DIN EN ISO/IEC 29184

DIN

ICS 35.030

Einsprüche bis 2023-01-18

Entwurf

Informationstechnologie – Online-Datenschutzerklärung und Einwilligung (ISO/IEC 29184:2020); Deutsche und Englische Fassung prEN ISO/IEC 29184:2022

Information technology –
Online privacy notices and consent (ISO/IEC 29184:2020);
German and English version prEN ISO/IEC 29184:2022

Technologies de l'information –
Déclarations de confidentialité en ligne et les consentements (ISO/IEC 29184:2020);
Version allemande et anglaise prEN ISO/IEC 29184:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-11-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

— vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;

— oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;

— oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 65 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

Nationales Vorwort

Der Text von ISO/IEC 29184:2020 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 29184:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-14 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 24760	siehe	DIN EN ISO/IEC 24760-1
		DIN EN ISO/IEC 24760-2
		DIN EN ISO/IEC 24760-3
ISO/IEC 27701	siehe	DIN EN ISO/IEC 27701
ISO/IEC 29100	siehe	DIN EN ISO/IEC 29100
ISO/IEC 29151		DIN EN ISO/IEC 29151

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 24760-1, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement — Teil 1: Terminologie und Konzept*

DIN EN ISO/IEC 24760-2, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement — Teil 2: Referenzarchitektur und Anforderungen*

DIN EN ISO/IEC 24760-3, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement — Teil 3: Umsetzung*

DIN EN ISO/IEC 27701, *Sicherheitstechniken — Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz — Anforderungen und Leitlinien*

DIN EN ISO/IEC 29100, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz*

DIN EN ISO/IEC 29151, *Informationstechnik — Sicherheitsverfahren — Leitfaden für den Schutz personenbezogener Daten*

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

– Entwurf –

Dezember 2022

prEN ISO/IEC 29184

Informationstechnologie – Online-Datenschutzerklärung und Einwilligung (ISO/IEC 29184:2020)

Information technology – Online privacy notices and consent (ISO/IEC 29184:2020)

Technologies de l'information – Déclarations de confidentialité en ligne et les consentements (ISO/IEC 29184:2020)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 6
1 Anwendungsbereich 7
2 Normative Verweisungen 7
3 Begriffe 7
4 Symbole und Abkürzungen 8
5 Allgemeine Anforderungen und Empfehlungen 8
5.1 Übergeordnetes Ziel 8
5.2 Benachrichtigung 8
5.2.1 Allgemeines 8
5.2.2 Verpflichtung zur Bereitstellung von Benachrichtigungen 8
5.2.3 Angemessene Formulierung 9
5.2.4 Mehrsprachige Benachrichtigung 9
5.2.5 Angemessener Zeitpunkt 9
5.2.6 Angemessener Ort 10
5.2.7 Angemessene Form 10
5.2.8 Laufende Versionierung und Bezugnahme 11
5.2.9 Barrierefreiheit 11
5.3 Inhalte von Benachrichtigungen 11
5.3.1 Allgemeines 11
5.3.2 Beschreibung des Zwecks 11
5.3.3 Darstellung der Beschreibung des Zwecks 12
5.3.4 Identifizierung der verantwortlichen Stelle 12
5.3.5 PbD-Erhebung 12
5.3.6 Erhebungsverfahren 13
5.3.7 Zeitpunkt und Ort der pbD-Erhebung 14
5.3.8 Nutzungsverfahren 14
5.3.9 Geografischer Standort und zuständiges Rechtssystem bei gespeicherten pbD 14
5.3.10 Übertragung an Dritte 15
5.3.11 Aufbewahrungsdauer 15
5.3.12 Mitwirkung der betroffenen Person 16
5.3.13 Anfragen und Beschwerden 16
5.3.14 Information über Zugang zu den bei der Einwilligung getroffenen Entscheidungen 16
5.3.15 Grundlage für die Verarbeitung 17
5.3.16 Risiken 17
5.4 Einwilligung 18
5.4.1 Allgemeines 18
5.4.2 Identifikation, ob die Einwilligung angemessen ist 18
5.4.3 Informierte und freiwillig erteilte Einwilligung 18
5.4.4 Bereitstellung der Information, welches Konto die betroffene Person verwendet 19
5.4.5 Unabhängigkeit von anderen Einwilligungen 19
5.4.6 Getrennte Einwilligung zu notwendigen und optionalen pbD-Elementen 20
5.4.7 Häufigkeit 20
5.4.8 Rechtzeitigkeit 20
5.5 Änderung der Bedingungen 21
5.5.1 Allgemeines 21
5.5.2 Erneuerungsbenachrichtigung 21
5.5.3 Erneuerung der Einwilligung 21
Anhang A (informativ) Beispiel für eine Benutzungsschnittstelle zur Einholung der Einwilligung einer betroffenen Person auf einem PC oder Smartphone 23

