1135063265 / Shutterstock

Kundenvertrauen erhöhen mit Privacy by Design

von Dr. Christian Thiel, Dominik Golle und Dennis Appelt

Was sind Privacy Patterns und wie nutze ich sie

Kunden vertrauen mir ihre personenbezogenen Daten an – und die möchte ich schützen. Privacy by Design ist ein Framework, dass mir dabei hilft, den Überblick zu behalten, und so auch Compliance- und IT-Sicherheitsrisiken zu senken. Die Privacy Patterns geben dabei konkrete Hinweise, wie Funktionalitäten datensparsam aber mit voller Funktionalität umgesetzt werden können. Angewendet auf eine Wordpress-Webseite sorgen unsere Privacy by Design Tipps für eine schön kurze Datenschutzerklärung.

Als Unternehmen kommt man nicht umhin, personenbezogene Daten zu verarbeiten. Sei es, weil Kunden sich auf der eigenen Webseite informieren, weil man bestellte Produkte ausliefert oder Profile für die Nutzung der eigenen Onlineservices angelegt werden. Und natürlich will man seine Kunden und ihre Daten schützen.

Der Schutz der Kundendaten steht auf zwei Säulen: IT-Sicherheit und Datenschutz. Cybersecurity findet meist schon ausreichend Beachtung. Gepusht durch die DSGVO und Kundenwünsche wird vermehrt auch Datenschutz berücksichtigt. Sogar ein über das gesetzlich geforderte Maß hinaus gehender Privatsphären-Schutz taucht langsam auf den Wunschzetteln der Geschäftsführung auf.

Eine Strategie, sich dem Thema Privacy und Datenschutz integriert zu nähern, ist Privacy by Design (PbD) – ein Framework aus Prinzipien, Strategien und „Kochrezepten" für Softwareentwickler. Solche „Privacy Patterns" ermöglichen es, uneingeschränkt funktionale Produkte zu erstellen und dabei trotzdem die Privatsphäre der Kunden über den gesamten Lebenszyklus hinweg zu schützen.

Wesentlich ist es nun, die Vorteile von datensparsamen und sicheren Produkten auch zu kommunizieren, und dadurch in Kundenbindung und Marktanteile zu übersetzen. Neben der Aufnahme der neuen Qualitätsmerkmale in die Standardkommunikation kann dies auch über spezielle Transparenz-Tools wie den Data Process Modeler geschehen. Mit diesen Tools kann einfach dargestellt werden, welche Kundendaten für welche Zwecke genutzt werden müssen.

> "Privacy by Design Is Important for Every Area of Your Business"
> Heidi Maher, Forbes Technology Council 2018

Das ist Privacy by Design

Das Konzept Privacy by Design wurde in den neunziger Jahren durch Ann Cavoukian geprägt, der ehemaligen Datenschutzbeauftragten der kanadischen Provinz Ontario. Entsprechend der von Cavoukian formulierten Prinzipien ist Privacy by Design darauf ausgerichtet, Datenschutz bereits bei der Entwicklung von Produkten und Geschäftsmodellen mitzudenken. Die abstrakten Prinzipien wurden in Zusammenarbeit mit der Europäischen Cybersicherheits-Agentur ENISA später in acht Privacy by Design Strategien konkretisiert:

1. Minimieren

Es werden nur so viele personenbezogene Daten gesammelt, wie unbedingt notwendig sind, um die Funktionalität zu erreichen. Man überlegt sich, ob die Datensammlung angemessen ist und ob es Wege gibt, auch mit weniger Daten ans Ziel zu kommen. Ein Beispiel wäre das Löschen von Metadaten, die von Geräten automatisch mitgesendet werden, wie beispielsweise den Standortdaten in Handyfotos.

