einsatz. Zu unseren Kunden zählen Unternehmen wie Ricola, Leffers oder MANN+HUMMEL. Neben dem Hauptsitz in Zürich ist Beekeeper mit Standorten in San Francisco, Berlin und London vertreten.

Weitere Informationen finden Sie unter www.beekeeper.io/de.