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

A.1 Allgemeines . . . 23
A.2 Beispiele für Benutzungsschnittstellen zur Einholung der anfänglichen Einwilligung auf einem PC oder Smartphone . . . 23
A.2.1 Identifikation, welches Konto die betroffene Person verwendet . . . 23
A.2.2 Reihenfolge der anzuzeigenden Elemente . . . 24
A.2.3 Darstellung der tatsächlichen Werte . . . 27
Anhang B (informativ) Beispiel für eine Einwilligungserklärung oder einen Einwilligungsdatensatz (ANMERKUNG in 5.4.3) . . . 29
B.1 Allgemeine Informationen und Zweck einer Einwilligungserklärung . . . 29
B.2 Inhalt und Format einer Einwilligungserklärung . . . 29
B.2.1 Allgemeines . . . 29
B.2.2 Beispiel einer für Menschen lesbaren Einwilligungserklärung — Einfach . . . 29
Literaturhinweise . . . 32

Bilder

Bild A.1 — Bildschirm für die Auswahl des Kontos . . . 24
Bild A.2 — Benachrichtigung im Tabellenformat . . . 25
Bild A.3 — Fall, in dem die Überschrift weggelassen wurde . . . 26
Bild A.4 — Fall, in dem die Einwilligung abgelehnt wurde . . . 27
Bild A.5 — Darstellung konkreter Werte . . . 28
Bild A.6 — Anzeige eines Beispiels . . . 28
Bild B.1 — Beispiel einer für Menschen lesbaren Einwilligungserklärung — Einfach . . . 30
Bild B.2 — Beispiel für Einzelheiten zu erhobenen Daten und wie die Organisation sie verwendet 31

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

Europäisches Vorwort

Der Text von ISO/IEC 29184:2020 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 29184:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 29184:2020 wurde von CEN als prEN ISO/IEC 29184:2022 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder der IEC-Liste der erhaltenen Patenterklärungen (siehe patents.iec.ch).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection* erarbeitet.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

Einleitung

Aufgrund der immer weiteren Verbreitung von Kommunikationsinfrastrukturen, z. B. privaten Breitband- und globalen Internetverbindungen, und der zunehmenden Nutzung von Smartphones und anderen Geräten (z. B. Wearables), die detailliert Aktivitäten von Personen erfassen, sowie durch verbesserte Fähigkeiten der Informationsverarbeitung wird eine zunehmend umfassendere Erhebung und Analyse von persönlichen Informationen ermöglicht. Solche technologischen Weiterentwicklungen eröffnen Perspektiven für Lebenserleichterungen für Verbraucher, neue Geschäftsmöglichkeiten, attraktivere Dienste und zusätzlichen Mehrwert. Andererseits werden Verbraucher zunehmend datenschutzbewusst und hinterfragen die Datenschutzfolgen, die durch die Erhebung und Nutzung personenbezogener Daten (pbD) durch Online-Dienste entstehen. Diese Kritik ist häufig auf das Fehlen einer eindeutigen Erklärung zurückzuführen, wie die pbD verarbeitet, gespeichert, gepflegt und verwaltet werden.

In diesem Dokument werden Steuerungsmaßnahmen und damit zusammenhängende zusätzliche Informationen für Organisationen festgelegt:

— um die Grundlage zu schaffen, damit Personen, deren pbD erhoben werden, eindeutige und leicht verständliche Informationen darüber erhalten, wie die Organisation diese pbD verarbeitet (z. B. bei der Bereitstellung von Diensten für Verbraucher oder bei einem Beschäftigungsverhältnis); und

— um die Einwilligung der betroffenen Personen auf faire, nachweisbare, transparente, eindeutige und widerrufbare (entziehbare) Weise einzuholen.

Dieses Dokument enthält Einzelheiten zur Umsetzung von zwei Datenschutzprinzipien aus ISO/IEC 29100 (d. h. Prinzip 1: Einwilligung und Wahlfreiheit, Prinzip 7: Offenheit, Transparenz und Benachrichtigung).

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

1 Anwendungsbereich

Dieses Dokument legt Steuerungsmaßnahmen fest, um den Inhalt und die Struktur von Online-Datenschutzerklärungen zu gestalten sowie den Prozess, mit dem die Einwilligung zur Erhebung und Verarbeitung personenbezogener Daten (pbD) von betroffenen Personen eingeholt wird.

Dieses Dokument ist in jedem Online-Kontext anwendbar, in dem eine verantwortliche Stelle oder eine beliebige andere Instanz, die pbD verarbeitet, betroffene Personen über diese Verarbeitung informiert.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 29100 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter http://www.electropedia.org/

3.1
ausdrückliche Einwilligung
die freiwillig erteilte, spezifische und informierte eindeutige Zustimmung der betroffenen Person zur Verarbeitung ihrer pbD, in Form einer bestätigenden Handlung der betroffenen Person, die diese Einwilligung anzeigt

Anmerkung 1 zum Begriff: Die ausdrückliche Einwilligung ist das Ergebnis eines Opt-in.

Anmerkung 2 zum Begriff: Die ausdrückliche Einwilligung kann auch als explizite Einwilligung bezeichnet werden.

BEISPIEL Die Einwilligung wird eingeholt, indem die betroffene Person aufgefordert wird, eine spezifische Handlung im Zusammenhang mit einer Benachrichtigung durchzuführen.

