

DIN EN ISO/IEC 27038

ICS 35.040

Einsprüche bis 2016-04-26

Entwurf

**Informationstechnik –
IT-Sicherheitsverfahren –
Spezifikation für digitales Schwärzen (ISO/IEC 27038:2014);
Deutsche und Englische Fassung FprEN ISO/IEC 27038:2016**

Information technology –
Security techniques –
Specification for digital redaction (ISO/IEC 27038:2014);
German and English version FprEN ISO/IEC 27038:2016

Technologies de l'information –
Techniques de sécurité –
Spécifications pour la rédaction numérique (ISO/IEC 27038:2014);
Version allemande et anglaise FprEN ISO/IEC 27038:2016

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-02-26 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de 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/stellungnahme 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 (Hausanschrift: 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 31 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN ISO/IEC 27038:2016) wurde vom Technischen Komitee ISO/IEC JTC 1/SC 27 „IT Security techniques“ erarbeitet, dessen Sekretariat vom DIN (Deutschland) gehalten wird. Auf Grundlage eines CEN/BT Beschlusses wurde ISO/IEC 27038:2014 im einstufigen Annahmeverfahren (UAP) als FprEN ISO/IEC 27038:2016 ohne Abänderung übernommen.

Das zuständige deutsche Spiegelgremium ist der Arbeitskreis NA 043-01-27-04 AK „IT-Sicherheitsmaßnahmen und Dienste“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der FprEN ISO/IEC 27038 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Informationstechnik — IT-Sicherheitsverfahren — Spezifikation für digitales Schwärzen (ISO/IEC 27038:2014)

*Technologies de l'information — Techniques de sécurité — Spécifications pour la rédaction numérique
(ISO/IEC 27038:2014)*

Information technology — Security techniques — Specification for digital redaction (ISO/IEC 27038:2014)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: Einstufiges Annahmeverfahren
Dokument-Sprache: D

STD Version 2.7g

Inhalt

	Seite
Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Begriffe	6
3 Symbole und Abkürzungen	7
4 Allgemeine Grundsätze des digitalen Schwärzens	7
4.1 Einleitung	7
4.2 Anonymisierung	7
5 Anforderungen	7
5.1 Überblick	7
5.2 Grundsätze des Schwärzens	8
6 Schwärzungsprozess	9
6.1 Einleitung	9
6.2 Papiererzeugnisse	9
6.3 Digitale Bilderzeugnisse	10
6.4 Einfaches digitales Schwärzen	10
6.4.1 Allgemeines	10
6.4.2 Zeichencodierung	10
6.5 Komplexes digitales Schwärzen	10
6.5.1 Allgemeines	10
6.5.2 Dokumente mit komplexem Dateiformat	11
6.5.3 Nicht-textuelle Informationen	11
6.6 Kontextinformationen	11
6.6.1 Einleitung	11
6.6.2 Einfaches Schwärzen	11
6.6.3 Erweitertes Schwärzen	12
7 Aufzeichnungen über Schwärzungen	12
8 Merkmale von Softwaretools zum Schwärzen	12
9 Anforderungen an das Testen von Schwärzungen	13
Anhang A (informativ) Schwärzen von PDF-Dokumenten	15

Europäisches Vorwort

Der Text von ISO/IEC 27038:2014 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und auf Grundlage eines CEN/BT Beschlusses als FprEN ISO/IEC 27038:2016 übernommen.

Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27038:2014 wurde vom CEN als FprEN ISO/IEC 27038:2016 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. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Standards werden in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe von gemeinsamen technischen Komitees ist es Internationale Standards zu erarbeiten. Entwürfe die vom gemeinsamen technischen Komitee verabschiedet worden sind, werden zur Abstimmung unter den NB verteilt. Die Veröffentlichung als Internationale Norm erfordert mindestens 75% positive Stimmen der abstimmenden Länder.

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

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology, SC 27, IT Security techniques*.

Einleitung

Manche Dokumente können Informationen enthalten, die einigen Gemeinschaften nicht offen zugänglich gemacht werden dürfen. Modifizierte Dokumente können für diese Gemeinschaften freigegeben werden, nachdem eine angemessene Bearbeitung des Originaldokuments erfolgt ist. Diese Bearbeitung kann das Entfernen von Abschnitten, Absätzen oder Sätzen betreffen, wobei gegebenenfalls erwähnt wird, dass diese entfernt worden sind. Dieser Vorgang wird als „Schwärzen“ des Dokuments bezeichnet.

Das digitale Schwärzen von Dokumenten ist ein relativ neuer Bereich des Dokumentenmanagements, der besondere Fragen und potentielle Risiken aufwirft. Wenn digitale Dokumente geschwärzt werden, dürfen die entfernten Informationen nicht wiederherstellbar sein. Demzufolge ist darauf zu achten, dass geschwärzte Informationen dauerhaft aus dem digitalen Dokument entfernt werden (z. B. dürfen sie nicht nur in nicht darstellbaren Teilen des Dokuments ausgeblendet werden).

