

GDPR ESSENTIALS FOR TECHNOLOGY COMPANIES

THE 20 QUESTIONS YOUR DATA PROTECTION OFFICER SHOULD BE ABLE TO ANSWER.

1. LEGAL BASIS & ACCOUNTABILITY

- IDENTIFIED AND DOCUMENTED THE LEGAL BASIS (ART. 6) FOR EACH PROCESSING ACTIVITY
- APPOINTED A DATA PROTECTION OFFICER WHERE REQUIRED (ART. 37)
- ESTABLISHED A RECORD OF PROCESSING ACTIVITIES (ART. 30)

2. DATA PROCESSING AGREEMENTS

- ALL PROCESSORS COVERED BY GDPR-COMPLIANT DPAs (ART. 28)
- SUB-PROCESSOR CHAINS DOCUMENTED AND CONTRACTUALLY CONTROLLED
- ANNUAL DPA AUDIT CYCLE ESTABLISHED
- STANDARD CONTRACTUAL CLAUSES IN PLACE FOR NON-EU TRANSFERS

3. CROSS-BORDER TRANSFERS

- MAPPED ALL DATA FLOWS TO THIRD COUNTRIES (ART. 44-49)
- TRANSFER IMPACT ASSESSMENT COMPLETED FOR EACH DESTINATION
- APPROPRIATE SAFEGUARDS IMPLEMENTED (SCCs, BCRs, ADEQUACY DECISIONS)

4. DATA SUBJECT RIGHTS

- PROCESS FOR ACCESS REQUESTS OPERATIONAL AND TESTED (ART. 15)
- DELETION AND RECTIFICATION WORKFLOWS DOCUMENTED (ART. 16-17)
- DATA PORTABILITY CAPABILITY IN PLACE FOR AUTOMATED PROCESSING (ART. 20)
- RESPONSE WITHIN 30-DAY DEADLINE CONSISTENTLY MET

5. BREACH NOTIFICATION

- 72-HOUR NOTIFICATION PROCESS TO SUPERVISORY AUTHORITY DEFINED (ART. 33)
- DATA SUBJECT NOTIFICATION CRITERIA AND TEMPLATES PREPARED (ART. 34)
- INCIDENT RESPONSE TEAM ROLES ASSIGNED AND REHEARSED
- BREACH REGISTER MAINTAINED AND CURRENT

6. TECHNICAL & ORGANISATIONAL MEASURES

- PRIVACY BY DESIGN EMBEDDED IN PRODUCT DEVELOPMENT (ART. 25)
- DATA PROTECTION IMPACT ASSESSMENTS CONDUCTED FOR HIGH-RISK PROCESSING (ART. 35)
- CONSENT MANAGEMENT SYSTEM IMPLEMENTED WHERE CONSENT IS THE LEGAL BASIS
- EMPLOYEE DATA PROTECTION TRAINING PROGRAMME ESTABLISHED AND DOCUMENTED

NEED GUIDANCE? CONTACT FRIEDRICH KURZ — fk@kurz.law · +49 30 2388 9840

VO-GRUNDLAGEN FÜR TECHNOLOGIEUNTERNEHMEN

DIE 20 FRAGEN, DIE IHR DATENSCHUTZBEAUFTRAGTER BEANTWORTEN KÖNNEN SOLLTE.

1. RECHTSGRUNDLAGE & VERANTWORTLICHKEIT

- RECHTSGRUNDLAGE (ART. 6) FÜR JEDE VERARBEITUNGSTÄTIGKEIT IDENTIFIZIERT UND DOKUMENTIERT
- DATENSCHUTZBEAUFTRAGTEN BESTELLT, SOWEIT ERFORDERLICH (ART. 37)
- VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN GEFÜHRT (ART. 30)

2. AUFTRAGSVERARBEITUNG

- ALLE AUFTRAGSVERARBEITER DURCH DSGVO-KONFORME AVV ABGEDECKT (ART. 28)
- UNTERAUFTRAGNEHMER-KETTEN DOKUMENTIERT UND VERTRAGLICH KONTROLLIERT
- JÄHRLICHER AVV-AUDIT-ZYKLUS ETABLIERT
- STANDARDVERTRAGSKLAUSELN FÜR DRITTLANDTRANSFERS ABGESCHLOSSEN

3. GRENZÜBERSCHREITENDE TRANSFERS

- ALLE DATENFLÜSSE IN DRITTLÄNDER ERFASST (ART. 44-49)
- TRANSFER IMPACT ASSESSMENT FÜR JEDES ZIELLAND DURCHGEFÜHRT
- GEEIGNETE GARANTIEEN IMPLEMENTIERT (SCCs, BCRs, ANGEMESSENHEITSBESCHLÜSSE)

4. BETROFFENENRECHTE

- AUSKUNFTSPROZESS OPERATIV UND GETESTET (ART. 15)
- LÖSCHUNGS- UND BERICHTIGUNGSWORKFLOWS DOKUMENTIERT (ART. 16-17)
- DATENPORTABILITÄT BEI AUTOMATISierter VERARBEITUNG GEWÄHRLEISTET (ART. 20)
- 30-TAGE-FRIST WIRD DURCHGEHEND EINGEHALTEN

5. MELDEPFLICHTEN BEI DATENPANNEN

- 72-STUNDEN-MELDEPROZESS AN DIE AUFSICHTSBEHÖRDE DEFINIERT (ART. 33)
- BENACHRICHTIGUNGSKRITERIEN UND VORLAGEN FÜR BETROFFENE VORBEREITET (ART. 34)
- INCIDENT-RESPONSE-TEAM MIT ROLLEN BESETZT UND ERPROBT
- VERZEICHNIS VON DATENSCHUTZVERLETZUNGEN GEFÜHRT UND AKTUELL

6. TECHNISCHE & ORGANISATORISCHE MASSNAHMEN

- PRIVACY BY DESIGN IN DER PRODUKTENTWICKLUNG VERANKERT (ART. 25)
- DATENSCHUTZ-FOLGENABSCHÄTZUNG BEI HOCHRISIKO-VERARBEITUNGEN DURCHGEFÜHRT (ART. 35)
- EINWILLIGUNGSMANAGEMENT IMPLEMENTIERT, WO EINWILLIGUNG DIE RECHTSGRUNDLAGE IST
- DATENSCHUTZ-SCHULUNGSPROGRAMM FÜR MITARBEITER ETABLIERT UND DOKUMENTIERT