[QUELLE: ISO/IEC 29100:2011, 2.4, modifiziert – die Wörter „in Form einer bestätigenden Handlung der betroffenen Person, die diese Einwilligung anzeigt“ wurden hinzugefügt.]

3.2
Benachrichtigung
Information über die Verarbeitung von pbD

Anmerkung 1 zum Begriff: Wird betroffenen Personen über unterschiedliche Kanäle in prägnanter, transparenter, verständlicher und leicht zugänglicher Form und in klarer und verständlicher Sprache zur Verfügung gestellt.

3.3
pbD-Element
pbD-Kategorie
pbD-Teilinformation
Deskriptor für einen Informationstyp oder einen Satz von Informationstypen

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

4 Symbole und Abkürzungen

JSON	JavaScript Object Notation
PC	Personal Computer
pbD	personenbezogene Daten
XML	Extensible Markup Language

5 Allgemeine Anforderungen und Empfehlungen

5.1 Übergeordnetes Ziel

Das übergeordnete Ziel dieses Dokuments ist es, betroffenen Personen zu ermöglichen, die Folgen einer Verarbeitung von pbD zu verstehen und in Übereinstimmung damit zu handeln; dazu zählen z. B. die Wahrscheinlichkeit und der Schweregrad möglicher Folgen der Verarbeitung sowie direkte und/oder beabsichtigte Folgen der Verarbeitung.

Organisationen, die die Übereinstimmung mit diesem Dokument nachweisen möchten, müssen für jede Steuerungsmaßnahme in Abschnitt 5 dokumentieren:

a) ob die Steuerungsmaßnahme anzuwenden ist;

b) wenn es Begründungen dafür gibt, dass die Steuerungsmaßnahme nicht anzuwenden ist, die Dokumentation und Validierung dieser Begründungen;

c) wie die Umsetzung der Steuerungsmaßnahme überprüft und validiert wird.

5.2 Benachrichtigung

5.2.1 Allgemeines

Ziel: Erforderliche Benachrichtigungen in einer für betroffene Personen angemessenen Sprache zu einem Zeitpunkt zur Verfügung zu stellen, der es den betroffenen Personen ermöglicht, ihre Einwilligung sinnvoll auszuüben, an Stellen, die für die betroffenen Personen leicht zu erkennen sind, und mit Bezugnahmen, die den betroffenen Personen Zugang zu ergänzenden Materialien zur Verfügung stellen, einschließlich früheren Benachrichtigungen und ihrer Beantwortung.

5.2.2 Verpflichtung zur Bereitstellung von Benachrichtigungen

Steuerungsmaßnahme

Die Organisation muss Situationen identifizieren, in denen das Zurverfügungstellen von Benachrichtigungen erforderlich ist, und muss, sofern erforderlich, für die betroffenen Personen eine Benachrichtigung entsprechend 5.3 zur Verfügung stellen.

Zusätzliche Informationen

Die Benachrichtigung sollte allen interessierten Parteien, einschließlich Außenstehenden, Informationen über die Datenschutzpraktiken der Organisation sowie über andere relevante Daten, beispielsweise Kontaktdaten, zur Verfügung stellen, darunter die Identität und offizielle Adresse der verantwortlichen Stelle und Kontaktstellen, von denen betroffene Personen zusätzliche Informationen erhalten können (siehe Anhang A).

Die Anzeige einer visuellen Meldung ist eine Möglichkeit, die Benachrichtigung zur Verfügung zu stellen. Um die Barrierefreiheit für Sehbehinderte sicherzustellen, können entweder Screenreader für visuelle Benachrichtigungen oder direkte akustische Benachrichtigungen zweckmäßig sein. Es können auch andere Arten der Benachrichtigung geeignet sein (siehe 5.2.9).

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

Die Organisation sollte eine Benachrichtigung für betroffene Personen zur Verfügung stellen. Die Benachrichtigung kann unter anderem erforderlich sein, wenn die Organisation die Erhebung neuer pbD plant (von der betroffenen Person oder einer anderen Quelle) oder wenn sie plant, bereits erhobene Daten für neue Zwecke zu verwenden.

5.2.3 Angemessene Formulierung

Steuerungsmaßnahme

Die Organisation muss die Benachrichtigung in einer Form zur Verfügung zu stellen, die eindeutig und für die betroffenen Zielpersonen leicht verständlich ist. Die Benachrichtigung muss leicht lesbar und in einer präzisen Sprache formuliert sein, die eine Person ohne juristische oder technische Ausbildung vernünftigerweise verstehen kann.

Zusätzliche Informationen

Bei der Formulierung der Benachrichtigung sollten bestimmte Kategorien oder Arten von betroffenen Personen berücksichtigt werden (z. B. benachteiligte gesellschaftliche Untergruppen).

5.2.4 Mehrsprachige Benachrichtigung

Steuerungsmaßnahme

Die Organisation muss die Benachrichtigung in der/den Sprache(n) zur Verfügung zu stellen, die den Spracherwartungen der betroffenen Zielpersonen entspricht.