2. Verstecken

Personenbezogene Daten und auch deren Querbeziehungen werden vor neugierigen Augen verborgen. Ziel ist es, die Hürden für eine Verkettung der Daten höher zu setzen, dadurch können die Daten weniger einfach missbraucht werden. Eine solche erwünschte „Nichtverkettbarkeit", also dass Daten nur mit unverhältnismäßig hohem Aufwand für einen anderen Zweck genutzt werden können, ist ein guter Filter für technische Entscheidungen: Die Verwendung von eindeutigen Kennungen wie beispielsweise IP-Adressen soll vermieden werden.

3. Verteilen

Hierzu werden personenbezogene Daten auf verteilten Systemen verarbeitet und in getrennten Bereichen gespeichert – sofern irgend möglich. Ziel ist es, eine Profilbildung zu verhindern. Ein Verteilen begünstigt auch die Zweckbindung: Bewerbungsdaten werden etwa in einer Datenbank gespeichert, auf die nur die Personalabteilung Zugriff hat.

4. Zusammenfassen

Kritische Daten werden nur zusammengefasst verwendet – und zwar so weit aggregiert und abstrahiert, dass sie für den Zweck gerade noch tauglich sind. Beispielsweise interessiert beim Verteilen von Zeitungen nicht, wer wann besucht wurde, sondern nur, ob alle Abonnenten eine Zeitung bekommen haben – die Informationen können zu einem einfachen „Ja“ oder „Nein“ zusammengefasst werden.

5. Informieren

Die Strategie „Informieren“ verfolgt als Ziel die Transparenz. Betroffene Personen müssen angemessen über die Verarbeitung sie betreffender Daten informiert werden: welche Daten von wem und wozu verarbeitet werden. Eine moderne Umsetzungsvariante ist ein Datenschutz-Cockpit, das Datenverarbeitungen übersichtlich und für Kunden verständlich darstellt – auch hier ist der Data Process Modeler hilfreich.

6. Kontrolle überlassen

Man überlässt den Kunden die Kontrolle, wie ihre Daten verarbeitet werden. Dabei kann detailliert eingestellt werden, welche Daten für welchen Zweck genutzt werden. Insgesamt sorgt die Strategie für Intervenierbarkeit – die Kontrolle über die Datenverarbeitung bleibt beim Betroffe-

1089401852 / Shutterstock

nen. Dies ist besonders wichtig im Angesicht der fortschreitenden Verbreitung von KI-getriebenen Blackbox-Lösungen – ohne Intervenierbarkeit würde hier dem Menschen das Heft aus der Hand genommen.

7. Durchsetzen

Eine fixierte Datenschutzrichtlinie darf nicht nur im Schrank liegen, sondern muss auch durchgesetzt werden. Zur Durchsetzung gehört das Einführen von technischen und organisatorischen Maßnahmen (TOMs), welche die Datenschutzregelungen konkret umsetzen. Neben grundlegenden TOMs wie der Zutrittskontrolle gehört dazu beispielsweise auch die Kontrolle von Zulieferern: Kann etwa der Sensorlieferant weiter auf die Geräte zugreifen, nachdem er sie installiert hat?

8. Nachweisen

Die Einhaltung von Bestimmungen und Richtlinien muss auch nachgewiesen werden können – und die entsprechende Dokumentation nicht erst anlässlich eines Audits entstehen. Zum Nachweis gehören ein Trail zwischen Datenschutz-Anforderungen und Produkt-Code, beispielsweise auf Code-Kommentar-Ebene und Zugriffs-Protokolle.

Konkrete Umsetzung mit Privacy Patterns

Die Privacy Patterns dienen dazu, die eher abstrakten Strategien in einzelne „Kochrezepte“ herunterzubrechen. Abhängig von den Rahmenbedingungen des (technischen) Datenflusses und den in der Privacystrategie festgelegten Zielen beschreibt das Pattern, welche Architektur oder welcher Algorithmus eingesetzt werden kann.

