ZD.B ZENTRUM DIGITALISIERUNG. BAYERN

Dr. Christian Thiel, Dominik Golle,
Prof. Dr. Dr. h.c. Manfred Broy

Privacy by Design als Win-win-Strategie für Wirtschaft und Verbraucher*innen

ZD.B DIGITAL DIALOGUE

POSITIONSPAPIER

Oktober 2019

Editorinnen:
Dr. Nina Höhne, Dr. Kathrin Barbara Zimmer

Eine Initiative von
Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

ZD.B ZENTRUM DIGITALISIERUNG. BAYERN

Inhalt

„Privacy by Design is important for every area of your business“

Forbes Technology Council 2018 [1]

EINLEITUNG

Vielen Verbraucher*innen wird der Schutz ihrer Privatsphäre immer wichtiger, dadurch steigt auch die Bedeutung des Prinzips „Privacy by Design“ (PbD), also des bewussten Umgangs mit personenbezogenen Daten bei der Entwicklung eigener Produkte. Die Europäische Datenschutzgrundverordnung [2] (DSGVO) schreibt PbD zwar regulatorisch vor, doch zur Umsetzung in Unternehmen fehlen konkrete Anleitungen und Best-Practice-Sammlungen. Das führt dazu, dass PbD bisher von wenigen Akteur*innen eingesetzt wird. Dabei kann PbD Datenschutz- und Compliance-Risiken für Unternehmen drastisch reduzieren und kommt dann auch Verbraucher*innen zugute. Die Potenziale dieser Win-win-Situation gilt es nun zu nutzen. Das vorliegende Whitepaper möchte dazu seinen Beitrag leisten, indem es nicht nur das Prinzip der PbD erläutert, sondern auch darlegt, warum und wie diese Win-win-Situation durch PbD erreicht werden kann.

PRIVACY BY DESIGN UND REGULATORISCHE GRUNDLAGEN

Die meisten Unternehmen erheben personenbezogene Daten und sind gehalten, diese zu schützen. Privacy by Design ist ein präventiver Ansatz, der darauf abzielt, Datenschutzrisiken zu begegnen, bevor sie auftreten. PbD besteht aus Grundsätzen, Managementstrategien und Rezepten für Entwickler (Patterns), die es ermöglichen, die Privatsphäre der Nutzer*innen über den gesamten Lebenszyklus von Produkten und Geschäftsmodellen zu schützen.

Welche regulatorischen Vorgaben gibt es, die den Einsatz von PbD verlangen? In der Europäischen Datenschutzgrundverordnung [2] (DSGVO) wird in Art. 25 I unter der im Deutschen wenig konkreten Überschrift „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ (engl.: data protection by design and by default) gefordert, dass *„der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen [...] trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.“* Diese Datenschutzgrundsätze sind unter anderem in Art. 5 I DSGVO nachzulesen, wo beispielsweise unter dem Stichwort „Transparenz“ festgelegt wird, dass personenbezogene Daten *„in einer für die betroffene Person nachvollziehbaren Weise verarbeitet“* werden müssen, oder unter „Zweckbindung“, dass erhobene Daten nur für vorher *„festgelegte, eindeutige und legitime Zwecke“* verwendet werden dürfen.

Damit schreibt der Gesetzgeber die Umsetzung von PbD vor, aber neben wenigen Beispielen in der DSGVO bleibt offen, welche technischen und organisatorischen Maßnahmen (TOMs) genau getroffen werden müssen, um Art. 25 rechtskonform umzusetzen. Rechtlich verbindliche Aussagen hierzu werden erst im Lauf der Zeit und im Wechselspiel von gelebter Praxis, Rechtsprechung und Gesetzgebung gefunden werden.

„Privacy by Design ist längst kein Thema, das nur für Suchmaschinen und soziale Netzwerke relevant ist. Viele Unternehmen unterschätzen noch sowohl die Menge und Bedeutung gesammelter Daten, als auch das Risiko und die Verantwortung, die damit einhergeht. Privacy by Design sollte daher nicht nur als Lösung für DSGVO-Compliance gesehen werden, sondern auch als Verpflichtung, die man gegenüber seinen Kunden und Nutzern hat."

Christof Baumgartner, XITASO Holding GmbH

Sieht man sich hingegen das in den neunziger Jahren geprägte Konzept von Privacy by Design an, wird glücklicherweise konkreter, was darunter zu verstehen ist. Geprägt wurde der Begriff von der ehemaligen Datenschutzbeauftragten der kanadischen Provinz Ontario, Ann Cavoukian. Gemäß den von ihr aufgestellten Prinzipien (siehe Info-Box und [3]) bedeutet PbD, Datenschutz bereits bei der Entwicklung von Produkten und Geschäftsmodellen mitzudenken. Das hat den Vorteil, dass nicht im Nachgang kostspielige Anpassungen vorgenommen werden müssen. Stattdessen können durch die Beachtung der PbD-Prinzipien bereits im Designprozess datenschutzrechtliche Vorgaben deutlich leichter und mit geringerem Aufwand implementiert werden.

