FZI

Fraunhofer IOSB

Fraunhofer IPA

Privacy by Design (PbD) Leitfaden für Mensch-Roboter-Kooperation

des Kooperationsprojekts

CyberProtect

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND WOHNUNGSBAU

Gefördert vom Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg

Aktenzeichen Zuwendungsbescheid:
3-4332.62-FZI/53

Änderungshistorie			
Rev.	Datum	Beschreibung	Autor
0.1	01.07.19	Struktur erstellt und abgestimmt	Erik Krempel
0.2	14.08.19	Kapitel 2	Erik Krempel
0.3	10.12.19	Kapitel 3	Erik Krempel
0.4	12.12.19	Kapitel 4	Erik Krempel
0.5	08.01.20	Redaktionelle Überarbeitung	Erik Krempel, Pascal Birnstill

I. Inhalt

II. Abkürzungsverzeichnis

DSGVO	(Europäische) Datenschutz-Grundverordnung
PbD	Privacy by Design
Req	Requirement; engl. Für Anforderung

I. Einleitung

Mit dem Inkrafttreten der Europäischen Datenschutzgrundverordnung (DSGVO) hat das Thema Datenschutz viel Aufmerksamkeit gewonnen. Gleichzeitig ist der Trend zu beobachten, dass mit jedem Entwicklungszyklus einer Technologie diese deutlich mehr Informationen über sich selbst und ihre Umwelt verarbeitet. Noch vor 20 Jahren hatte ein Auto fast keine Informationen über seine Außenwelt. Heute sind schon weit vor der Oberklasse Sensoren verbaut, die Verkehrszeichen erkennen oder die Aufmerksamkeit des Fahrers überwachen. Diese beiden Entwicklungen zusammen bedeuten, dass heute in viel mehr Bereichen über das Thema Datenschutz nachgedacht werden muss.

Die industrielle Produktion ist einer dieser neuen Bereiche. Mit dem zunehmenden Einsatz von Robotern und einer steigenden Individualisierung der Prozesse steigt die Menge der verarbeiteten Daten. Gerade dann, wenn Mensch und Roboter zusammen arbeiten reicht es nicht mehr aus nur den Roboter zu überwachen, sondern das System braucht eine Erfassung der Menschen in der Produktion. Gerade für Bereiche in denen es bisher wenig Erfahrung über die Folgen der Verarbeitung personenbezogener Daten gibt, fordert die DSGVO den Einsatz von Privacy by Design (PbD). Dies stellt Entwickler und Anwender vor große Herausforderungen. Datenschutz ist für sie eine neue Herausforderung und gleichzeitig ist PbD selbst für etablierte Technologien nicht selbsterklärend. Da kein standardisiertes Vorgehen existiert um PbD umzusetzen, ist der Erfolg stark von der Erfahrung der Anwender abhängig.

An dieser Stelle setzt das vorliegende Dokument an. Es erklärt zuerst die Grundprinzipien von PbD und zeigt anschließend an Beispielen wie es in der Produktion eingesetzt werden kann. Eine Anwendung wird betrachtet und untersucht welche funktionalen und nicht funktionalen Anforderungen daraus entstehen. Danach wird im Systemdesign ein System entworfen, dass alle gestellten Anforderungen mit einem Maximum an Datenschutz umsetzt.

II. Anforderungsanalyse

Aufgabe der Anforderungsanalyse ist es, all diese Anforderungen zu sammeln und für ein nachfolgendes Systemdesign bereitzustellen. Das sind sowohl die funktionalen Anforderungen, die sich aus den technischen Bausteinen einer Technologie ergeben, als auch funktionale Anforderungen, die sich aus begleitenden Anforderungen, etwa vorgeschriebenen Standards zur Produktsicherheit, ergeben. Ein Beispiel dafür wäre ein Notausschalter der eine Anlage in einen sicheren Zustand führt.

Daneben existieren verschiedene Quellen für nichtfunktionale Anforderungen die ebenfalls im Systemdesign berücksichtigt werden müssen. Mögliche Quellen sind

rechtliche Vorgaben, IT-Sicherheit oder auch Privacy by Design, was wiederum durch eine rechtliche Vorgabe in der DSGVO motiviert ist.