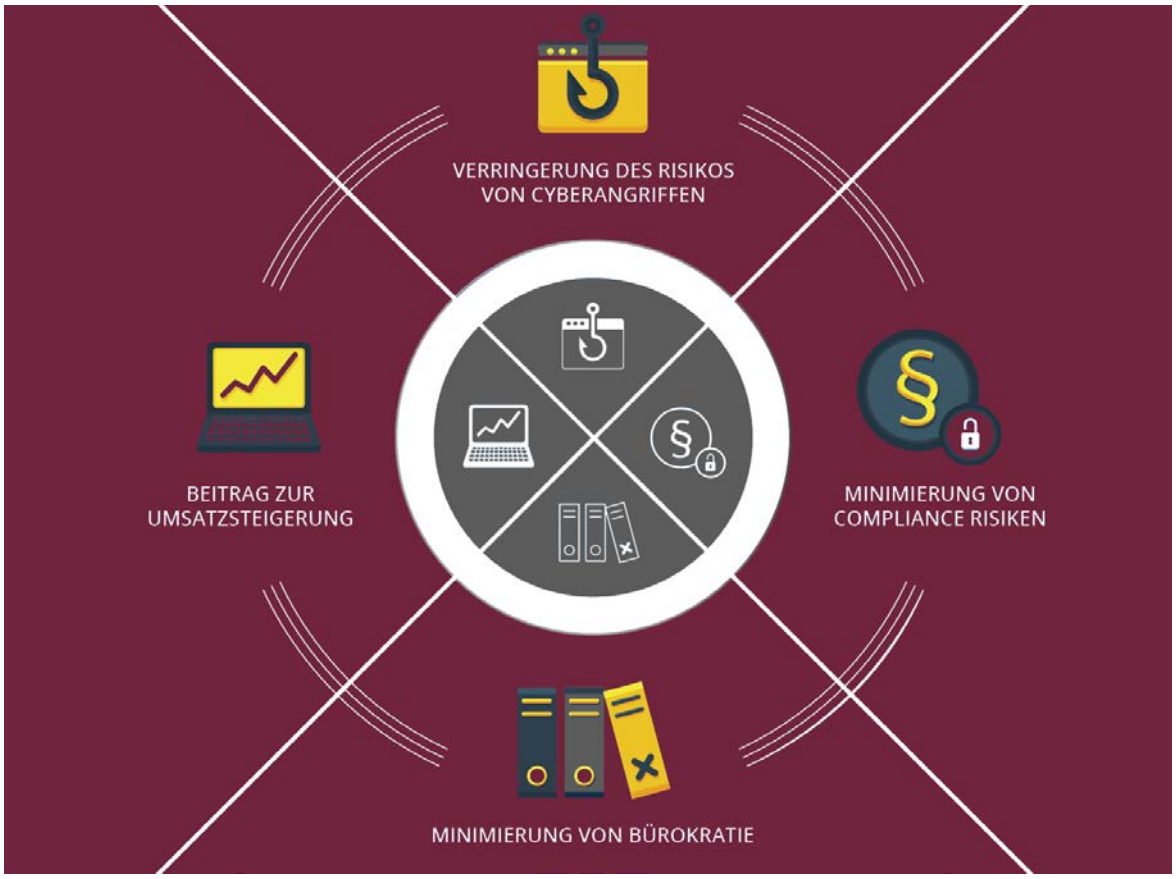
Die größte deutschsprachige Sammlung von Privacy Patterns findet sich auf https://Privacyby-Design.Digital. Die einzelnen Patterns sind dort gegliedert beschrieben: Der Kontext beschreibt die Rahmenbedingungen, unter welchen das Pattern typischerweise eingesetzt wird. Danach wird ausgeführt, welches Privacy-Problem überhaupt zu lösen ist, welche Faktoren dabei eine Rolle spielen, und welche Konflikte und Ungleichgewichte dabei auftreten. Konkret wird in der Lösung dann gezeigt, mit welchem Ansatz oder welcher Strategie eine Datenschutz-Herausforderung aufgelöst werden kann. Mit den Beispielen bekommt man ein Gefühl dafür, in welchem Kontext die Lösung nützlich sein kann und wo sie bereits produktiv eingesetzt wird. Da Patterns meist nicht allein verwendet, sondern häufig kombiniert werden, sind verwandte Patterns zum Weiterlesen verlinkt.