Präzise formuliert ist PbD also ein vorbeugender Ansatz, der versucht, Datenschutzrisiken zu begegnen, bevor sie auftreten. Voraussetzung hierfür ist jedoch, dass das Management Datenschutz- und Privatsphäre-Themen ernst nimmt und im Unternehmen verankert. Grundsätzlich sollen nur so viele Daten gesammelt werden, wie für einen vorher bestimmten Zweck nötig sind. Privacy ist mithin schon in der Entwurfs- und Architekturphase eines Systems, Produkts oder Geschäftsmodells zu berücksichtigen. Dazu betrachtet PbD Daten aus einer Lifecycle-Perspektive. Das heißt, ihre Prinzipien sollen von (der Planung) der Datenerhebung über die Verarbeitung und Speicherung der Daten bis hin zu ihrer letztlichen Löschung angewendet werden. Auf diese Weise werden Wege gefunden, widerstreitende Interessen wie Sicherheit und Datenschutz zu vereinen, um dadurch im Idealfall ein System zu schaffen, in dem sich beispielsweise Cybersecurity- und Datenschutzkomponenten gegenseitig stärken. Auch eine transparente und nachvollziehbare Außenkommunikation über die Datenverarbeitung im Unternehmen ist Teil von PbD. Der Leitgedanke des Konzepts ist der Respekt vor der Privatsphäre des Endnutzers.

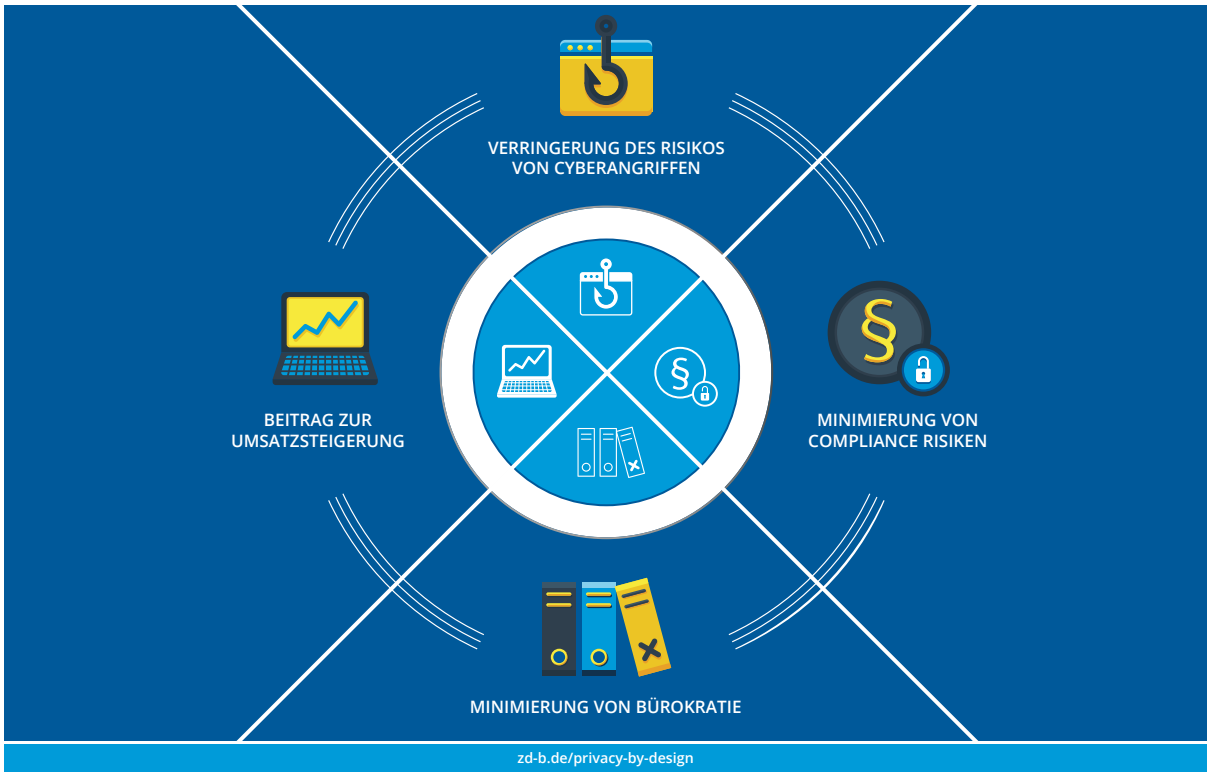
Das Konzept von Privacy by Design nach Ann Cavoukian umfasst sieben grundlegende Prinzipien [3]:

1. Proaktiv, nicht reaktiv; Vorbeugen statt heilen
2. Privatsphäre als Standardeinstellung
3. Eingebauter Datenschutz – von Anfang an
4. Volle Funktionalität – Mehrwert statt Nullsummenspiel
5. Durchgängige Sicherheit – über die gesamte Daten-Lebensdauer
6. Sichtbarkeit und Transparenz – offen gestalten
7. Respekt für die Privatsphäre – vom Nutzer her denken

Wie die Umsetzung von PbD in der Praxis aussehen kann, sei noch an einem Beispiel beschrieben: In der Vergangenheit war es notwendig, dass Sprachassistenten alle an sie gerichteten Wörter aufzeichnen und an den Hersteller übermitteln, damit dort per Abgleich mit großen Datenmengen errechnet werden kann, was diese Wörter bedeuten. Mit heutiger Technologie und Rechenpower kann die Spracherkennung aber direkt auf dem Gerät erfolgen, sodass keine Datenübermittlung der Sprachbefehle mehr notwendig ist. Die Sprachbefehle werden rein lokal verarbeitet und nur das Ergebnis, nicht die Stimme selbst, werden übermittelt, um beispielsweise ein Suchergebnis zurückzuspielen. So kann die Sprachaufzeichnung direkt wieder vom Gerät gelöscht werden, ohne dass eine Datenübermittlung stattfindet. Es hört tatsächlich nur noch der lokale Sprachassistent mit und nicht das Herstellerunternehmen.[1]

1 Mit snips AIR gibt es bereits eine Europäische Firma, die das Konzept einer lokalen Sprachverarbeitung zum Hauptargument für ihr Produkt gemacht hat. (https://air.snips.ai/).