Dieses Dokument geht schwerpunktmäßig auf die Integration von Anforderungen aus Privacy by Design ein. Das Vorgehen ist auch dann anwendbar, wenn weitere nichtfunktionale Anforderungen beachtet werden müssen.

Funktionale Anforderungen

Funktionale Anforderungen definieren, welche konkreten Ziele und Funktionen das System erreichen soll. Diese Anforderungen sind spezifisch für jedes System und nur beschränkt auf andere Systeme zu übertragen.

Privacy by Design

Das erstmals 2009 von Ann Cavoukian veröffentlichte Privacy by Design beschreibt, wie allgemein Systeme ausgestaltet sein sollen, die personenbezogenen Daten verarbeiteten [CAV09]. Betrachtet man PbD genauer wird schnell klar, dass die sieben Prinzipien eher einen ideellen Endzustand als einen strukturierten Weg dahin aufzeigen. Weiter wird klar, dass es für Systeme erdacht wurde, denen sich die betroffenen Personen freiwillig und selbstbestimmt aussetzen, wie es für eine Webseite der Fall wäre. Ist dies nicht der Fall kann PbD zwar weiterhin angewendet werden, erfordert dann aber weiteres Hintergrundwissen zu Datenschutzgesetzen, um zu einsetzbaren Ergebnissen zu führen. Die sieben Prinzipien von PbD werden hier kurz vorgestellt und diskutiert. In zwei anschließenden Beispielen wird dann verdeutlicht, wie sich PbD auf ein Systemdesign auswirkt.

PbD1: Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe

> *„Der Privacy by Design (PbD) Ansatz ist von proaktiven statt reaktiven Maßnahmen geprägt. Er sieht in die Privatsphäre vordringende Ereignisse voraus und verhindert sie, bevor sie geschehen können. Privacy by Design kommt zum Einsatz, bevor die Risiken für den Datenschutz aufgetreten sind, es bietet keine Abhilfe im Falle von datenschutzrechtlichen Verletzungen, wenn sie erst einmal eingetreten sind – es verhindert vielmehr deren Auftreten. Kurz gesagt, Privacy by Design verhindert bereits, dass Fakten geschaffen werden.“*

PbD2: Datenschutz als Standardeinstellung

> *„Wir können uns alle einer Sache gewiss sein – die Standardeinstellungen sind entscheidend! Privacy by Design soll den größtmöglichen Schutz der Privatsphäre bringen, indem sichergestellt wird, dass personenbezogene Daten automatisch in jedem IT-System und bei allen Geschäftspraktiken geschützt werden. Wenn eine Person nichts unternimmt, bleibt der Schutz ihrer Privatsphäre immer noch intakt. Einzelpersonen sind nicht gefordert, selbst etwas für den Schutz ihrer Privatsphäre zu unternehmen – der Schutz ist bereits systemimmanent, als Standardeinstellung.“*

Anmerkung: PbD2 definiert die Anforderung, dass die Standardeinstellung eines Systems immer den maximalen Datenschutz erfüllt. Es ist zulässig, dass ein System auf Benutzerwunsch mehr seiner persönlichen Daten erfasst oder diese auch mit anderen teilt. Dies muss aber auf ausdrücklichen Wunsch des Nutzers erfolgen.

PbD3: Der Datenschutz ist in das Design eingebettet

> *„Privacy by Design ist in das Design und die Architektur von IT-Systemen und Geschäftspraktiken eingebettet. Es wird nicht nach dem Vorfall als add-on eingebaut. Das Ergebnis ist, dass der Datenschutz eine wesentliche Komponente der Kernfunktionalität wird. Datenschutz ist ein wesentlicher Bestandteil des Systems, ohne Abstriche bei der Funktionalität.“*

Anmerkung: PbD3 wird in meistens schon alleine dadurch umgesetzt, dass PbD während des Systemdesigns beachtet wird. Wenn Datenschutz erst nachträglich in ein System integriert wird, ist der Aufwand höher.