Zusätzliche Informationen

Die Organisation kann der betroffenen Person eine Liste der unterstützten Sprachen in den jeweiligen Sprachen anzeigen und der betroffenen Person die Auswahl der Sprache erlauben. Es ist wichtig, den Namen der Sprache in der jeweiligen Sprache anzuzeigen, da die betroffene Person ihn eventuell nicht erkennen kann, wenn er in einer anderen Sprache angezeigt wird.

Web-Browser ermöglichen die Einstellung der Benutzerpräferenz für eine bevorzugte Sprache; dies kann für diesen Zweck verwendet werden. Es ist aber möglicherweise keine gute Idee, sich allein auf die Sprachpräferenz des Browsers zu verlassen, da die betroffene Person einen gemeinsam genutzten Computer verwenden kann.

5.2.5 Angemessener Zeitpunkt

Steuerungsmaßnahme

Die Organisation muss den geeigneten Zeitpunkt festlegen und dokumentieren (z. B. unmittelbar vor Erhebung der pbD), zu dem die Benachrichtigung der betroffenen Personen erfolgt, wenn die fragliche Aktivität für die Datenschutzinteressen der betroffenen Personen relevant ist.

Zusätzliche Informationen

Wenn eine Organisation für eine betroffene Person eine Benachrichtigung zur Verfügung stellt und dann die pbD zu einem späteren Zeitpunkt erhebt, und in Fällen, in denen die Daten von einer anderen Quelle erhoben werden, kann der Zeitpunkt der Benachrichtigung erheblich vom Zeitpunkt der pbD-Erhebung abweichen.

Die Organisation sollte eine Benachrichtigung zur Verfügung stellen, falls die Verwendung der pbD unerwartete oder bedeutsame Folgen für die betroffene Person haben kann. Wenn eine Organisation beabsichtigt, zusätzliche pbD zu erheben, sollte sie eine weitere Benachrichtigung zur Verfügung stellen.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

5.2.6 Angemessener Ort

Steuerungsmaßnahme

Die Organisation muss Benachrichtigungen in einer für das entsprechende Produkt oder den Dienst angemessenen Form zur Verfügung stellen, sodass betroffene Personen die Benachrichtigungen leicht finden und elektronisch darauf zugreifen können; auch an Online-Stellen.

Zusätzliche Informationen

Zu den angemessenen Online-Stellen können unter anderem Links auf der Web-Startseite oder Zielseite der Organisation, auf der Startseite einer mobilen App, auf Online-Formularen oder in Zugangsportalen gehören.

In manchen Fällen dürfen pbD ohne eine vorherige Interaktion mit der betroffenen Person verarbeitet werden. Aus Sicht der betroffenen Personen kann es tatsächlich sehr schwierig sein, herauszufinden, wer ihre Daten verarbeitet; daher ist es nicht hilfreich, die Datenschutzerklärung nur auf der Website der Organisation anzuzeigen. Es ist nützlich, eine Stelle zur Verfügung zu stellen, wo betroffene Personen die Datenschutzerklärungen solcher Organisationen abrufen können. Falls dies durchführbar und anwendbar ist, sollte die Organisation in Betracht ziehen, ein öffentlich zugängliches gemeinsames Verzeichnis bereitzustellen, wo interessierte Parteien die relevanten Benachrichtigungen einfach finden und darauf zugreifen können.

5.2.7 Angemessene Form

Steuerungsmaßnahme

Die Organisation muss festlegen, wie die Benachrichtigung in Bezug auf den Zeitpunkt der Verarbeitung zur Verfügung gestellt und zugänglich gemacht wird.

Zusätzliche Informationen

Die Organisation kann die Steuerungsmaßnahme mit unterschiedlichen Verfahren umsetzen, darunter mehrschichtige Benachrichtigungen, Dashboards, Just-in-Time-Benachrichtigungen und Icons. Sie kann die Benachrichtigungen auch in einem maschinenlesbaren Format zur Verfügung stellen, sodass die Software für die Anzeige der Benachrichtigungen diese parsen kann, um die Benutzungsschnittstelle zu optimieren und betroffene Personen bei der Entscheidungsfindung zu unterstützen.

Wenn die Organisation die Steuerungsmaßnahme mit einer mehrschichtigen Benachrichtigung umsetzt, sollte die erste Schicht alle Informationen enthalten, die für die betroffene Person unerwartet sind oder bedeutsame Folgen haben können; diese Folgen werden mithilfe der in 5.3.3 beschriebenen Beurteilung bestimmt. Die anderen Schichten sollten über alle Erhebungs- und/oder Verarbeitungsaktivitäten informieren, um der betroffenen Person detaillierte Informationen zu diesen Aktivitäten zur Verfügung zu stellen.

Organisationen sollten die erste Schicht jeder Benachrichtigung so anzeigen, dass die betroffene Person sie so schnell wie möglich lesen kann. Sie sollte nicht mehr als einige wenige Bildschirme umfassen. Aufgrund von Platzbeschränkungen kann es unmöglich sein, den gesamten Inhalt auf einem Bildschirm darzustellen. In diesem Fall sollten Organisationen zuerst die Zusammenfassung anzeigen. Im Kontext von mobilen Geräten und Smartphones wäre es für eine bessere Lesbarkeit sinnvoll, einen „mehrschichtigen Ansatz“ für die Benachrichtigung und Einwilligung zu wählen, mit einem kurzen Text mit Schlüsselinformationen und einem Link zur „Volltextversion“ der Benachrichtigung bzw. Einwilligung.

