








Framework zum Datenschutz durch Technikgestaltung

Governance:

Umfasst das Datenschutzbewusstsein innerhalb der Organisation, interne Richtlinien, Maßnahmen im Rahmen der Rechenschaftspflicht, Transparenz gegenüber Betroffenen, sowie Kooperation mit Dritten und Datenverarbeitern (einschließlich Vereinbarungen über die Datenverarbeitung)

Themen	Anonymisierung	1. Datenminimierung Art. 5(1)c	2. Pseudonymisierung Art. 4(5)	3. Verschlüsselung Art. 6(4)e, 32(1)a	4. Zugangskontrolle Art. 32(1), 5(1)f	5. Datenschutzfreundliche Voreinstellungen Art. 25(2)	6. Löschungs- / Aufbewahrungsbedingungen Art. 5(1)e	7. Unterstützung der Rechte der betroffenen Person Art. 12-22
Aktionen								
Technisch	Anonymisierung und Sammlung (z. B. Differential Privacy)	Nur absolut notwendige Daten sammeln. Unnötige Daten sofort löschen.	Entfernung aller direkt identifizierenden Elemente, Hashing, polymorphe Pseudo-ID.	z. B. Public-Key-Verschlüsselung, Festplattenverschlüsselung.	Digitaler Datentresor, physische Zugangskontrollen, logische Zugangskontrollen, Authentifizierung und Autorisierung.	Datenschutzfreundliche Einstellungen als Standard, transparente Benutzerschnittstelle, Berechtigungsmanagement.	Automatische Löschung, "Markieren" der Daten am Ende der Frist, "Sticky Policies", Data Fading.	Datenschutz-Dashboard, Kommunikation und Support (Art. 5(1)a).
Unterstützende Unterlagen	Keine zusätzlichen Maßnahmen erforderlich, keine persönlichen Daten enthalten.	Beschreibung des Zwecks der Datenverarbeitung und Liste der erforderlichen Daten.	Richtlinie zur Trennung von identifizierenden Daten und anderen Daten oder Vereinbarungen.	Informationssicherheitsstandards (Art. 32(1)) und Richtlinien.	Autorisierungsmatrix und Protokollierung auf Basis des Wissens- und Zugangsbedarfs.	Registrierung Opt-in / Opt-out und Berechtigungen.	Richtlinie und Überblick der Aufbewahrungsbedingungen, Verwaltung von elektronischem Abfall.	Datenschutzerklärung, Richtlinie für Zugriffsanfragen sowie Berichtigung und Löschung von personenbezogenen Daten.
Alternativen	Falls Daten nicht anonymisiert sind, folgen Sie diesem Schema	Falls möglich, einen Teil des Datensatzes anonymisieren / zusammenfassen, Data Fading.	Anderweitige Sicherheitsmaßnahmen.	Anderweitige Sicherheitsmaßnahmen (eigenständiger Server).	Zugriffsprotokolle, mit Kontrollen.	Keine Alternative, nur Vorgaben erfüllen.	Anonymisieren und zusammenfassen (archivieren, falls erlaubt).	Keine Alternative, rechtliche Verpflichtung.

Datenschutzprüfung

Eine Datenschutzfolgenabschätzung kann die Anforderungen prüfen und erforderliche Maßnahmen aufzeigen (Art. 35 DSGVO).

Framework zum Datenschutz durch Technikgestaltung

Warum dieses Framework?

In der Datenschutz-Grundverordnung ist der Datenschutz durch Technikgestaltung ausdrücklich erforderlich für die Verarbeitung von personenbezogenen Daten (Art. 25 DSGVO). Datenschutz durch Technikgestaltung bedeutet, dass Organisationen bei der Entwicklung von (neuen) Produkten und Dienstleistungen auf den Schutz der personenbezogenen Daten achten müssen. Die Implementierung von Datenschutzmaßnahmen in frühen Entwicklungsstadien ist kostensparend, da durch sie spätere kostspielige Eingriffe verhindert werden und bereits frühzeitig die Einhaltung der Vorgaben erleichtert wird. In der Praxis ist es jedoch oft unklar, wie die Einhaltung der Anforderungen bezüglich des Datenschutzes durch Technikgestaltung erreicht werden kann.