PbD4: Volle Funktionalität – eine Positivsumme, keine Nullsumme

> *„Privacy by Design will allen berechtigten Interessen und Zielen entgegenkommen, und zwar durch eine Positivsumme, die ein zufriedenstellendes Ergebnis für beide Seiten erzielt, und nicht durch einen veralteten Nullsummenansatz, bei dem schließlich unnötige Kompromisse erforderlich werden. Durch Privacy by Design wird die Vortäuschung falscher Dichotomien wie Datenschutz versus Sicherheit vermieden. Privacy by Design zeigt, dass es möglich ist, beides zugleich zu erreichen.“*

Anmerkung: PbD4 ist für das Verständnis und Erfüllung komplizierteste der sieben Grundprinzipien. Es fordert, dass alle berechtigten Interessen durch ein System erfüllt werden. Das sind insbesondere das Interesse der Systemanbieter, der maximale Funktionalität erreichen möchte, und der Dienstnehmer, der maximalen Schutz für seine persönlichen Daten fordert. Der Vorwand, dass man entweder Funktionalität oder Datenschutz erreichen kann (Nullsummenspiel) darf nicht dazu genutzt werden, Datenschutzanforderungen nicht zu erfüllen. In der Praxis sind erfahrene technische Datenschützer in der Lage diesen anscheinenden Konflikt aufzulösen und sowohl Datenschutz als auch Funktionalität zu erreichen (Positivsumme).

PbD5: Durchgängige Sicherheit – Schutz während des gesamten Lebenszyklus

> *„Nachdem Privacy by Design vor der Ersterfassung der Information in das System „eingebettet“ wurde, erstreckt sich dessen Wirkung auf den gesamten Lebenszyklus der Daten - starke Sicherheitsmaßnahmen sind für den Datenschutz unerlässlich, und zwar von Anfang bis Ende. Dadurch wird erreicht, dass alle Daten sicher gespeichert und am Ende des Prozesses sicher und rechtzeitig vernichtet werden. So sorgt Privacy by Design von der Wiege bis zur Bahre durchgängig für eine sichere Datenverarbeitung.“*

Anmerkung: PbD5 fordert eine konsequente Umsetzung von IT-Sicherheitsmaßnahmen zum Schutz der Daten vor versehentlichen Verlust, unerlaubtem Zugriff oder unbeabsichtigten Veränderungen.

PbD6: Sichtbarkeit und Transparenz – Für Offenheit sorgen

> *„Privacy by Design will allen Beteiligten die Sicherheit geben, dass das System unabhängig von Geschäftspraktiken oder Technologien wirklich die angekündigten Maßnahmen und Ziele verfolgt und sich einer unabhängigen Prüfung unterwirft. Seine einzelnen Komponenten und Verfahren bleiben sichtbar und transparent, und zwar gleichermaßen für Nutzer und Anbieter. Denken Sie daran, Vertrauen ist gut, Kontrolle ist besser.“*

PbD7: Die Wahrung der Privatsphäre der Nutzer – Für eine nutzerzentrierte Gestaltung sorgen

> *„Privacy by Design erfordert vor allem von den Architekten und Betreibern (von IT-Systemen), dass für sie die Interessen der Einzelpersonen an erster Stelle stehen. Sie [die Systeme] bieten Maßnahmen wie strenge datenschutzfreundliche Voreinstellungen und angemessene Benachrichtigungen an und eröffnen benutzerfreundliche Optionen. Sie sorgen für eine nutzerzentrierte Gestaltung.“*

Anmerkung: PbD7 fordert eine nutzerzentrierte Gestaltung der Technologie. Eine klare Trennung zwischen den Begriffen Nutzern und Betreibern ist hierbei wichtig. Die Nutzer in unserem Umfeld sind die Betroffenen, also die Werker. Es geht darum das System nach ihren Wünschen und Vorstellungen auszugestalten. Insbesondere geht es auch darum, ihre Daten vor dem Zugriff durch das Unternehmen als Betreiber zu schützen.