Wenn Organisationen Elemente der zu erhebenden pbD anzeigen, sollte dies in Gruppen geschehen, wobei diejenigen mit der größten möglichen Datenschutzfolge zuerst aufgeführt werden, sodass die betroffenen Personen die Unterschiede klar erkennen können.

Organisationen sollten Inhalte, einschließlich relevanter Informationen, die auf dem ersten oder den folgenden Bildschirmen weggelassen wurden, den betroffenen Personen als Referenz zur Verfügung stellen, falls diese es wünschen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

ANMERKUNG Im Fall von Online-Benachrichtigungen können zur Anzeige von Inhalten Pop-ups und Drill-downs verwendet werden. Für betroffene Personen kann es schwierig sein, eine große Menge an Vertragsbedingungen zu lesen, insbesondere, wenn sie gerade eine bestimmte Handlung ausführen wollen.

Maschinenlesbare Benachrichtigungen können in einem standardisierten XML- oder JSON-Format zur Verfügung gestellt werden. Dadurch wird es möglich, dass Geräte einzelne Punkte angemessen auswählen und gegebenenfalls Grafiken und Icons anzeigen. Allerdings müssen sich Organisationen bewusst sein, dass sich die Interpretation grafischer Darstellungen durch betroffene Personen abhängig von deren kulturellen Hintergründen erheblich unterscheiden kann. Es können Leitfäden für die entsprechende Region oder Kultur erstellt werden, um zu vermeiden, dass betroffene Personen verwirrt werden.

5.2.8 Laufende Versionierung und Bezugnahme

Steuerungsmaßnahme

Die Organisation muss die Version der Benachrichtigung aufbewahren und verfügbar machen, die zum Zeitpunkt der Einwilligung der betroffenen Person angezeigt wurde, sowie die aktuellste relevante Version zur einfachen Referenzierung durch die betroffene Person.

Zusätzliche Informationen

Benachrichtigungsversionen sollten so lange aufbewahrt werden, wie sie mit den aufbewahrten pbD assoziiert sind.

5.2.9 Barrierefreiheit

Steuerungsmaßnahme

Die Organisation muss eine Benachrichtigung in einer zugänglichen Form zur Verfügung stellen, die der zugrundeliegenden Technologie des Online-Dienstes angemessen ist.

Zusätzliche Informationen

Insbesondere wenn zu erwarten ist, dass Einzelpersonen mit Problemen hinsichtlich der Barrierefreiheit auf Benachrichtigungen zugreifen, sollte es diesen ermöglicht werden, den Inhalt der Benachrichtigungen zu verstehen. Dies kann beinhalten, dass sichergestellt wird, dass der Benachrichtigungstext für Personen mit Sehbehinderungen akustisch wiedergegeben werden kann.

Richtlinien wie beispielsweise ISO/IEC 40500 unterstützen beim Entwurf von Barrierefreiheit.

5.3 Inhalte von Benachrichtigungen

5.3.1 Allgemeines

Ziel: Sicherstellen, dass die betroffene Person in der Benachrichtigung ausreichende Informationen vorfindet, um zu verstehen, wie die pbD verarbeitet werden und welche Rechte die betroffene Person hat.

5.3.2 Beschreibung des Zwecks

Steuerungsmaßnahme

Die Organisation muss sicherstellen, dass die Benachrichtigung Informationen über den Zweck enthält, für den die pbD verarbeitet werden.

Zusätzliche Informationen

Für betroffene Personen ist es wichtig, den Zweck der Verarbeitung der erhobenen pbD zu verstehen, damit sie eine aussagekräftige Einwilligung geben können. Um die Benachrichtigung kurz zu halten, kann für jeden

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

Zweck eine Benennung oder ein kurzer Satz angegeben werden, aber es sollte möglich sein (z. B. über einen Hyperlink), diese Benennung bzw. diesen Satz mit einer Kurzbeschreibung des Zwecks zu verknüpfen, die ausreicht, damit betroffene Personen eine aussagekräftige Einwilligung geben können.

Beim Entwurf von Benachrichtigungen muss sorgfältig vorgegangen werden, da eine zu detaillierte Darstellung dazu führen kann, dass diese häufig überarbeitet werden muss.

5.3.3 Darstellung der Beschreibung des Zwecks

Steuerungsmaßnahme

Die Organisation muss den Zweck der Erhebung jedes pbD-Elements angeben sowie angemessene Informationen zu plausiblen Risiken der Verarbeitung in der Reihenfolge nennen, die durch die allgemeine Risikobeurteilung ermittelt wurde.

ANMERKUNG Die Folgen und Risiken sind notwendigerweise offensichtlich.

