TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2020"

Berlin, 03.-04.11.2020

Big Data & DSGVO

RA Dr. Christoph Bausewein CIPP/E

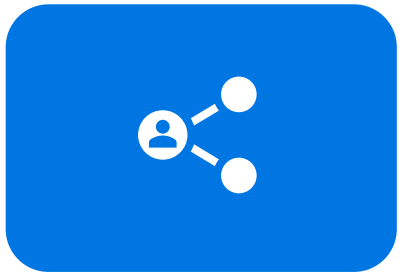
Director & Counsel, Data Protection & Policy bei CrowdStrike

Bundesverband der Datenschutzbeauftragten

DSGVO Datenschutzprinzipien

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Zweckbindung



Datenminimierung

Richtigkeit

Speicherbegrenzung

Integrität und Vertraulichkeit

Rechenschaftspflicht

Risikobasierter Ansatz der DSGVO

- Kommt in verschiedenen Regelung zum Ausdruck:
  - Die DSGVO verlangt für die Verarbeitung von personenbezogenen Daten „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ (**Art. 32 Abs. 1 DSGVO**)
  - Wenn eine neue Datenverarbeitung vermeintlich ein hohes Risiko birgt, hat eine Datenschutz-Folgenabschätzung (**Art. 35 DSGVO**) stattzufinden, die das Risiko analysiert und ggf. unterstützt, geeignete Abhilfemaßnahmen zu entwickeln
  - **Erwägungsgrund 76** schreibt einen objektiven Maßstab für die Risikoanalyse vor: “Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.” (Hervorhebungen hinzugefügt)

Relevante Risiken

- **Erwägungsgrund 75** enthält eine Auflistung der Risiken, die bei der Gestaltung von technischen und organisatorischen Maßnahmen zum Datenschutz zu beachten sind:

  - „Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem *physischen, materiellen oder immateriellen Schaden* führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, *wenn personenbezogene Daten*, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten *verarbeitet* werden, *wenn persönliche Aspekte bewertet werden*, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn *personenbezogene Daten schutzbedürftiger natürlicher Personen*, insbesondere Daten von Kindern, *verarbeitet* werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.”

    (Hervorhebungen hinzugefügt; *allgemeine Voraussetzungen kursiv;* aufgezählte Einzelkriterien unterstrichen)

Was verlangt die DSGVO mit Blick auf die Nutzung von Big Data?

- **Privacy by Design**

RECHTMÄßIGKEIT
Art. 6 Abs. 1 lit. f DSGVO, Art. 88 Abs. 1 i.V.m. § 26 Abs. 1 S. 1 BDSG (Betriebs-vereinbarung)

TRANSPARENZ
Datenschutzhinweis zu Datenanalysen, Monitoring und Tracking mit präventivem Charakter

FAIRNESS
Interessen und Erwartungen der betroffenen Person berücksichtigen, keine Fehlvorstellungen ausnutzen

ZWECKBINDUNG
Personenbezogene Daten, die zum Zweck der Datensicherheit verarbeitet werden, dürfen nur zu diesem und anderen legitimen und angezeigten Zweck verwendet werden
(vgl. 14. TB BFDI, § 31 BDSG a.F.)

DATENMINIMIERUNG
Benötigte Datenquellen nach Bedarf auswählen und nutzen

SPEICHERBEGREZUNG
Datenlöschung nach Zweckerfüllung, vorbehaltlich weiterer legitimer Zwecke

INTEGRITÄT + VERTRAULICHKEIT
TOM (starke Policies inkl. Verhaltensregeln und Zwecksetzung – Applicable Use

RECHENSCHAFT
Logging, Regelmäßige Audits + Reports

- Bedarfsweise **Datenschutz-Folgenabschätzung** bei zu erwartendem „hohen Risiko“ für die Betroffenen

Datenschutz-Folgenabschätzung

Liegt ein “hohes Risiko” vor

- Vgl. dazu WP 248 Rev. 01 17/DE der Art. 29 Datenschutzgruppe (Vorgänger EDPB) und das Kurzpapier 18 der DSK (Datenschutzkonferenz der deutschen Aufsichtsbehörden)

Blick in jeweilige “Blacklists” nach Art. 35 Abs. 4 DGSVO

- Zwischenzeitlich hat fast jede Aufsichtsbehörde ihre eigene Blacklist herausgegeben

Bedarfsweise individuelle Vorabprüfung

- Enthält die jeweilige Blacklist kein einschlägiges Beispiel kann nicht automatisch geschlussfolgert werden, dass keine DSFA erforderlich ist; vielmehr muss eigenständig das Risiko im Rahmen einer Vorabprüfung eingeschätzt werden (so etwa der LfDI Ba-Wü in seiner Blacklist)