III. Beispiel 1: Generisches Assistenzsystem in der Produktion

Die in CyberProtect betrachteten Szenarien stellen aus Sicht der der Mensch-Roboter-Interaktion völlig unterschiedliche Herausforderungen. Aus dem Blickwinkel von Privacy erlauben sie jedoch, sie in ein abstraktes Szenario zu überführen. Dieses ist in Abbildung 1 abgebildet und ist stellvertretend für viele Systeme zu sehen.

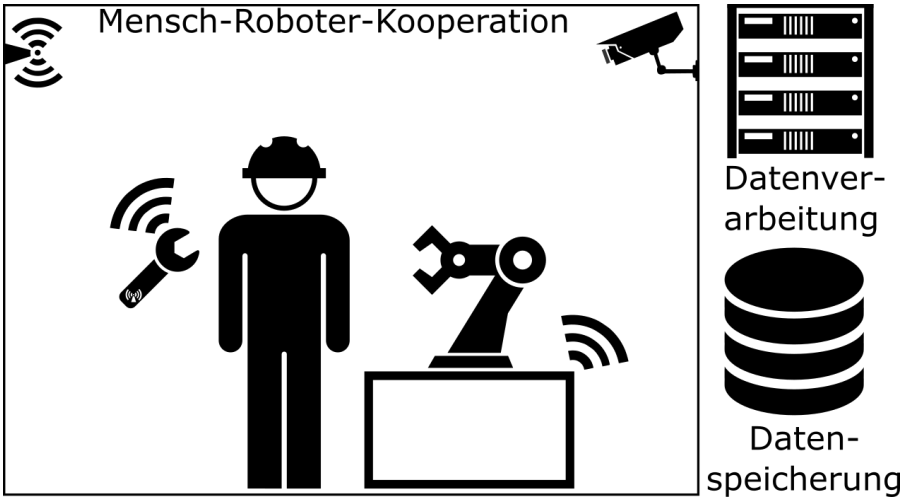

Abbildung 1: Systemmodell der Mensch-Roboter-Kooperation

Ein Werker arbeitet zusammen mit einem Roboter an einem Arbeitsplatz. Es sind keine trennenden Bauteile wie Gitter oder Zäune vorhanden womit vom Roboter eine mögliche Gefährdung für den Werker ausgeht. Ob Werker und Roboter gemeinsam an einem Werkstück arbeiten (Kollaboration), beide wechselseitig Aufgaben am selben Werkstück ausführen (Kooperation) oder völlig eigenständige Arbeiten ausführen, ist für das Szenario nicht relevant. Wichtig ist jedoch, dass beide multisensoriell erfasst werden. Das kann beispielsweise eine Kamera sein, die sicherstellt, dass kein Mensch im Arbeitsbereich des Roboters ist. Genauso können aber auch einzelne Werkzeuge, beispielsweise eine Drehmomentschrauber, drahtlos Informationen über die ausgeführten Arbeiten versenden.

Absehbar ist zudem, dass zukünftig Roboter nicht nur fest montiert, sondern auch als bewegliche Akteure auftreten. Mit Autopickern, die benötige Bauteile aus dem Lager direkt bis zum Werker transportieren, sehen wir diese Entwicklung bereits heute. Für die mobilen Anwendungen müssen drahtlose Verfahren zur Kommunikation mit den Robotern verwendet werden. Dies stellt zusätzliche Anforderungen an Safety, Security und Privacy und wird deshalb in das Szenario aufgenommen.

Funktionale Anforderungen

Da keine reale Anwendung, sondern das abstrakte Systemmodell betrachtet wird, erscheint es auf den ersten Blick sinnvoll, sich nur auf die nichtfunktionalen Anforderungen aus Privacy by Design zu konzentrieren. Gleichzeitig besteht die Möglichkeit, dass funktionale und nichtfunktionale Anforderungen im Konflikt zueinanderstehen.