Die beliebtesten Patterns auf der Webseite sind derzeit:

- „Situationsbezogene Datenschutzhinweise“
- „Unsichtbare Metadaten löschen“
- „Verschlüsselung auf Nutzerseite”

Vier Gründe, Privacy by Design im Unternehmen einzusetzen

Privacy by Design (PbD) bei sich im Unternehmen umzusetzen, bringt einige handfeste Vorteile:



Die vier zentralen Vorteile von Privacy by Design

1. Verringerung des Risikos von Cybervorfällen

PbD mildert die Folgen von Cybervorfällen ab, weil sensible Daten nach diesem Konzept entweder gar nicht, nur in aggregierter Form oder auf voneinander abgeschotteten Systemen verarbeitet werden. Das Risiko eines Totalabflusses von Daten kann so größtenteils ausgeschlossen werden. Wenn ein Abflussereignis eintritt, kann sehr schnell und verlässlich festgestellt werden, welche Daten es betrifft – das ermöglichte eine zielgerichtete Reaktion und Kommunikation, auch in Richtung der Aufsichtsbehörden.

2. Minimierung von Compliancerisiken

PbD ist eine effektive Strategie, um die mit dem Aspekt des Datenschutzes verbundenen Compliance-Risiken zu minimieren. Im Rahmen von PbD gilt es sich bereits während des Entwicklungsprozesses 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. Zudem bewirkt der PbD-Grundsatz der Datenminimierung, dass nur geschäftlich notwendige Daten verarbeitet werden. Dies erhöht abermals die Übersichtlichkeit der Datenflüsse.

3. Minimierung von Bürokratie

Ein durchgängiger PbD-Ansatz führt zur Verringerung der mit Datenschutz verbundenen Bürokratie, da die geforderte DSGVO-Dokumentation gewissermaßen „nebenbei“ in der Planungsphase entsteht. Dadurch entfällt der große Aufwand, die interne IT-Infrastruktur nachträglich verstehen und aus Datenschutzsicht nochmals dokumentieren zu müssen.

4. Beitrag zur Umsatzsteigerung

Die Anwendung von PbD hat durch die Senkung von Risiken und Bürokratie nicht nur einen mittelbaren Einfluss auf die Wertschöpfung eines Unternehmens, sondern kann auch direkt zur Umsatzsteigerung beitragen. Einerseits ist es im B2B-Geschäft gang und gäbe, dass bei bestimmten Produkten und Dienstleistungen eine Datenschutz Compliance nachgewiesen werden muss (vgl. DSGVO Art. 5, 24 und 26). Andererseits lassen sich im B2C-Geschäft die häufig beschworenen Datenschutzbemühungen der Unternehmen durch den Einsatz von Privacy by Design glaubhaft untermauern und ein erhöhtes Vertrauen der Verbraucher äußert sich dann in einer stärkeren Kundenbindung.

> „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 und nicht zu einer Hürde für unsere Kunden.“
>
> Josef Willkommer, Mitgründer und Geschäftsführer, TechDivision GmbH

Webseiten mit Privacy by Design

Viele Produkte haben ein Gegenstück im Netz – und Privacy by Design lässt sich gut für Webseiten einsetzen. Eine hilfreiche Anlaufstelle zur praktischen Umsetzung ist die Top 10 „Privacy Risks“ der OWASP-Foundation, die dieses Jahr in einer aktualisierten Version erscheint.

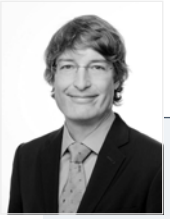
Unsere eigenen Erfahrungen mit dem Privacy-Härten einer Wordpress-Webpräsenz waren sehr positiv. Von normalen Besuchern werden seit dem Launch von PrivacybyDesign.digital keinerlei personenbezogene Daten erfasst – was die Datenschutzerklärung erheblich verkürzt und vereinfacht hat.