WELCHE VORTEILE HAT PRIVACY BY DESIGN FÜR UNTERNEHMEN?



Mittelbar trägt PbD durch die Minimierung von Risiken[2] und Bürokratie zur Wertschöpfung eines Unternehmens bei. PbD kann jedoch auch als Verkaufsargument genutzt werden und damit unmittelbar beitragen, den Unternehmensumsatz zu steigern. PbD steigert zusätzlich die Widerstandsfähigkeit des Unternehmens gegen Hackerangriffe.

Konkret hat PbD für Unternehmen also folgende Vorteile:

1. Privacy by Design verringert das Risiko von Cybervorfällen

Cybervorfälle, also erfolgreiche Angriffe auf IT-Systeme, werden von Unternehmen nach Betriebsausfällen als das größte und gleichzeitig am meisten unterschätzte Risiko identifiziert [5]. Wobei bei einem Abfluss personenbezogener Daten auch die Aufsichtsbehörden informiert werden müssen.[3]

PbD mildert die Folgen von Hackerangriffen ab, weil sensible Daten nach diesem Konzept entweder gar nicht verarbeitet werden oder nur in aggregierter Form oder auf voneinander abgeschotteten Systemen. Das Risiko eines Totalabflusses von Daten kann damit größtenteils ausgeschlossen werden.

Ein Beispiel: Ein System soll per Gesichtserkennung ermitteln, wie viele Personen sich zu einem gegebenen

Zeitpunkt in einem Raum befinden. Dazu filmen Kameras den Ort des Interesses und schicken den Film an einen zentralen Server im Unternehmen, damit auf den Bildern unterschiedliche Gesichter erkannt und daraus die Summe der Personen berechnet werden kann, die sich in die-

2 Definition von Risiko: Eintrittswahrscheinlichkeit mal Konsequenzen eines Ereignisses. In diesem Sinne wird ein Risiko nicht nur dadurch gesenkt, dass die Eintrittswahrscheinlichkeit verringert wird, sondern auch dadurch, dass man die Schwere der Konsequenzen eines Ereignisses mindert (siehe etwa [4]). Dies ist ein Kernanliegen von PbD.

3 Art. 33 DSGVO: „Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde“

„Wir sind eine Firma, die im Digitalen Raum Vertrauen schaffen will. Daher raten wir unseren Kunden zu Lösungen, die Privacy by Design als zentralen Bestandteil berücksichtigen. Hierzu bieten wir eine breite Palette an leicht zu integrierenden, eleganten Lösungen um Privacy by Design zu einem positiven Merkmal eines jeden Projekts zu machen, nicht zu einer Hürde für unsere Kunden."

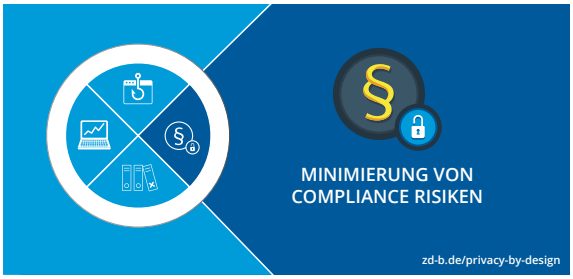
Josef Willkommer, Mitgründer und Geschäftsführer, TechDivision GmbH

sem Raum aufgehalten haben. Gesichtserkennung ist aus Datenschutzperspektive jedoch hochproblematisch. Da heutzutage deutlich mehr Rechenleistung auf geringerem Raum verbaut werden kann, würde dieses System nach den Prinzipien von Privacy by Design wie folgt funktionieren: Die Kamera erkennt die unterschiedlichen Gesichter durch lokal verbaute Software und errechnet daraus die Summe der in einem Raum zu einem gegebenen Zeitpunkt befindlichen Personen. Deren Gesichter werden von der Kamera daraufhin unverzüglich wieder gelöscht, nur die Gesamtzahl der Personen wird an das Unternehmen übermittelt. In diesem Fall ist zur Erfüllung des Zwecks eines Geräts keine Übermittlung sensibler Daten notwendig, weil die Datenverarbeitung lokal abläuft und nur die für die Bereitstellung des Produkts notwendigen aggregierten Daten weitergegeben werden. Dies senkt die Wahrscheinlichkeit und insbesondere die Schwere der Auswirkungen von Cybervorfällen: Die kritischen Filmdaten werden ja bereits in der Kamera gelöscht und können nicht entwendet werden.