Diese Internationale Norm legt Methoden für das digitale Schwärzen von digitalen Dokumenten fest.

Schwärzen kann sowohl das Entfernen von Dokument-Metadaten als auch das Entfernen von Informationen (z. B. eines Bildes), die in das Dokument importiert wurden, bedeuten.

Es kann die Möglichkeit bestehen, geschwärzte Informationen in einem geschwärzten digitalen Dokument anhand ihres Kontextes zu identifizieren. Beispielsweise kann die Länge des Ersatztextes für die geschwärzten Informationen auf die Länge der geschwärzten Informationen und demzufolge auf die Informationen selbst Hinweis geben. Diese Internationale Norm stellt zwei Kategorien des Schwärzens vor:

- EINFACHES Schwärzen, bei dem der Kontext nicht berücksichtigt wird;
- ERWEITERTES Schwärzen, bei dem der Kontext berücksichtigt wird.

Schwärzungsverfahren können zur Anonymisierung von Informationen in einem Dokument eingesetzt werden, z. B. durch das Entfernen von Namen in Sätzen. Sie können außerdem das Entfernen von Zahlen in Sätzen und deren Ersatz durch „XXX“ umfassen.

1 Anwendungsbereich

Diese Internationale Norm legt Merkmale von Techniken zum digitalen Schwärzen in digitalen Dokumenten fest. Diese Internationale Norm legt außerdem Anforderungen an Softwaretools zum Schwärzen und an Methoden, mit denen getestet wird, ob das digitale Schwärzen sicher abgeschlossen wurde, fest.

Diese Internationale Norm umfasst nicht das Schwärzen von Daten aus Datenbanken.

2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

2.1

Anonymisierung

Prozess, durch den personenbezogene Daten (PII, en: personally identifiable information) unwiderruflich so verändert werden, dass ein Betroffener nicht mehr direkt oder indirekt identifiziert werden kann, weder durch die verantwortliche Stelle allein noch in Zusammenarbeit mit jeder anderen Partei

[QUELLE: ISO/IEC 29100:2011, Begriff 2.2]

2.2

Dokument

aufgezeichnete Informationen, die als eine Einheit behandelt werden können

Anmerkung 1 zum Begriff: Dokumente können Text, Bilder, Video- und Audioinhalte, Metadaten und andere zugehörige Inhalte enthalten.

2.3

personenbezogene Daten

PII

(en: personally identifiable information)

sämtliche Informationen, die (a) verwendet werden können, um den Betroffenen, auf den sich solche Informationen beziehen, zu identifizieren, oder die (b) im direkten oder indirekten Zusammenhang mit dem Betroffenen stehen oder möglicherweise stehen

Anmerkung 1 zum Begriff: Um festzustellen, ob ein Betroffener identifizierbar ist, sollten alle Mittel überprüft werden, die vernünftigerweise vom Datenschutzvertreter, der im Besitz der Daten ist, oder von einer beliebigen anderen Partei verwendet werden können, um diese natürliche Person zu identifizieren.

[QUELLE: ISO/IEC 29100:2011, Begriff 2.9]

2.4

Schwärzen

dauerhaftes Entfernen von Informationen aus einem Dokument

2.5

fachlicher Prüfer

Person(en), die ein Dokument hinsichtlich der Schwärzungsanforderungen beurteilt/beurteilen

Anmerkung 1 zum Begriff: Mehrere Personen können ein bestimmtes Dokument gleichzeitig beurteilen.

3 Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

PII	personenbezogene Daten (en: personally identifiable information)
PDF	transportables Dokumentenformat (en: portable document format)
OCR	optische Zeichenerkennung (en: optical character recognition)
XML	erweiterbare Auszeichnungssprache (en: extensible markup language)

4 Allgemeine Grundsätze des digitalen Schwärzens

4.1 Einleitung

Schwärzen wird zum unwiderruflichen Entfernen bestimmter Informationen aus einem Dokument vorgenommen. Es sollte durchgeführt werden, wenn z. B. ein Wort oder zwei einzelne Wörter, ein Satz oder ein Absatz, ein Bild, ein Name, eine Anschrift und/oder eine Unterschrift aus einem Dokument zu entfernen sind, bevor das Dokument anderen Personen, die nicht berechtigt sind, die entfernten Informationen einzusehen, zugänglich gemacht wird.

Der Prozess des digitalen Schwärzens bedeutet nicht nur einfach das Entfernen von Informationen, sondern auch die Angabe, soweit notwendig, dass einige Informationen entfernt wurden, damit der Leser weiß, dass das Dokument geschwärzt wurde. Beispielsweise kann es notwendig sein, zu wissen, dass einige Wörter oder einige Absätze gelöscht wurden, um die Semantik der nicht geschwärzten Informationen aufrechtzuerhalten.