Die zentralen technischen Kniffe für mehr Privacy auf der Wordpress-Webseite waren:

- Technisch frühestmögliches Abschneiden der IP-Adresse – auch in den Logfiles beim Hoster
- Webfonts und JS-Frameworks auf dem eigenen Server vorhalten
- Ausschalten von Kommentarfunktion, Emojis, Gravatar-Bildern, und Youtube/Twitter/Facebook-Einbettungen
- Verzicht auf Plugins, die ihre Funktionalität über externe Server erbringen – leider ein Großteil der Formularplugins
- Verwendung eines rein lokalen Statistiktools, beispielsweise Matomo

Investition in die Zukunft

Mit Privacy by Design bekommt man ein Instrument, um auf Management- und Entwicklerebene bewusster mit Kundendaten umzugehen. Auch helfen die Privacy Patterns bei der praktischen Umsetzung in der Prozess- und Produktentwicklung. Sich mit Privacy by Design Gedanken über eine Datenstrategie zu machen ist zudem eine direkte Investition in die Zukunft!



AUTOR

Dr. Christian Thiel

Koordinator der Themenplattform „Verbraucherbelange in der Digitalisierung“ bei Bayern Innovativ

Christian Thiel erfasst breit, was sich durch die Digitalisierung an der Stellung des Verbrauchers ändert und unterstützt Unternehmen dabei, verbraucherfreundlicher zu werden. Ein Werkzeug ist dabei die Integration von Privacy by Design in Unternehmensabläufe – siehe sein Whitepaper zu Privacy by Design.

In seiner Promotion brachte er Maschinellen Lernverfahren der Künstlichen Intelligenz bei, mit Unsicherheit in Daten und Labels umzugehen. Eine Fähigkeit, die ihm jetzt hilft, verschiedene menschliche Player und ihre Interessen für gemeinsame Projekte zusammen zu bringen.

https://www.bayern-innovativ.de/verbraucherbelange
https://www.xing.com/profile/Christian_Thiel17
https://www.linkedin.com/in/dr-christian-thiel-4a454619a/ (Profil nur nach Anmeldung sichtbar)

AUTOR

Dominik Golle

Koordinator der Themenplattform „Verbraucherbelange in der Digitalisierung“ bei Bayern Innovativ

Dominik Golle ist seit 10 Jahren an der Schnittstelle von (digitaler) Technologie und Gesellschaft tätig. In seiner derzeitigen Rolle entwickelt er Strategien und Werkzeuge für eine verbraucherfreundliche Digitalisierung, wie zum Beispiel die free an open source Software Data Process Modeler für mehr Transparenz von Datenverarbeitungen in Unternehmen.

Er absolvierte einen Master of Public Policy an der Hertie School of Governance und hat in Konstanz, Abuja, Barcelona und Berlin studiert.

https://www.bayern-innovativ.de/verbraucherbelange
https://www.linkedin.com/in/dominikgolle

AUTOR

Dennis Appelt

Werkstudent der Themenplattform “Verbraucherbelange in der Digitalisierung“ bei Bayern Innovativ | Masterstudent am Munich Center for Technology in Society der TU München

Dennis Appelt beschäftigt sich breit mit den Auswirkungen von Technologie auf unsere Gesellschaft. Neben der Digitalisierung und der Softwareentwicklung liegt sein Fokus auf der Elektromobilität – so entsteht seine Masterarbeit zu den Vorteilen und Risiken der Wiederverwendung von bereits benutzten Lithium-Ionen-Batterien. Seine Erfahrungen als Ingenieur helfen dabei, die technischen Hintergründe und die Sicht der Entwickelnden miteinzubeziehen.

https://www.bayern-innovativ.de/verbraucherbelange
https://www.linkedin.com/in/denapp (Profil nur nach Anmeldung sichtbar)