2. Privacy by Design minimiert Compliance-Risiken

Compliance-Prozesse sollen sicherstellen, dass sich Unternehmen gemäß gültigem Recht verhalten. Hier wird in Umfragen das Thema Datenschutz regelmäßig als das größte Risiko angegeben [6]. PbD ist eine effektive Strategie, um dieses Risiko zu minimieren. Denn PbD umzusetzen bedeutet, sich bereits im Zuge der Entwicklung von Produkten und Geschäftsmodellen Gedanken darüber zu machen, welche personenbezogenen Daten für welche Zwecke benötigt und erhoben werden. Dies führt zu einem genaueren Bild der Compliance-relevanten Datenflüsse im Unternehmen. Der PbD-Grundsatz der Datenminimierung bewirkt, dass nur geschäftlich notwendige Daten verarbeitet werden, was abermals die Übersichtlichkeit der Datenflüsse erhöht.

Die bei der Umsetzung von PbD entstehende Dokumentation dient dann auch dazu, Compliance so nachzuweisen, wie in Art. 24 I DSGVO gefordert.



3. Privacy by Design minimiert Bürokratie

Ein durchgängiger PbD-Ansatz führt auch zur Verringerung der mit Datenschutz verbundenen Bürokratie.

Unternehmen müssen laut Art. 5 II sowie Art. 24 I DSGVO jede Form der Datenverarbeitung dokumentieren und auch nachweisen, dass die Verarbeitung rechtmäßig erfolgt. In das Verzeichnis der Verarbeitungstätigkeiten müssen die Zwecke und Rechtsgrundlagen der Verarbeitung, die Kategorien der personenbezogenen Daten und betroffenen Personen, die Kategorien etwaiger Empfänger von Daten, falls diese weitergeleitet werden, die Fristen für die Löschung der Daten und gegebenenfalls noch weitere Angaben aufgenommen werden. Zudem muss dokumentiert werden, dass bei der Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen getroffen wurden, die geeignet sind, die Vorgaben der DSGVO zu erfüllen. Die Eignung der technischen und organisatorischen Maßnahmen bemisst sich dabei primär am Risiko der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen im Sinne der oben getroffenen Risikodefinition. Diese umfassenden Dokumentations- und Rechenschaftspflichten ändern die Kosten-Nutzen-Rechnung einer Datenverarbeitung.

„Durch Privacy by Design zukunftssicher Daten verarbeiten - nicht nur hinsichtlich der DSGVO eine gute Idee. Um welche Entwicklung oder Produkt es sich auch handelt - eine durchdachte Integration von Datenschutz in Arbeitsabläufe senkt Risiken und steigert die Effektivität."

Denis Nolte, safectory GmbH

Ist PbD im Unternehmen allerdings bereits in die Prozesse implementiert, entsteht die geforderte DSGVO-Dokumentation sozusagen „nebenbei" in der Planungsphase und verursacht somit weniger Aufwand.

Eine Anekdote aus der Entwicklungsabteilung einer deutschen Games-Entwicklungsfirma veranschaulicht den Abbau des Bürokratieaufwands: Die Entwickler bekamen zur Auflage, für jedwedes personenbezogene Datum, das sie in ihrem Modul verarbeiten wollten, eine kurze Begründung zu schreiben. Um das Verfassen dieser Notiz zu vermeiden, wurde in der Folge deutlich öfter auf lokal im jeweiligen Modul schon vorhandene Daten zugegriffen und damit die Komplexität und Abhängigkeiten des Codes verringert. Als Nebeneffekt entstehen auf diese Weise schlankere Produkte, die leichter und kostengünstiger zu warten sind.

4. Privacy by Design kann zur Umsatzsteigerung beitragen

PbD hat nicht nur, wie oben skizziert, durch die Senkung von Risiken und Bürokratie einen mittelbaren Einfluss auf die Wertschöpfung eines Unternehmens, sondern kann auch direkt zur Umsatzsteigerung beitragen:

Im Business-to-Business-Geschäft (B2B) ist es gang und gäbe, dass bei bestimmten Produkten und Dienstleistungen nachgewiesen werden muss, dass der Datenschutz sichergestellt ist. Unter anderem durch Art. 5, 24 und 26 DSGVO sind Anbieter (auch Auftragsverarbeiter, gemeinsam Verantwortliche) gesetzlich dazu verpflichtet, die Einhaltung von Datenschutzbestimmungen nachweisen zu können. Dies trifft dann auch Anbieter, die als Zulieferer Systemkomponenten verkaufen, die im Endprodukt personenbezogene Daten verarbeiten.

Ein weit verbreitetes Beispiel hierfür sind Anbieter von Newsletter-Software – hier erwartet jede Firma, welche die Software zum Versand nutzt, eine strikte und dokumentierte Einhaltung der DSGVO, so dass sichergestellt ist, dass Kundendaten nicht in falsche Hände geraten.[4]

Im Business-to-Customer-Geschäft (B2C) lässt sich die häufig gehörte Ankündigung *„Der Schutz Ihrer Daten ist für uns von größter Bedeutung"* durch den Einsatz von PbD glaubhaft untermauern. Größeres Verbrauchervertrauen äußert sich dann in einer stärkeren Kundenbindung. Dass Privacy ein Wettbewerbsvorteil sein kann, wird schon seit Langem betont [7]. Momentan erlebt diese Argumentation auch unter dem Titel „Corporate Digital Responsibility" (CDR) eine Renaissance in Deutschland. Zwar bedeutet CDR mehr als Datenschutz, aber Privacy stellt eine der wichtigsten Säulen jeder CDR-Strategie dar.[5] Immer mehr Unternehmen positionieren sich daher unter der Überschrift CDR, und auch die Politik hat das Thema für sich entdeckt [8]. Gerade in einem Land wie Deutschland mit seiner starken Datenschutztradition lassen sich Geschäftsmodelle rund um das Thema Privacy leichter entwickeln als andernorts.

