

DIN EN ISO/IEC 29184



ICS 35.030

**Informationstechnologie –
Online-Datenschutzerklärung und Einwilligung (ISO/IEC 29184:2020);
Deutsche Fassung EN ISO/IEC 29184:2023**

Information technology –
Online privacy notices and consent (ISO/IEC 29184:2020);
German version EN ISO/IEC 29184:2023

Technologies de l'information –
Déclarations de confidentialité en ligne et les consentements (ISO/IEC 29184:2020);
Version allemande EN ISO/IEC 29184:2023

Gesamtumfang 36 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

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 EN ISO/IEC 29184:2023 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 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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	siehe	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.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 24760-1, *IT-Sicherheit und Datenschutz — 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*

– Leerseite –

Deutsche Fassung

Informationstechnik —
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)

Diese Europäische Norm wurde vom CEN am 24. März 2023 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

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 Angemessene Stelle	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

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

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 EN ISO/IEC 29184:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Oktober 2023, und etwaige entgegenstehende nationale Normen müssen bis Oktober 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN und CENELEC abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 29184:2020 wurde von CEN als EN ISO/IEC 29184:2023 ohne irgendeine Abänderung genehmigt.

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-Directives, 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-Directives, 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 <http://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.

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 Maßnahmen 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).

1 Anwendungsbereich

Dieses Dokument legt Maßnahmen 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

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