Die funktionalen Anforderungen folgen dabei aus den grundlegenden Funktionalitäten des abstrakten Systemmodells. So ist klar, dass ein System das einem Werker in der Produktion assistiert, diesen und die Handlungen erkennen muss (Req1). Dies ist

Grundvoraussetzung dafür, dass ein Assistenzsystem situationsabhängige und individuelle Assistenzfunktionen anbieten kann (Req2).

Anforderungen aus Privacy by Design

Obwohl das Systemmodell sehr abstrakt ist, lassen sich hier bereits sehr eindeutige Anforderungen an die Ausgestaltung ableiten. Systeme, die personenbezogene Daten verarbeiten, sollen immer eine Zweckbindung umsetzen und somit verhindern, dass Daten außerhalb des ursprünglich definierten Zweckes verwendet werden (Req03). Personenbezogene Daten dürfen nur dann mit Dritten geteilt werden, wenn die betroffene Person dies wünscht (Req04). Jede Verarbeitung von personenbezogenen Daten muss für die betroffenen Personen transparent sein (Req05) und muss auf das Minimum an Daten reduziert sein (Req06).

Da das betrachtete Szenario lediglich von einer Verarbeitung der Daten für Assistenzfunktionen ausgeht, wird eine Speicherung ausgeschlossen (Req07). Typisch für PbD ist weiterhin, dass Datenschutz proaktiv verfolgt wird (Req08) und dadurch tief in das Design eines Systems einfließt (Req09). Req08 und Req09 ergeben sich dabei automatisch dadurch, dass PbD in der Entwicklung genutzt wird. Sie werden nur zur Vollständigkeit in die Liste der Anforderungen aufgenommen.

Übersicht Anforderungen

- Req01: Das Assistenzsystem muss den Benutzer und seine Handlungen erkennen.
- Req02: Das System muss situationsabhängige Assistenzfunktionen bieten.
- Req03: Das System muss eine Zweckbindung erzwingen. Insbesondere muss verhindert werden, dass es zur Mitarbeiterüberwachung missbraucht wird.
- Req04: Ohne direkten Wunsch der Betroffenen dürfen Echtzeitdaten das System nicht verlassen.
- Req05: Das System muss für alle Betroffenen einen hohen Level an Transparenz bereitstellen.
- Req06: Das System muss die Erhebung und Verarbeitung personenbezogener Daten minimieren.
- Req07: Assistenzsysteme sind als reine Livesysteme zu gestalten. Es werden keine Daten gespeichert.
- Req08: Das System muss einen proaktiven Ansatz für Datenschutz verfolgen.
- Req09: Datenschutz muss tief in das Design des Systems eingebettet sein.

Systemdesign

Das nachfolgende Systemdesign stellt eine Beispielarchitektur für ein Assistenzsystem in der Produktion dar, das die gesammelten funktionalen und nichtfunktionalen Anforderungen in einem System entworfen nach Privacy by Design umsetzt. Es dient lediglich zur Orientierung. Andere mögliche Umsetzungen für die gelisteten Anforderungen sind denkbar und es kann weiterhin nicht garantiert werden, dass das beschriebene Design direkt in die Anwendung übertragen werden kann.

Im Betrieb erkennt das System Benutzer und ihre Handlungen multisensoriell (Req01). Diese Datenverarbeitung bildet die Grundlage, um eine situationsabhängige Assistenz bieten zu können (Req02).

Die Erfassung der Daten erfolgt dabei immer anlassbezogen und ist für die Benutzer einfach über entsprechende Hinweise am Gerät erkennbar (Req05). Werden für bestimmte Situationen Teile oder alle der verfügbaren Sensordaten nicht benötigt, werden diese auch nicht erhoben (Req06). Die Daten aller Sensoren werden als Livedaten genutzt. Sie werden erfasst, direkt ausgewertet und nicht gespeichert (Req07). Eine Weiterleitung der Livedaten an weitere Systeme findet nicht statt (Req04). Ebenso gibt es neben der Assistenzfunktion keine weitere Nutzung der erfassten Daten (Req01).