Schließlich bringt PbD Unternehmen dazu, sich mit der wichtigsten Frage des Informationszeitalters zu konfrontieren: Welche Daten müssen wir heute erheben, damit unser Geschäftsmodell auch morgen noch nachhaltig ist? Ausgangspunkt ist, dass laut DSGVO schon bei der Datenerhebung dem Kunden gegenüber alle Zwecke der Datenverarbeitung angegeben werden müssen (Art. 5 I DSGVO, „Zweckbindung"). Auf diese Weise müssen sich Unternehmen vorab intensiv mit künftigen Angeboten und Geschäftsmodellen auseinandersetzen und sichern damit ihre Umsätze. Mit so viel Voraussicht kommen dann sogar Privacy-freundliche Big-Data-Geschäftsmodelle [9] in Frage.

4 Die Anbieter werben dann oft offensiv mit „DSGVO-konformes E-Mail-Marketing". Marketingfirmen, die sich schon seit Jahren um ein Einwilligungs-Management bemüht haben, mussten durch die DSGVO nicht viel an ihrer Funktionalität ändern.

5 Die Themenplattform Verbraucherbelange wird 2019 ein Whitepaper zu Digital Corporate Responsibility veröffentlichen.

WELCHE VORTEILE HAT PRIVACY BY DESIGN FÜR VERBRAUCHER*INNEN?

Digitale Produkte und Dienstleistungen basieren oftmals auf der Auswertung personenbezogener Daten, die von und über ihre Nutzer*innen generiert werden. Diese Daten können zusammengeführt und verarbeitet werden, um Angebote zu personalisieren und zu individualisieren. Das geschieht mittels Algorithmen und im Regelfall ohne menschliche Zwischeninstanz. Verbraucher*innen stehen im Zuge dieser Entwicklung vor neuen Herausforderungen: Denn aus den Spuren, die sie in digitalen Diensten hinterlassen, können Rückschlüsse über ihr künftiges Verhalten gezogen werden.

Durch eigene Erfahrungen mit personalisierten Preisen beim Online-Einkauf, gefühlte Manipulation durch Werbeansprachen oder berufliche Rückmeldungen auf private Posts in sozialen Netzwerken hat sich bei vielen Verbraucher*innen längst ein Bewusstsein dafür ausgebildet, dass Daten, die sie im Internet von sich preisgeben, ihr Leben beeinflussen – auch mit negativen Folgen.

Immer mehr Verbraucher*innen wünschen sich deshalb eine Kontrollmöglichkeit über die Art und Weise, wie mit ihren digitalen Profilen und den daraus entstehenden Prognosen verfahren wird, und Transparenz darüber, aus welchen Datenquellen diese entstehen.

Privacy by Design verspricht nun, den seitens der Verbraucher*innen bestehenden Unsicherheiten mit drei Grundsätzen zu begegnen: bessere Information, mehr Kontrolle und konsequente Datenbeschränkung.

1. Privacy by Design gibt Verbraucher*innen bessere Informationen

PbD beinhaltet eine bessere Sichtbarkeit und Transparenz von Datenverarbeitungen, sie umfasst also tatsächlich verständliche Informationen darüber, was mit personenbezogenen Daten geschieht, wofür sie verarbeitet und wie lange sie gespeichert werden. Dafür kann es dann nötig sein, grafische Kommunikationsmetaphern zu entwickeln. Insgesamt geht das Informationsprinzip von PbD sogar über die datenbezogenen Transparenzanforderungen der DSGVO hinaus. Für Unternehmen bedeutet das im Endeffekt auch, dass sie ihr Geschäftsmodell so klar beschreiben müssen, dass sich potenzielle Kund*innen bewusst dafür oder dagegen entscheiden können.

2. Privacy by Design gibt Verbraucher*innen mehr Kontrolle

PbD-Ansätze gehen mit mehr Kontrolle über die Verarbeitung personenbezogener Daten einher. Verbraucher*innen können detailliert entscheiden, welche ihrer Daten für welchen Zweck verwendet werden dürfen – und sie können die Verwendung dann auch nachvollziehen. Als Werkzeug dafür beginnen sich Privacy Dashboards durchzusetzen, welche die erteilten Einwilligungen anzeigen und es erlauben, diese zu ändern und zu widerrufen. Die Umsetzung des Privacy-Schutzziels Intervenierbarkeit **[10]** hat zur Folge, dass Unternehmen in ihre IT-Systeme Abstraktionsschichten einbauen, die es nicht nur den hausinternen Ingenieuren sondern auch den Kund*innen erlauben, auf verschiedenen Ebenen in die Datenverarbeitung einzugreifen. Als Nebeneffekt behalten damit Menschen die letztlichen Steuermöglichkeiten über künftige volldigitale Entscheidungsprozesse und Infrastrukturen.