Dokumentation der Datenschutz-Folgenabschätzung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Gewährleistungsziel	Summarische Risikobetrachtung	Index
Verfügbarkeit	Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
VB.1	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	IT-Fehlfunktion	Hard- und/oder Software-Fehlfunktion führen dazu, dass erforderliche digitale Daten unwiederbringlich verloren gehen.	Aufgrund der Komplexität des HCM-Systems (zahlreiche, zusammenwirkende Komponenten, häufige Updates usw.) ist ein Datenverlust durch IT-Fehlfunktionen sehr wahrscheinlich.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	8	M.1 Basis Backup-Struktur nutzen M.2 Dienstleistungsangebot HCM-Hersteller nutzen	Datenverluste bei von der Stadt betriebenen Systemen, die mit dem HCM-System vergleichbar sind, gehen gegen Null.	gr
VB.2	= VB.1 =	Interner User	User-Interaktionen mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Aufgrund der angespannten Personalsituation werden teilweise auch noch sehr unerfahrene HCM-Sachbearbeiter eingesetzt.	2	Fehlbedienungen von internen Usern, die zu einem Datenverlust führen (z.B. Daten versehentlich überschreiben), sind punktuell und werden i.d.R. rasch erkannt und wieder berichtigt.	2	4	M.1 Basis Backup-Struktur nutzen M.3 Löschberechtigung restriktiv vergeben M.4 HCM-Benutzer schulen	Die Maßnahmen zusammen führen zu einer deutlich reduzierten Eintrittswahrscheinlichkeit.	gr
VB.3	= VB.1 =	Externer User	Interaktionen externer User (z.B. Finanzprüfer, Auditoren) mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Zugriffe externer User auf das produktive HCM-System finden nur selten statt.	2	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	4	M.5 Lesenden Zugriff für berechtigte Dritte konfigurieren	Fehlbedienungen von externen Benutzern, die zu einem Datenverlust führen, sind nicht vorstellbar, da solche Benutzer stets nur mit Leserechten ausgestattet sind (bewährtes Standardbenutzerprofil).	gr
VB.4	= VB.1 =	Interner Administrator	Interaktionen eines User mit weitreichenden Administratorenrechten mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Da es das Alltagsgeschäft von Administratoren ist, mit produktiven IT-Systemen richtig umzugehen, ist der Eintritt unwahrscheinlich.	2	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	4	M.1 Basis Backup-Struktur nutzen M.3 4-Augen-Prinzip für tragende Personaldatenänderungen umsetzen M.6 HCM-Administratoren zertifizieren	Blickt man auf die schon lange aktive Administrationstätigkeit mit Umsetzung der Maßnahmen zurück, so erscheint der Eintritt als sehr unwahrscheinlich.	gr
VB.5	= VB.1 =	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware gehen erforderliche Daten unwiederbringlich verloren.	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	8	M.7 Basis Schadsoftware-/ Hackerabwehrsystem nutzen M.1 Basis Backup-Struktur nutzen	Datenverluste bei ebenfalls betriebenen IT-Systemen, die mit dem HCM-System vergleichbar sind, sind entsprechend eingestuft. Bzgl. HCM-System sind keine Besonderheiten erkennbar.	ge
VB.6	Monatlichen Gehaltsabrechnung kann nicht rechtzeitig durchgeführt werden	Interner User	Fehlendes, nicht mittelfristig ersetzbares Personal bringt monatliche Personalabrechnung zum Stehen.	Altersstruktur des betroffenen Personals und relativ hohe Fluktation von Experten im HCM-Umfeld verschärfen die Situation.	4	Falls die Entgeltabrechnung nicht ordnungsgemäß läuft, kann dies zu ernsthaften finanziellen Schwierigkeiten der Beschäftigten führen.	3	12	M.8 Kopfmonopole mittels Teambildung reduzieren M.9 Dienstleistung Dritter nutzen M.10 Manuelle Abschlagzahlung	Trotz der ergriffenen Maßnahmen für die aktive und passive Risikobewältigung kann das Risiko nicht in den grünen Bereich gebracht werden.	ge
VB.7	= VB.6 =	IT-Fehlfunktion	*noch weiter zu ergänzen*	usw.	1	usw.	3	3	usw.	usw.	ge

Quelle | Formular Download unter https://www.datenschutz-bayern.de/dsfa/

Big Data & Cybersecurity

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Cybersecurity ist essentiell für Datenschutz und die Einhaltung der DSGVO

Cybersecurity funktioniert nicht ohne Big Data Analysen

Big Data Analysen sind erforderlich, um Einbrüche in Netzwerke zu erkennen, einzukreisen und abzustellen, Daten zu schützen, Risiken einzuschätzen und Angreifer zu identifizieren

Survival of the Fastest

Zulässigkeit von Big Data Analysen nach der DSGVO

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"Under data protection law organizations must have appropriate security measures and robust procedures in place to ensure that any attempt to infiltrate computer systems is made as difficult as possible."

Steve Eckersley, Director of Investigations, UK Information Commissioner's Office
Winter 2020 statement in issuing a £500,000 fine

Rechtmäßigkeit von Big Data Analysen zu Cybersecurity-Zwecken

- Nach Ansicht des Gesetzgebers stellt die „Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT, beziehungsweise Computer Security Incident Response Teams – CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten“ ein berechtigtes Interesse des jeweiligen Verantwortlichen dar (**Erwägungsgrund 49 der DSGVO**)

Links

- WP221: https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/WP221_StatementDevelopmentBlogData.html
- WP248: https://www.datenschutz-bayern.de/technik/orient/wp248.pdf
- DSFA Formular: https://www.datenschutz-bayern.de/dsfa/DSFA-RM-Personalverwaltung.pdf
- Aufsatz von Schroeder: “Der risikobasierte Ansatz in der GS-GVO” https://beckassets.blob.core.windows.net/product/readingsample/9002683/9002683_zd%2011-2019%20-%20beitrag%20schr%C3%B6der.pdf?utm_content=buffer29d97&utm_medium=social&utm_source=facebook&utm_campaign=facebook
- DSFA Blacklist LfDI Baden-Württemberg: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf
- Code for Big Data Best Practices der Spanischen Datenschutzaufsichtsbehoerde (auf Spanisch): https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf
- Hinweise und Muster zur DSFA das LDA Bayern: https://www.datenschutz-bayern.de/dsfa/
- EU Member State DPIA Whitelists, Blacklists and Guidance: https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/