Das vorgeschlagene Assistenzsystem zeigt eine mögliche Verarbeitungskette für Daten auf. Dabei war Privacy by Design als Quelle für nichtfunktionale Anforderungen direkt im Systemdesign eingebettet (Req09). Dies stellt eine proaktive Betrachtung des Datenschutzes sicher (Req08).

IV. Beispiel 2: QSelect

Das zweite Beispiel QSelect orientiert sich an einer typischen Qualitätskontrolle in der Produktion. Hierzu wird ein Werkstück an einem Arbeitsplatz auf Fehler kontrolliert. QSelect verbaut einen augensicheren Laserpointer, mit dem Prüfer Fehlerpositionen intuitiv anleuchten und damit markieren können. Eine Sensoreinheit, die über dem Bauteil angebracht wird, misst in Echtzeit die Laserpunktposition und speichert anvisierte Fehlerpunkte als 3D-Koordinate digital ab. Die Interaktion erfolgt dabei über eine Projekten die mittels eines Beamers direkt auf das Bauteil projiziert wird.

Nach der eigentlichen Qualitätskontrolle geht das Bauteil an einen zweiten Arbeitsplatz zur Ausbesserung. Hierfür werden die in der Qualitätskontrolle erfassten Fehler auf das Bauteil projektiert. Die Ausbesserung der Fehler durch einen Werker soll per Video dokumentiert und gespeichert werden.

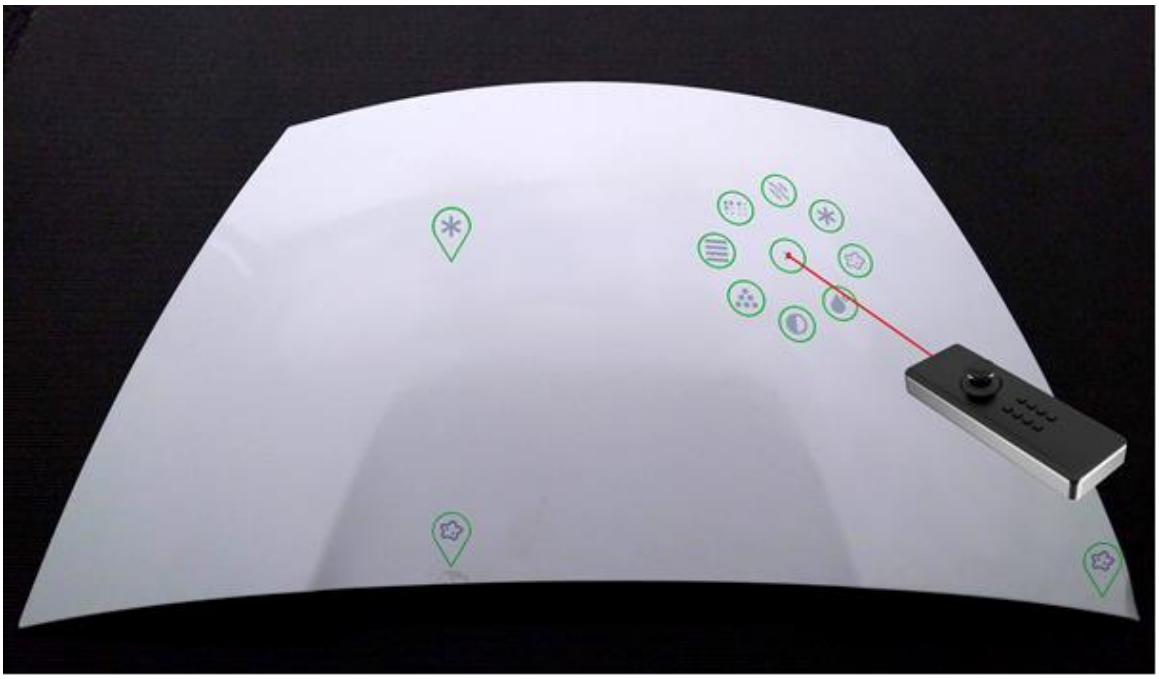

Abbildung 2: QSelect bei der Fehlermarkierung

Funktionale Anforderungen

Die Anforderungen aus technischer Sicht sind in diesem Beispiel schon sehr viel konkreter als in Beispiel 1 und werden verkürzt dargestellt.

