

DIN EN 17799



ICS 03.120.20; 03.160

**Anforderungen an den Datenschutz bei Verarbeitungsvorgängen;
Deutsche Fassung EN 17799:2023**

Personal data protection requirements for processing operations;
German version EN 17799:2023

Exigences de protection des données à caractère personnel pour les opérations de
traitement;
Version allemande EN 17799:2023

Gesamtumfang 30 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Das Dokument EN 17799:2023 wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) und der Deutschen Kommission Elektrotechnik Elektronik Informationstechnik (DKE).

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

ISO/IEC 27000:2018	siehe	DIN EN ISO/IEC 27000:2020-06
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27701	siehe	DIN EN ISO/IEC 27701
ISO/IEC 29134	siehe	DIN EN ISO/IEC 29134
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 27000:2020-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020*

DIN EN ISO/IEC 27002, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen*

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 29134, *Informationstechnik — Sicherheitsverfahren — Leitlinien für die Datenschutz-Folgenabschätzung*

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

- Leerseite -

Deutsche Fassung

Anforderungen an den Datenschutz bei Verarbeitungsvorgängen

Personal data protection requirements for processing
operations

Exigences de protection des données à caractère
personnel pour les opérations de traitement

Diese Europäische Norm wurde vom CEN am 4. September 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
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Übersicht	7
5 Planung	7
5.1 Allgemeines	7
5.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien	7
5.3 Umfang der Tätigkeiten zur Verarbeitung personenbezogener Daten	7
5.3.1 Allgemeines	7
5.3.2 Aufzeichnungen über Datenverarbeitungstätigkeiten	7
5.3.3 Ermittlung der Rechtsgrundlage	8
5.3.4 Minimierung der Datenmenge	8
5.3.5 Aufbewahrungsfristen	9
5.4 Richtlinie zum Schutz personenbezogener Daten	9
5.5 Rollen und Verantwortlichkeiten	10
5.5.1 Allgemeines	10
5.5.2 Interne Rollen	11
5.5.3 Externe Rollen	11
5.6 Risikomanagement	12
5.6.1 Allgemeines	12
5.6.2 Datenschutz-Risikobeurteilung und Auswirkungsanalyse	12
5.6.3 Bewertung der Auswirkungen auf den Datenschutz	13
5.6.4 Umgang mit Risiken und Risikobehandlungsplan	14
5.7 Schutz personenbezogener Daten durch Technik und durch datenschutzfreundliche Voreinstellungen	14
6 Operative Tätigkeiten	15
6.1 Allgemeines	15
6.2 Datenschutzerklärung und Einwilligung	15
6.2.1 Datenschutzerklärung	15
6.2.2 Einwilligung	16
6.3 Aktualisierung von Rollen	16
6.4 Schutz personenbezogener Daten	16
6.4.1 Löschung von Daten	16
6.4.2 Umsetzung und Anwendung von Sicherheitsmaßnahmen	17
6.4.3 Umgang mit Verletzungen des Schutzes personenbezogener Daten	17
6.5 Anträge der betroffenen Personen zur Durchsetzung ihrer Rechte	18
6.5.1 Allgemeines	18
6.5.2 Zugang zu Daten	18
6.5.3 Berichtigung	19
6.5.4 Löschung	19
6.5.5 Einschränkung der Verarbeitung	19
6.5.6 Datenübertragbarkeit	20
6.5.7 Widersprüche	20
6.5.8 Automatisierte Entscheidungen, einschließlich Profiling	20
6.5.9 Beschwerden und Einsprüche	20
6.6 Schulung und Sensibilisierung	20
7 Kontrolle	21
7.1 Allgemeines	21
7.2 Interne Audits	21

7.3 Regelmäßiger Bericht 22

7.4 Nichtkonformitäten und Korrekturmaßnahmen 22

Anhang A (informativ) Zuordnung der Anforderungen an Verantwortliche und
Auftragsverarbeiter 24

Literaturhinweise 26

Tabellen

Tabelle A.1 — Zuordnung der Anforderungen an Verantwortliche und Auftragsverarbeiter 24

Europäisches Vorwort

Dieses Dokument (EN 17799:2023) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, 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 April 2024, und etwaige entgegenstehende nationale Normen müssen bis April 2024 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN 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 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.

Einleitung

Der Schutz personenbezogener Daten ist in der Europäischen Union durch Rechtsakte geregelt, von denen der wichtigste die EU-Verordnung 2016/679 (im Folgenden „Verordnung“ oder „DSGVO“) ist. Darin wird der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten geregelt, aber nicht in einen Zusammenhang mit einer Reihe von daraus folgenden oder darauf bezogenen Tätigkeiten gesetzt.

Darüber hinaus bezieht sich die Verordnung auf die Einführung von datenschutzspezifischen Zertifizierungsverfahren und von Datenschutzsiegeln und -abzeichen, die dazu dienen, die Einhaltung der Verordnung durch für die Datenverarbeitung Verantwortliche und Auftragsverarbeiter bei Verarbeitungsvorgängen darzustellen.

Diese Bemühungen werden auch eine solide Grundlage für die Konformität mit der Datenschutz-Grundverordnung (DSGVO) und die Angleichung der europäischen Datenschutzlandschaft an globale Normen bilden. Diese Normen haben einen grundlegend anderen Schwerpunkt, da sie auf ein Managementsystem und nicht wie das vorliegende Dokument auf Dienstleistungen und Prozesse ausgerichtet sind.

ISO/IEC 27701 wurde als EN angenommen, und CEN/CLC JTC 13 erarbeitet einen neuen Normungsvorhaben zur „Präzisierung für den europäischen Kontext“. Diese Bestrebungen werden auch eine solide Grundlage für die Konformität mit der Datenschutz-Grundverordnung (DSGVO) und die Angleichung der europäischen Datenschutzlandschaft an globale Normen bilden. Diese Normen haben jedoch einen grundlegend anderen Schwerpunkt, da sie auf ein Managementsystem und nicht wie das vorliegende Dokument auf Dienstleistungen und Prozesse ausgerichtet sind.