Zusätzliche Informationen

Die Organisation erklärt, wie die pbD verwendet werden, und zwar auf eine Weise, die der betroffenen Person ein klares und einfaches Verständnis des Zwecks ermöglicht. Wenn der Zweck der Verwendung sich zwischen den erhobenen pbD-Elementen unterscheidet, sollte die Organisation eindeutig kennzeichnen, welcher Zweck für welches pbD-Element zutrifft.

5.3.4 Identifizierung der verantwortlichen Stelle

Steuerungsmaßnahme

Die Organisation muss der betroffenen Person die relevanten Informationen (z. B. Identität und Kontaktdaten) über die verantwortliche Stelle zur Verfügung stellen.

Zusätzliche Informationen

Die Identifizierung der verantwortlichen Stelle erfolgt üblicherweise anhand des Unternehmensnamens, aber sie kann auch die Anzeige der Unternehmensnummer, des Stammsitzes/der betrieblichen Adresse und (falls angemessen) von Abteilungsinformationen umfassen.

5.3.5 PbD-Erhebung

Steuerungsmaßnahme

Die Organisation muss Informationen zur Verfügung stellen, die es den betroffenen Personen ermöglichen zu verstehen, welche pbD-Elemente erhoben werden, selbst wenn die Erhebung bestimmter pbD-Elemente offensichtlich ist.

Zusätzliche Informationen

Zusätzlich zu allgemeinen Aussagen wie „Wir erfassen Ihre persönlichen Informationen“ sollte die Organisation eine Liste der spezifischen erhobenen pbD-Elemente zur Verfügung stellen (z. B. „Wir erfassen Ihren Namen, Ihre Adresse und Ihre Telefonnummer.“), falls dies aufgrund der Folgen, die mit der in 5.3.3 beschriebenen Beurteilung ermittelt wurden, angemessen ist, und zwar auch dann, wenn offensichtlich ist, welche Informationen erhoben werden.

Um zu identifizieren, welche pbD in der Benachrichtigung aufzuführen sind, sollte die Organisation ISO/IEC 29100:2011, 4.4 zu Rate ziehen.

Die Organisation sollte den tatsächlichen Wert eines zu erhebenden pbD-Elements zum Zeitpunkt der Erhebung angeben, falls dies relevant, machbar und praktikabel ist. Falls dies nicht machbar ist, kann die Organisa-

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

tion ein eindeutiges Beispiel für die erhobenen Elementwerte mit dem zugehörigen Namen des pbD-Elements zur Verfügung stellen. Dadurch kann die betroffene Person verstehen, welche Daten durch den Namen eines pbD-Elements referenziert werden und welche Arten von Werten erhoben werden.

BEISPIEL Anstatt den Begriff „Telefonnummer“ zu nennen, kann die Organisation Folgendes angeben: „Telefonnummer (01-234-5678)“

Wenn die verantwortliche Stelle die pbD der betroffenen Person über deren Geräte oder über Identitätsanbieter erhält, kann der betroffenen Person der tatsächliche Wert zusammen mit der Benachrichtigung angezeigt werden, bevor er an die verantwortliche Stelle übermittelt wird (Beispiele hierzu siehe A.2.3). Die Anzeige der tatsächlichen Werte der pbD-Elemente unterstützt betroffene Personen bei der Entscheidung, ob sie diese der verantwortlichen Stelle zur Verfügung stellen wollen, insbesondere, wenn es mehrere Elemente des gleichen Typs gibt. So kann die betroffene Person beispielsweise bei der Telefonnummer zustimmen, ihre betriebliche Telefonnummer zur Verfügung zu stellen, nicht aber ihre persönliche Mobiltelefonnummer.

Es sollte sorgfältig darauf geachtet werden, das Risiko eines pbD-Lecks zu verringern, beispielsweise durch Schulter-Surfen usw. Verfahren wie Maskierung und Drill-down sollten in Betracht gezogen werden.

Falls durch die pbD-Verarbeitung neue pbD erzeugt werden, ist es unmöglich, den tatsächlichen Wert vor der Einwilligung anzuzeigen. In solchen Fällen kann die Bereitstellung eines Beispielwerts wünschenswert sein. Wenn beispielsweise Kaufdaten von einem Shop zur Verfügung zu stellen sind und die betroffene Person zum Zeitpunkt der Einwilligung keinen Einkauf getätigt hat, stehen keine tatsächlichen Daten zur Anzeige zur Verfügung. In einem solchen Fall kann es wünschenswert sein, das Verständnis der betroffenen Person einzuholen, indem beispielhafte Kaufdaten angezeigt werden und die betroffene Person informiert wird, welche Arten von Daten erhoben werden.

5.3.6 Erhebungsverfahren

Steuerungsmaßnahme

Die Organisation muss betroffenen Personen eindeutige Erklärungen der verwendeten Erhebungsverfahren sowie Informationen über etwaige, mit bestimmten Erhebungsverfahren in Zusammenhang stehende Risiken zur Verfügung stellen.