3. Privacy by Design stellt sicher, dass nur wirklich notwendige Daten verarbeitet werden

Wie oben ausgeführt, ist es ein Prinzip von PbD, sich schon sehr früh im Entwicklungsprozess Gedanken darüber zu machen, welche Daten für welche Funktionalität benötigt werden. Als Ergebnis werden in den Produkten nur diejenigen Daten verarbeitet, die für die Funktionalität notwendig sind. Juristisch ist dies gespiegelt in einer strengen Zweckbindung der Daten und technisch beispielsweise mit Löschroutinen zum aktiven Vergessen unnötiger Daten. Durch PbD-Prozesse sorgen Unternehmen dafür, dass die Zweckbindung auch von ihren Verarbeitungsdienstleister*innen und -partner*innen minutiös eingehalten wird. Bei Unternehmen, die durchgehend auf PbD setzen, können Verbraucher*innen also davon ausgehen, dass diese ihre Zusagen zur Datenverwendung strikt in allen Teilbereichen und IT-Systemen durchsetzen.

Dieser Dreiklang aus Information, Kontrolle und Datenbeschränkung führt dazu, dass Verbraucher*innen die Übersicht darüber behalten, wo welche Eingriffe in ihre Privatsphäre stattfinden, und sie können informiert entscheiden, welche Daten sie zu welchen Zwecken preisgeben möchten. Mittelfristig werden Verbraucher*innen dann solche Produkte und Dienstleistungen nachfragen, die ihnen über PbD die Hoheit über ihre Daten geben. Immer mehr Unternehmen[6] bieten beispielsweise gegen eine monatliche Gebühr E-Mail-Dienste ohne Erhebung von persönlichen Daten und ohne Tracking-Tools an und positionieren sich damit gegen das noch dominierende Geschäftsmodell, bei dem Verbraucher*innen für E-Mail-Dienste mit ihren Daten „bezahlen".

FAZIT

PbD ist nicht nur rechtlich geboten, es rechnet sich auch für Unternehmen, indem Cyber- und Compliance-Risiken gesenkt und Datenschutz-Bürokratie minimiert wird. Außerdem kann ein PbD-Ansatz sowohl im B2B-, als auch im B2C-Bereich zur Umsatzsteigerung beitragen. Für die Umsetzung von Privacy by Design stehen vermehrt Verfahren, Privacy Patterns und Technologien bereit (siehe Anhang) - Unternehmen können sich so an erprobten Best Practices orientieren.

Verbraucher*innen erhalten durch PbD bessere Informationen und mehr Kontrolle über die Verarbeitung ihrer personenbezogenen Daten. Es werden nur noch die personenbezogenen Daten erhoben und verarbeitet, die tatsächlich zur Erbringung einer Dienstleistung oder für ein Produkt benötigt werden. In diesem Sinne stellt die Verwendung von Privacy by Design eine Win-win-Situation für Wirtschaft und Verbraucher*innen dar. In den Worten von Ann Cavoukian [3]: *„Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum ‚win-win' manner"*.

6 Zwei dieser privatsphäre-freundlichen E-Mail-Anbieter aus Deutschland sind Posteo.de und Mailbox.org.

ANHANG: PRIVACY BY DESIGN UMSETZEN – STRATEGIEN, PRIVACY PATTERNS UND PRIVACY ENHANCING TECHNOLOGIES

Aus der wissenschaftlichen Entstehungsgeschichte von PbD gibt es einen großen Fundus an Literatur, die Vorgehensweisen und konkrete Technologien beschreibt, um PbD zu implementieren. Dieser Fundus bildet ein solides Fundament, um die rechtlichen Anforderungen zu erfüllen.

Der Weg in die Umsetzung wurde 2014 von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) beschrieben. In ihrem Bericht „Privacy and Data Protection by Design – from policy to engineering" [11] skizziert sie ein Top-down-Verfahren mit zunehmend konkreten Verfahrensebenen, mit denen PbD im Unternehmen sowie seinen Produkten und Services implementiert werden kann:

Auf der Ebene der **Designstrategien** werden grundlegende Entscheidungen bezüglich des Privacy Designs eines Systems getroffen. Hier werden bestimmte Ziele festgelegt, die das System erfüllen soll. So ein Ziel kann zum Beispiel lauten, dass grundsätzlich so wenig Daten wie möglich erhoben und verarbeitet werden sollen, oder Datensätze, wenn möglich, immer getrennt voneinander gespeichert und verarbeitet werden müssen. Im Bericht werden die acht Strategien aufgeteilt in technisch-datenzentrierte und in management-prozessbezogene.

Die zweite Ebene stellen **Privatsphäre-Entwurfsmuster** (engl.: Privacy Patterns) dar. Hier werden die vormals abstrakten Strategien in einzelne Ingenieurs-Kochrezepte heruntergebrochen, um die Komplexität weiter zu reduzieren. Ausgehend davon, welches der in der Designstrategie festgelegten Ziele umgesetzt werden soll, sowie abhängig von den Rahmenbedingungen des (technischen) Datenflusses, wird beschrieben, welche Architektur oder welcher Algorithmus eingesetzt werden kann. Sollen beispielsweise so wenig Daten wie möglich erhoben werden, kann dies dadurch erreicht werden, dass vor der Datenerhebung präzise festgelegt wird, welche Daten benötigt werden. Sind manche Daten nur für bestimmte Subsysteme relevant, kann von vorneherein sichergestellt werden, dass nur diese Subsysteme Zugriff auf die Daten erhalten. Die umfangreichste, öffentlich zugängliche Sammlung an Privacy Patterns findet sich auf der Webseite privacypatterns.org der UC Berkeley School of Information.[7]

Die dritte Ebene umfasst schließlich die zahlreichen **Privacy Enhancing Technologies** (PETs), also konkrete, bereits implementierte Technologien, mit denen Privacy Patterns umgesetzt werden. Dies können zum Beispiel[8] bestimmte Verschlüsselungs- oder Anonymisierungsprogramme sein. Welche PETs jeweils anzuwenden sind, ergibt sich teilweise aus den Designentscheidungen, die auf den oberen Ebenen getroffen wurden.