4.2 Anonymisierung

Ein Ziel der Schwärzung ist z. B. das Entfernen von personenbezogenen Daten (PII) aus einem Dokument (Anonymisierung). Wenn dieses Ziel besteht, dann muss der Schwärzungsprozess so ausgestaltet sein, dass die Identität der Person, deren Daten geschwärzt werden, geschützt ist.

Obwohl ein Name in einem Dokument geschwärzt wurde, kann es z. B. auch sein, dass die Identität der Person aus den verbleibenden Informationen hervorgeht. Wenn die Anonymisierung erforderlich ist, müssen alle Informationen, die zur Identifizierung der Person genutzt werden könnten, geschwärzt werden. Dazu zählen alle Informationen, die in Verbindung mit weiteren Informationen (die aus anderen Quellen stammen können) auf die Identität der Person schließen lassen.

5 Anforderungen

5.1 Überblick

Organisationen sollten in der Lage sein, die Dokumente zu erkennen, die geschwärzt werden müssen, bevor sie anderen Teilen der Organisation oder Dritten (z. B. der Öffentlichkeit) zugänglich gemacht werden.

Das Schwärzen sollte von fachlichen Prüfern durchgeführt oder überwacht werden, die über das nötige Wissen über die Dokumente verfügen und entscheiden können, welche Informationen zu schwärzen sind. Falls die fachlichen Prüfer, die diese Informationen festlegen, das Schwärzen nicht selbst vornehmen, müssen sie gezielte Anweisungen geben, wie „Datum der Aufzeichnungen ...“, Absatz-Nr. ..., Zeilenstart ... und Zeilenende ...“ usw.

Das Schwärzen muss in Kopien des digitalen Dokuments vorgenommen werden. Aus dem Schwärzungsprozess muss ein neues digitales Dokument hervorgehen, in dem gewisse Informationen vollständig und unwiderruflich entfernt wurden. Dieses neue digitale Dokument muss auf die gleiche Weise wie das Originaldokument gehandhabt und veräußert werden.

Bei der Festlegung der Informationen, die vor der Freigabe des Dokuments zu schwärzen sind, sollten keine ganzen Sätze oder Absätze gekennzeichnet werden, falls nur ein oder zwei Wörter in diesem Satz oder Absatz zu schwärzen sind, es sei denn, nach der Freigabe wäre eine Identifizierung der geschwärzten Informationen anhand des Kontextes möglich.

Soweit notwendig, müssen Informationen, die darauf hinweisen, dass ein digitales Dokument geschwärzt wurde, mit dem digitalen Dokument verknüpft sein. Zur Identifizierung der Tatsache, dass ein Schwärzungsprozess erfolgt ist, dürfen die geschwärzten Informationen durch einen Satz, der angibt, dass einige Informationen geschwärzt wurden, ersetzt werden.

Wenn das Schwärzen in einem digitalen Dokument vorgenommen wird, müssen sämtliche Metadaten des digitalen Dokuments hinsichtlich der Schwärzungsanforderungen überprüft und ebenfalls angemessen geschwärzt werden.

Wenn das Schwärzen in einem digitalen Dokument erfolgt, das Bild-, Video- und/oder Audioinformationen enthält, müssen Schwärzungstechniken eingesetzt werden, die die betroffenen Informationen entfernen.

5.2 Grundsätze des Schwärzens

Das Schwärzen von digitalen Dokumenten muss in Übereinstimmung mit den folgenden Grundsätzen durchgeführt werden:

- Speichern des digitalen Originaldokuments

Die Original- bzw. Master-Version eines digitalen Dokuments darf nicht geschwärzt werden — das Schwärzen muss in einer Kopie des digitalen Dokuments vorgenommen werden. Digitale Originaldokumente (z. B. das nicht geschwärzte Dokument) müssen gespeichert werden und dürfen nur Befugten zugänglich sein.

- vollständiges Entfernen von geschwärzten Informationen

Das Schwärzen muss die geforderten Informationen aus der geschwärzten Version des Dokuments unwiderruflich entfernen. Die Informationen müssen vollständig aus dem digitalen Dokument und nicht nur aus den darstellbaren Inhalten entfernt werden.

- sicherheitsbewertetes Schwärzen

Das Schwärzen muss stets mit den von der Organisation genehmigten Methoden durchgeführt werden.

- kontrollierte Umgebung

Elektronisches Schwärzen muss in einer Umgebung durchgeführt werden, die nur für diejenigen Personen zugänglich ist, die im Hinblick auf das Schwärzen geschult und befugt sind.

- Zwischenstadien

Alle geschwärzten Dokumente in Zwischenstadien des Schwärzungsprozesses sollten gelöscht werden. Nur das digitale Originaldokument und die jeweilige geschwärzte Version sollten beibehalten werden. Wenn ein bestimmtes digitales Dokument auf verschiedene Weisen zu schwärzen ist (z. B. für unterschiedliche Empfänger), kann es angebracht sein, Zwischenstadien des Dokuments vorübergehend beizubehalten, bis alle Schwärzungsprozesse abgeschlossen sind.