In der Qualitätskontrolle ist eine Erfassung des Bauteils, und des Laserpointers (Req01) notwendig. Weiter muss die Interaktionsoberfläche korrekt auf das Bauteil projiziert werden (Req02). Markierte Fehler werden im System gespeichert (Req03).

In der Ausbesserung muss ebenfalls das Bauteil erkannt und darauf die Interaktionsfläche projiziert werden. Weiter müssen die Fehler geladen und projiziert

werden (Req04). Durchgeführte Ausbesserungen sollen mittels einer über dem Bauteil positionierten Kamera erfasst und gespeichert werden (Req05). Dabei ist es unvermeidlich, dass auch der durchführende Mitarbeiter von der Kamera beobachtet wird.

Anforderungen aus Privacy by Design

Das zweite Beispiel wurde absichtlich so ausgewählt, dass es kritischere Bereiche im Datenschutz betrifft. Hier entstehen potentielle Konflikte mit den technischen Anforderungen, die anschließend in Systementwurf aufgelöst werden müssen.

Grundsätzlich ist das System nach PbD so zu gestalten, dass eine Zweckbindung erreicht wird (Req06). In diesem Fall ist besonders zu verhindern, dass das System zur Mitarbeiterüberwachung missbraucht wird. Ohne den direkten Wunsch des Mitarbeiters dürfen weder Livedaten (Req07) noch die gespeicherten Daten das System verlassen (Req08). Weiter muss das System ein hohes Maß an Transparenz sicherstellen (Req09). Zusätzlich erfordert PbD, dass die Menge der verarbeiteten personenbezogenen Daten minimal ist (Req10). Wie minimal an dieser Stelle zu interpretieren ist, wird im Systemdesign weiter diskutiert. Klar ist jedoch, dass alle erfassten personenbezogenen Daten durchgehend vor unberechtigtem Zugriff zu schützen sind (Req13).

Ebenfalls direkt aus den sieben Grundprinzipien lassen sich die Anforderungen ableiten, dass das System Datenschutz proaktiv anstrebt (Req11) und dieser im Design des Systems eingebettet ist (Req12). Sie werden nur zur Vollständigkeit in die Liste der Anforderungen aufgenommen.

Dabei ist es für ein erfolgreiches Privacy by Design wichtig, dass nicht Datenschutz gegen Funktionalität getauscht wird, sondern beide Anforderungen gleichberechtigt beachtet und erfüllt werden (Req14).

Übersicht Anforderungen

- Req01: Das Bauteile und die Projektion des Laserpointer auf dem Bauteil werden durch Sensoren erfasst.
- Req02: Die Interaktionsoberfläche wird auf das Bauteil projiziert.
- Req03: Markierte Fehler werden im System gespeichert.
- Req04: In der Fehlerbehandlung werden die zuvor erfassten Fehler auf das Bauteil projiziert.
- Req05: Die Fehlerausbesserung wird mittels gespeichertem Video dokumentiert.
- Req06: Zweckbindung muss erzwungen werden.

- Req07: Ohne direkten Wunsch des Mitarbeiters dürfen Livedaten das System nicht verlassen.
- Req08: Ohne direkten Wunsch des Mitarbeiters dürfen gespeicherter Aufnahmen das System nicht verlassen.
- Req09: Die Datenerfassung muss für die Mitarbeiter transparent sein.
- Req10: Das System muss die Erhebung und Verarbeitung personenbezogener Daten minimieren.
- Req11: Das System muss einen proaktiven Ansatz für Datenschutz verfolgen.
- Req12: Datenschutz muss tief in das Design des Systems eingebettet sein.
- Req13: Personenbezogene Daten sind vor unberechtigtem Zugriff geschützt.
- Req14: Datenschutz und Funktionalität fließen gleichberechtigt in den Systementwurf ein.