Technologieseitig ein vielversprechendes Vorhaben ist das Projekt AppPets, das zwischen Februar 2016 und Januar 2019 vom Bundesministerium für Bildung und Forschung (BMBF) mit dem Ziel gefördert wurde, die Umsetzung von technischem Datenschutz in mobilen Anwendungen zu erleichtern.[9] In den auf der Projektwebseite aufgeführten Publikationen werden zahlreiche Umsetzungsmöglichkeiten von PbD für mobile Anwendungen beschrieben.

Sowohl Privacy Patterns als auch Best Practices für häufige Geschäftsprozesse werden aufbereitet auf einer Webseite zur Verfügung stehen, die das Zentrum Digitalisierung.Bayern gerade im Rahmen eines Projekts mit dem Bayerischen Ministerium für Umwelt und Verbraucherschutz einrichtet.

Grundsätzlich impliziert Privacy by Design, dass die Privatsphäre der Nutzer*innen betreffende Entscheidungen früh in der Produktentwicklung bedacht werden. Auch bereits existierende Systeme können im Nachhinein Privacy-optimiert werden. So zeigte sich beispielsweise in einer Versuchsreihe zur Verschlüsselung von Suchanfragen in Web Search Engines im Rahmen einer Promotion an der Universität Passau, dass bestehende Algorithmen so abgeändert werden konnten, dass die Privatsphäre der Nutzer*innen besser geschützt wird. [12]

7 Sammlung von Privacy Patterns: https://privacypatterns.org
8 Viele Privacy Patterns und PETs nennt beispielsweise der ENISA-Bericht [11].
9 Das Projekt AppPets: http://app-pets.org/

ÜBER DIE AUTOREN

Themenplattform Verbraucherbelange

Diese Publikation ist in der ZD.B-Themenplattform (TP) Verbraucherbelange entstanden. Die beiden Koordinatoren der Plattform, Christian Thiel und Dominik Golle, haben in ihrer Arbeit die Relevanz von Privacy by Design erlebt und zusammen mit Manfred Broy in diesem Whitepaper die Argumente für PbD zusammengetragen.

Die Aufgabe der TP Verbraucherbelange ist es, durch einen kontinuierlichen Austausch mit Wissenschaft, Wirtschaft und Verbraucherorganisationen, Verbraucherbelange in der Digitalisierung zu identifizieren, zu antizipieren und praxistaugliche Lösungen zur Stärkung von Verbraucher*innen frühzeitig in digitale Produkte, Dienste und Geschäftsmodelle einzubringen („Verbraucherbelange by Design“).

Dazu fördert die Themenplattform Projekte zur Verbreitung von Privacy Best Practices und von Verbrauchertechnologien, publiziert beispielsweise zu Corporate Digital Responsibility, und konzipiert Workshops und Veranstaltungen, um Wissen zu vermitteln und Verbraucherbelange-Stakeholder – auch in der Politik – zu vernetzen.

Dr. Christian Thiel

Dr. Christian Thiel ist Koordinator der ZD.B-Themenplattform Verbraucherbelange. Er erfasst breit, was sich durch die Digitalisierung an der Stellung des Verbrauchers ändert und unterstützt Unternehmen dabei, verbraucherfreundlicher zu werden.

Die technischen Grundkenntnisse erwarb sich Christian Thiel mit dem Studium der Informatik an der Universität Ulm. In seiner Promotion bis 2010 brachte er Maschinellen Lernverfahren der Künstlichen Intelligenz bei, auch mit Unsicherheit in Daten und Labels umzugehen. Diese Kenntnisse wandte er dann an, um für ein Startup in Passau das Suchmaschinen Keyword Bid Management zu optimieren.

Seit 2011 engagiert sich Christian Thiel in München für den Austausch von Wissenschaft und Wirtschaft: Beim Bavarian Information and Communication Technology Cluster BICCnet war er verantwortlich für die Themen Embedded Systems, Big Data und Internationalisierung. Im Themenbereich Smart Cities leitete er internationale EU-Projekte (FP7, H2020) und positionierte dabei bayerische Kompetenzen international sichtbar. Als einer der Kernautoren der acatech-Studie agendaCPS beschrieb er 2012 die technischen und gesellschaftlichen Voraussetzungen und Herausforderungen von Cyber-Physical Systems.

Dominik Golle

Dominik Golle ist Koordinator der ZD.B-Themenplattform Verbraucherbelange und unterstützt Unternehmen dabei, verbraucherfreundlicher zu werden.

Zudem ist er Datenschutzbeauftragter am ZD.B sowie Gründer und Koordinator des Hertie Network on Digitalization, einer weltweiten Alumnivereinigung der gemeinnützigen Hertie Stiftung zu digitalpolitischen Themen.