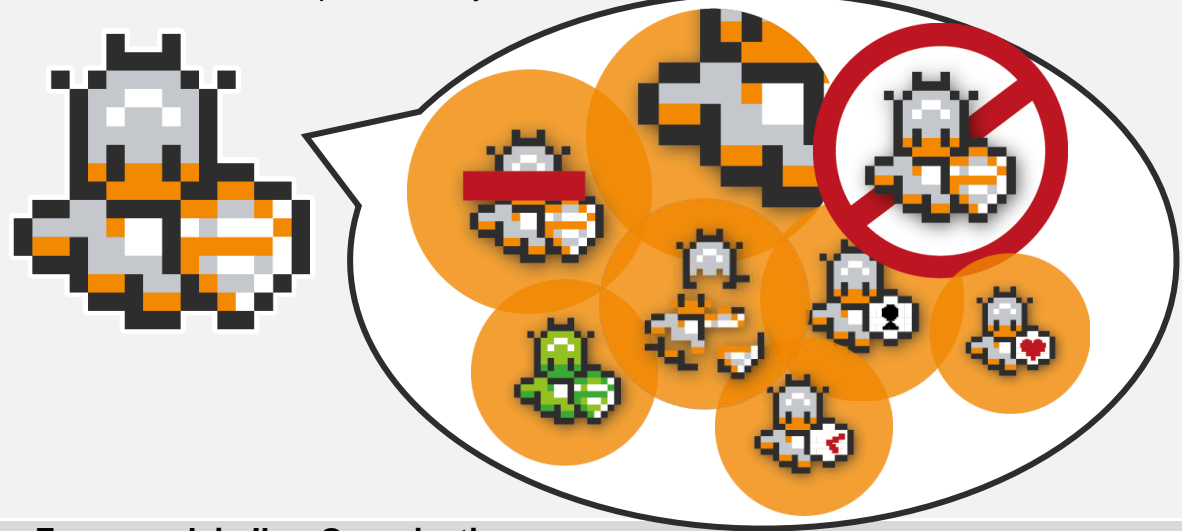
Wie sollte dieses Framework verwendet werden?

Dieses Framework stellt einen Leitfaden zum Thema Datenschutz durch Technikgestaltung dar, der die verschiedenen Erfordernisse der Datenschutz-Grundverordnung einbindet.

Anonymisierte Daten sollten immer bevorzugt werden. Wenn das nicht möglich ist, können den Anweisungen in den anderen Spalten des Frameworks gefolgt werden. In allen Fällen gibt es eine technische/organisatorische Komponente mit unterstützenden Unterlagen oder organisatorischen Maßnahmen. Durch die Verwendung dieses Frameworks und die Überprüfung, welche Aspekte in Ihrer Organisation bereits berücksichtigt werden, entsteht ein Überblick über die Art und Weise, wie Ihre Organisation die Vorgaben zum Datenschutz durch Technikgestaltung erfüllt.

Da nicht immer alle technischen Aspekte erfüllt werden können, werden einige alternative Schutzmaßnahmen vorgeschlagen.

Lassen Sie sich von Captain Privacy leiten!



Integrieren Sie dieses Framework in Ihre Organisation

Das Framework kann intern als Teil des Gesamtpakets Datenschutz und Data Governance verwendet werden. Um die Einhaltung der Vorgaben zu gewährleisten, empfehlen wir regelmäßige Kontrollen auf Basis des Frameworks. Zusätzlich kann eine Datenschutzfolgenabschätzung klären, welche Maßnahmen erforderlich sind, wenn neue Produkte oder Dienstleistungen entwickelt oder neue Aktivitäten zur Verarbeitung von Daten eingeführt werden.