Systemdesign

Der hier beschriebene Systementwurf dient als Beispiel und ist eine Art wie die Anforderungen zu erfüllen sind. Die gewählte Umsetzung hat zum Ziel eine mögliche Mitarbeiterüberwachung zu vermeiden und definiert die Kooperation des Mitarbeiters als unumgänglichen Voraussetzung für den Zugriff auf Videos. Je nach Einsatzgebiet können auch andere Lösungen notwendig sein, etwa derart, dass durch das hinzuziehen des Betriebsrats oder einer anderen vertrauenswürdigen Instanz, ein Zugriff ohne Kooperation des Mitarbeiters möglich ist.

Das beschriebene Verfahren in der Qualitätskontrolle kann wie beschrieben umgesetzt werden. Ein Bauteil wird am Arbeitsplatz erfasst und ein Werker markiert darauf Fehler mittels seines Laserpointers (Req01). Die Interaktionsoberfläche für die Fehlermarkierung wird mittels eines Beamers auf das Bauteil projiziert (Req02) und Fehler im System gespeichert (Req03). Zu keinem Zeitpunkt müssen personenbezogene Daten am Arbeitsplatz für die Qualitätskontrolle vom System erfasst werden.

Der Arbeitsplatz zur Fehlerausbesserung wird durch den Entwurf nach Privacy by Design umgestaltet. Auch hier werden die Bauteile durch die Sensoren erfasst (Req01) und die Interaktionsoberfläche (Req02) sowie die zuvor gespeicherten Fehler projiziert (Req04). Größere Änderungen entstehen durch die Anforderung die Ausbesserung mittels Video zu dokumentieren.

Der hier gewählte Weg sieht vor, dass sich ein Werker am Ausbesserungsarbeitsplatz vor Beginn der Arbeiten anmeldet. Dies ist nicht intuitiv, da dadurch mehr personenbezogene Daten verarbeitet werden als zuvor. Die explizite Anmeldung ist der erste Baustein um die Erfassung für den Werker transparent zu machen. Zusätzlich

wird die aktive Aufzeichnung durch einen visuellen Marker dargestellt (Req09). Die explizite Anmeldung erlaubt es weiter die Daten deutlich besser zu schützen als zuvor. Alle erfassten Videodaten werden verschlüsselt gespeichert (Req05). Der Schlüssel hat zwei Teile. Der erste gehört zum Mitarbeiter und der zweite Teil gehört zum Betriebsrat. Dies stellt sicher, dass nur der Werker zusammen mit dem Betriebsrat Zugriff auf die Videos herstellen kann. Somit ist der Werker davor geschützt beispielsweise durch Druck von seinem Vorgesetzten Zugriff auf die Videos zu erlauben. Weiter kann der Betriebsrat alleine auch keinen Zugriff erhalten (Req06, Req08, Req13).

Neben dieser geschützten Speicherung der Ausbesserung kommt es zu keiner weiteren Nutzung oder Teilung der Livedaten (Req07). Um zusätzlich die Menge an personenbezogenen Daten zu minimieren werden im System nicht dauerhaft Videos gespeichert, sondern immer nur dann, wenn aktiv ein Fehler ausgebessert wird. In Umrüstzeiten, wenn kein Werkstück vorhanden ist oder in Pausen findet keine Datenspeicherung statt (Req10).

Dieser Systementwurf stellt sicher, dass gleichzeitig eine Speicherung der Videodaten ermöglicht wird, die Daten aber vor unberechtigtem Zugriff geschützt sind. Er zeigt damit, dass selbst augenscheinliche Widersprüche sich weitgehend auslösen lassen, wenn alle Anforderungen früh und gleichberechtigt im Systementwurf berücksichtigt werden (Req14). Die Maßnahmen zum Datenschutz wurden proaktiv ergriffen (Req11) und somit ist der Datenschutz tief im Design integriert (Req12).

V. Refrenzen

[CAV09] Cavoukian, Ann. "Privacy by design: The 7 foundational principles." Information and Privacy Commissioner of Ontario, Canada (2009).