Dominik Golle verbrachte sein Studium der Politik- und Verwaltungswissenschaften in Deutschland, Nigeria und Spanien, bevor er 2014 einen Master of Public Policy an der Hertie School of Governance in Berlin absolvierte, wo er sich vorwiegend mit technologiepolitischen Fragestellungen auseinandersetzte. Er arbeitete unter anderem im Business Development der Computer Science Corporation und als Leiter der Unternehmenskommunikation des Start-Ups CitoCode, bevor er als Referent für Wirtschafts- und Forschungskooperationen der TU München von Berlin nach Süden zog.

Prof. Dr. Dr. h.c. Manfred Broy

Prof. Dr. Dr. h.c. Manfred Broy leitete von 1989 bis 2015 als ordentlicher Professor für Informatik am Institut für Informatik der Technischen Universität München den Lehrstuhl Software & Systems Engineering. Seine Forschung zielt auf die Beherrschung der Evolution leistungsstarker Software-Systeme durch den Einsatz wohldurchdachter Prozesse und Modelle, langlebiger flexibler Softwarearchitekturen und moderner Werkzeuge auf Basis mathematisch und logisch fundierter Methoden. Er gründete 2009 das Forschungsinstitut für angewandte Forschungstechnik fortiss. Durch die unter der Leitung von Manfred Broy erarbeitete acatech-Studie agendaCPS zu Cyber-Physical Systems wurden maßgebliche Initiativen auf nationaler Ebene wie Industrie 4.0 angestoßen.

Von 2016 bis April 2019 baute er als Gründungspräsident das Zentrum Digitalisierung.Bayern auf. Neben dem Transfer Wissenschaft - Wirtschaft war ihm dabei stets ein Anliegen, immer wieder den Menschen in den Mittelpunkt zu stellen, dem die Digitalisierung dienen muss.

LITERATURVERZEICHNIS

1 Maher, Heidi: „Privacy By Design Is Important For Every Area Of Your Business“, Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/04/10/privacy-by-design-is-important-for-every-area-of-your-business/ (abgerufen am: 7.11.2018)

2 Europäische Union (Hrsg.): „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“, 2016.

3 Cavoukian, Ann: „Privacy by Design – The 7 Foundational Principles“. Information and Privacy Commissioner of Ontario, 2010.

4 Goddard Space Flight Center und NASA (Hrsg.): „Goddart Technical Standard: Risk Management Reporting“, 2009.

5 Allianz Global Corporate & Specialty SE (Hrsg.): „Allianz Risk Barometer 2018 – die größten Geschäftsrisiken 2018“. Januar 2018.

6 Potinecke, Harald/ Teicke, Tobias/Block, Florian: „CMS Compliance Barometer 2017“, 2017.

7 Hoffman, David: „Privacy Is a Business Opportunity“. Harvard Business Review, 18. April 2014.

8 Bundesministerium der Justiz und für Verbraucherschutz: „Digitalisierung verantwortungsvoll gestalten: Corporate Digital Responsibility-Initiative legt erste Arbeitsergebnisse vor“. Oktober 2018. https://www.bmjv.de/SharedDocs/Artikel/DE/2018/100818_CDR.html (abgerufen am: 23.10.2018)

9 D’Acquisto, Giuseppe/Domingo-Ferrer, Josep/Kikiras, Panayiotis/ Torra, Vicenç/de Montjoye, Yves-Alexandre/ Bourka, Athena: „Privacy by design in big data“. Heraklion: European Union Agency for Network and Information Security ENISA, 2015.

10 Hansen, Marit/Thiel, Christian: „Cyber-Physical Systems und Privatsphärenschutz“. in: Datenschutz Datensicherheit – DuD, Bd. 36, Nr. 1, S. 26–30, Januar 2012.

11 Domingo-Ferrer, Joseph/Hansen, Marit/Hoepman, Jaap-Henk/Le Métayer, Daniel/Tirtea, Rodica/Schiffner, Stefan/Danezis, George „Privacy and Data Protection by Design – from policy to engineering“, Heraklion: European Union Agency for Network and Information Security ENISA, 2014. https://publications.europa.eu/en/publication-detail/-/publication/6548a14b-9863-410d-a8a6-c15a0137d281 (abgerufen am 16.9.2019)

12 Petit, Albin: „Introducing Privacy in Current Web Search Engines“, PhD-Thesis, Universität Passau 2017.

IMPRESSUM

Herausgeber
Zentrum Digitalisierung.Bayern
Lichtenbergstr. 8
85748 Garching
+49 89 2488071 00
E-Mail: verbraucherbelange@zd-b.de
https://zentrum-digitalisierung.bayern/verbraucherbelange

Autoren
Dr. Christian Thiel, christian.thiel@zd-b.de
Dominik Golle, dominik.golle@zd-b.de
Prof. Dr. Dr. h.c. Manfred Broy

Editorinnen
Dr. Nina Höhne
Dr. Kathrin Barbara Zimmer

Bilder
Infografiken: bilderbuero, Hamburg
Autorenfotos: blende11 Fotografen

Datum
Oktober 2019

Version
1.0

ZD.B ZENTRUM DIGITALISIERUNG. BAYERN

Zentrum Digitalisierung.Bayern
Lichtenbergstr. 8
85748 Garching
+49 89 2488071 00
E-Mail: verbraucherbelange@zd-b.de
www.zentrum-digitalisierung.bayern