Zusätzliche Informationen

PbD können auf unterschiedliche Weise erhoben werden. PbD können beispielsweise:

a) direkt von der betroffenen Person erhoben werden, z. B. durch ein Web-Formular;

b) indirekt erhoben werden, z. B. von einer dritten Partei wie beispielsweise einer Wirtschaftsauskunftei;

c) durch die verantwortliche Stelle beobachtet werden, z. B durch Beobachtung von Browser-Fingerabdrücken und aufgerufenen Webseiten;

d) durch die verantwortliche Stelle gefolgert werden, z. B. Profiling der betroffenen Person durch Analyse der mit den Verfahren a) bis c) erhobenen Daten.

Falls sich die Erhebungsverfahren in Abhängigkeit vom pbD-Element unterscheiden, sollte die Organisation auf der Grundlage der Folgen, die mit der in 5.3.3 beschriebenen Beurteilung ermittelt wurden, die betroffene Person darüber informieren, welches Erhebungsverfahren für welches pbD-Element verwendet wird. Wenn das gleiche Erhebungsverfahren für mehrere pbD-Elemente verwendet wird, dann können die pbD-Elemente unter dem entsprechenden Erhebungsverfahren gruppiert werden. Wenn aber die Datenschutzfolge, die durch eine allgemeine Beurteilung der Folgen für die entsprechende Population betroffener Personen bestimmt wurde, bei einem oder mehreren pbD-Elementen in der Gruppe erheblich höher ist als bei den anderen, dann sollte dies getrennt kommuniziert werden, damit die betroffene Person sich dessen bewusst wird.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

ANMERKUNG Dies dient der Verhinderung von Angriffen, bei denen der Angreifer die pbD-Elemente mit hohen Folgen zwischen harmlosen Elementen verbirgt, um die betroffene Person zur Einwilligung zu verleiten („Hide-a-Tree-in-a-Forest"-Attacke).

5.3.7 Zeitpunkt und Ort der pbD-Erhebung

Steuerungsmaßnahme

Die Organisation muss in der Benachrichtigung angeben, wann und wo die pbD im Allgemeinen erhoben werden; eine solche Benachrichtigung ist aber nicht erforderlich, falls die pbD-Erhebung erfolgt, indem eine betroffene Person eine Handlung wie beispielsweise die explizite Abgabe von Informationen durchführt.

Zusätzliche Informationen

Wenn pbD nicht direkt erhoben werden, kann es für die betroffene Person nicht offensichtlich sein, wann und wo die pbD-Erhebung erfolgt. Die Angabe dieser Informationen in der Benachrichtigung hilft der betroffenen Person, die Situation zu verstehen.

Üblicherweise sollten Benachrichtigungen vor der pbD-Erhebung zur Verfügung gestellt werden. Wenn beispielsweise pbD mittels eines Web-basierten Formulars erhoben werden, kann die Datenschutzerklärung (oder eine Zusammenfassung der Erklärung mit einem Link zur vollständigen Erklärung) oben im Formular enthalten sein. Ein zweites Beispiel ist die pbD-Erhebung mittels Videoüberwachung in einem öffentlichen Bereich; hier sollte am Zugang zum durch die Überwachung abgedeckten Bereich ein Hinweis („Bereich wird videoüberwacht") mit Einzelheiten zur verantwortlichen Stelle und Kontaktdaten angezeigt werden.

5.3.8 Nutzungsverfahren

Steuerungsmaßnahme

Die Organisation muss in der Benachrichtigung angeben, wie die pbD genutzt werden.

Zusätzliche Informationen

PbD können:

— direkt genutzt werden;

— nach Weiterverarbeitung genutzt werden (z. B. Ableitung, Schlussfolgerung, Entpersonalisierung, Kombination mit anderen Daten);

— mit anderen Daten kombiniert werden (z. B. geolokalisiert, durch Verwendung von Cookies, von Dritten);

— durch automatisierte Entscheidungsfindungsverfahren genutzt werden (z. B. Profiling, Klassifizierung).

Wenn die pbD vor der Nutzung verarbeitet werden (z. B. Entpersonalisierung, Aggregation), ist es wünschenswert, die Art der durchgeführten Transformationen zu nennen.

5.3.9 Geografischer Standort und zuständiges Rechtssystem bei gespeicherten pbD

Steuerungsmaßnahme

Die Organisation muss den/die geografischen Speicher- und Verarbeitungsort(e) der pbD angeben und auf den/die rechtlichen Zuständigkeitsbereich(e) verweisen, denen die Handhabung der Daten unterliegt.

Zusätzliche Informationen

Die Organisation sollte die geeignete Granularität der geografischen Standort(e) (z. B. Land, Region) unter Berücksichtigung aller in ISO/IEC 29100:2011, 4.5 beschriebenen Datenschutzanforderungen ermitteln.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

5.3.10 Übertragung an Dritte

Steuerungsmaßnahme

Die Organisation muss in der Benachrichtigung angeben, ob die pbD im Rahmen der normalen Geschäftstätigkeit an Dritte übertragen werden.

ANMERKUNG 1 Die Übertragung schließt die Offenlegung/Kommunikation der pbD ein.

Zusätzliche Informationen

Wenn eine Organisation pbD an Dritte überträgt, muss die Benachrichtigung direkt oder indirekt folgende Angaben enthalten:

— an wen die pbD übertragen werden;

— den/die geografischen Standort(e), an den/die die pbD übertragen werden, und alle Änderungen beim Rechtssystem, die sich ergeben können;

— zu welchem Zweck die pbD übertragen werden;

— die negativen Folgen für die betroffene Person oder die Risiken solcher Folgen, die durch die Datenübertragung entstehen; und

— die entsprechende Sicherung der Übertragung (z. B. Sicherung der Vertraulichkeit und Integrität).

Zwar muss die Organisation die einzelnen Drittempfänger identifizieren und auf diese hinweisen, aber sie kann gegebenenfalls eine Gruppe von Empfängern mittels eindeutig definierter Kriterien angeben.

Die in 5.3.10 spezifizierten Kriterien sollten eindeutig als Teil einer Zweckbestimmungskategorie oder -definition definiert werden.

ANMERKUNG 2 5.3.10 gilt nur für die Übertragung an Dritte und nicht für die Übertragung an einen Auftragsdatenverarbeiter.

5.3.11 Aufbewahrungsdauer

Steuerungsmaßnahme

Die Organisation muss Informationen über die Aufbewahrungsdauer und/oder einen Entsorgungsplan für die von ihr erhobenen pbD zur Verfügung stellen.

Zusätzliche Informationen

Die Information über die Aufbewahrungsdauer und/oder den Entsorgungsplan kann in Form eines festgelegten Zeitraums (z. B. 5 Jahre) ab dem Datum der Erhebung oder eines spezifischen Ereignisses oder Datums (z. B. Entsorgung am 1. Januar 2025) erfolgen. Sie kann auch aus Kriterien bestehen, aufgrund derer dieser Zeitraum oder Zeitplan bestimmt wird.

ANMERKUNG Eine Organisation kann pbD für unterschiedliche Zwecke erheben. Die Aufbewahrungsdauer kann sich abhängig vom Zweck unterscheiden. Daher kann die Aufbewahrungsdauer der Daten auch abhängig vom Zweck festgelegt werden.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12

5.3.12 Mitwirkung der betroffenen Person

Steuerungsmaßnahme

Die Organisation muss Informationen über die Rechte der betroffenen Person zum Zugriff auf ihre pbD (z. B. Zugang, Berichtigung, Löschung, Einspruch, Einschränkung, Datenübertragbarkeit, Zurückziehung der Einwilligung usw.) sowie die Rechte zur Korrektur oder Löschung ihrer pbD zur Verfügung stellen.

Zusätzliche Informationen

Die Benachrichtigung sollte direkt oder indirekt die folgenden Aspekte des Zugriffs beinhalten:

a) auf welche pbD-Elemente die betroffene Person Zugriff anfordern kann und das Verfahren, wie die betroffene Person eine solche Anforderung stellen kann;

b) welche Informationen die betroffene Person für eine angemessene Authentisierung zur Verfügung stellen muss, bevor der Zugriff auf die pbD autorisiert wird (zur Vermeidung des Risikos einer unangemessenen Offenlegung);

c) den Zeitraum, innerhalb dessen eine Anforderung bearbeitet wird;

d) alle Gebühren, die für einen solchen Zugriff berechnet werden, falls die Berechnung von Gebühren zulässig ist;

e) die Mittel, wie betroffene Personen die Richtigkeit und Vollständigkeit der pbD anfechten und sie ändern können, soweit dies angemessen ist;

f) die Umstände, unter denen Informationen nicht geändert oder gelöscht werden, und Einzelheiten zu den Möglichkeiten, wie eine betroffene Person Einwände bezüglich der Richtigkeit der pbD anzeigen kann; und

g) falls die Einwilligung die rechtliche Grundlage ist, wie diese widerrufen werden kann, falls der Widerruf möglich ist oder von den einschlägigen Rechtsvorschriften gefordert wird.

5.3.13 Anfragen und Beschwerden

Steuerungsmaßnahme

Die Organisation muss Informationen über die Kontaktdaten für Anfragen zur Verarbeitung der pbD, die in der Benachrichtigung angegeben wurden, und über das Recht zum Einreichen von Beschwerden bei einer Aufsichtsbehörde zur Verfügung stellen.

Zusätzliche Informationen

Die Kontaktinformationen umfassen, sind aber nicht beschränkt auf Telefonnummern, Websites, E-Mail-Adressen und physische Standorte, wo Anfragen gestellt werden können.

5.3.14 Information über Zugang zu den bei der Einwilligung getroffenen Entscheidungen

Steuerungsmaßnahme

Die Organisation muss die betroffene Person darüber informieren, wo und wie sie auf den gespeicherten Nachweis der anfänglich getroffenen Einwilligungsentscheidung und spätere Änderungen durch die betroffene Person (einschließlich Widerruf) sowie das Datum dieser Entscheidungen zugreifen kann.

Zusätzliche Informationen

Entscheidung und Einwilligung sind verschiedene Konzepte. Die Entscheidung ist die durch die betroffene Person durchgeführte Handlung. Wenn die Entscheidung der betroffenen Person nicht auf einer informierten und

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29184:2022-12