DIE FRANZÖSISCHE REPUBLIK

Ministerium für Gesundheit und Prävention

Anordnung zur Änderung der Anordnung vom 11. Juni 2018 zur Genehmigung des Akkreditierungsrahmens der Zertifizierungsstellen und des Zertifizierungsrahmens für das Hosting personenbezogener Gesundheitsdaten

NOR: SPRD2325104A

Der Minister für Gesundheit und Prävention und der Minister für Wirtschaft und Finanzen,

Gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung);

Gestützt auf die Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, insbesondere auf die Notifizierung Nr. XX;

Gestützt auf den französischen Code de la santé publique, insbesondere auf die Artikel L. 1111-8 und R. 1111-10,

Gestützt auf das Gesetz Nr. 78-17 vom 6. Januar 1978 über Informatik, Dateien und Freiheiten in der geänderten Fassung;

Gestützt auf die Anordnung vom 11. Juni 2018 zur Genehmigung des Akkreditierungsrahmens der Zertifizierungsstellen und des Zertifizierungsrahmens für das Hosting personenbezogener Gesundheitsdaten;

Gestützt auf die Stellungnahme der Nationalen Kommission für Informatik und Freiheiten vom 13. Juli 2023;

Gestützt auf die Notifizierung Nr. .../.../F, die der Europäischen Kommission unter .... übermittelt wurde,

verfügen hiermit:

Artikel 1

Die Artikel 1 und 2 der genannten Anordnung vom 11. Juni 2018 erhalten folgende Fassung:

“ *Artikel 1* — Der Akkreditierungsrahmen der Zertifizierungsstellen für das Hosting personenbezogener Gesundheitsdaten gemäß Artikel R. 1111-10 des Code de la santé publique in der geänderten Fassung im Anhang dieser Anordnung wird angenommen.“

“ *Artikel 2*. - Der Zertifizierungsrahmen für das Hosting personenbezogener Gesundheitsdaten gemäß Artikel R. 1111-10 des Code de la santé publique in der geänderten Fassung im Anhang dieser Anordnung wird angenommen.“

Artikel 2

Die obigen Bestimmungen von Artikel 2 der Anordnung vom 11. Juni 2018 treten in ihrem Wortlaut, der sich aus dieser Anordnung ergibt, innerhalb von sechs Monaten nach ihrer Veröffentlichung in Kraft. Sie gelten für Anträge auf Erteilung einer Konformitätsbescheinigung und für Anträge auf Erneuerung einer solchen Bescheinigung, die ab diesem Datum bei einer Zertifizierungsstelle eingereicht werden.

Artikel 3

Der Minister für Gesundheit und Prävention und der Wirtschaftsminister sind jeweils für die Durchführung dieser Anordnung verantwortlich, die im *Amtsblatt* der Französischen Republik veröffentlicht wird.

Erstellt am XXX.

Für und im Namen des Ministers für Gesundheit und Prävention:

Hela Ghariani

Delegierte für digitale Gesundheit

Für und im Namen des Ministers für Wirtschaft und Finanzen:

Thomas Courbe

Generaldirektor der Unternehmen

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

La transformation commence ici Die Transformation beginnt hier

Zertifizierungsrahmen für das Hosting von Gesundheitsdaten (HDS)

Anforderungen

Status: Fortlaufend | *Klassifikation Eingeschränkt* | *Version: v0.1*

Agence du numérique en santé (Agentur für digitale Gesundheit)
2-10 Rue d'Oradour-sur-Glane – 75015 Paris
Tel. 01 58 45 32 50
esante.gouv.fr

Referenzdokumente

Vorschriften

Verweis	Dokument
[ART_L1111-8]	Artikel L. 1111-8 des Code de la santé publique über das Hosting von Gesundheitsdaten https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549
[DSGVO]	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 („Datenschutz-Grundverordnung“) https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
[ART R1111-8-8]	Artikel R. 1111-8-8 des Code de la santé publique über die Tätigkeit des Hostings von Gesundheitsdaten https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036656709
[ART R1111-9] bis [ART R1111-11]	Artikel R1111-9 bis R-1111-11 des Code de la santé publique über das Hosting personenbezogener Gesundheitsdaten in digitalen Medien, die einer Zertifizierung unterliegen. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/ LEGISCTA000006196138/#LEGISCTA000036658495

Weiterführende Normen

Verweise	Dokument
[ISO 27001]	NF ISO/IEC 27001:2023 Informationssicherheit, Cybersicherheit und Datenschutz – Managementsysteme für Informationssicherheit – Anforderungen

Änderungsverlauf

Fassung	Ausstellungsdatum	Anmerkungen
V1.1	Juni 2018	Veröffentlichte Fassung der Anordnung vom 11. Juni 2018 zur Genehmigung des Akkreditierungsrahmens der Zertifizierungsstellen und des Zertifizierungsrahmens für das Hosting personenbezogener Gesundheitsdaten
V1.1.20230330	März 2023	Entwurf der Überarbeitung, deren wichtigste Änderungen sind: ► Die Definition des Anwendungsbereichs von Aktivität 5 „Verwaltung und Betrieb des Informationssystems mit Gesundheitsdaten. ► Unter Berücksichtigung der Norm NF ISO/IEC 27001: 2023. ► Eine Erinnerung an die in Artikel R.1111-11 des Code de la santé publique genannten vertraglichen Anforderungen. ► Standardisierung der Darstellung von Garantien. ► Strengere Anforderungen an Datenübermittlungen außerhalb der Europäischen Union.

INHALTSVERZEICHNIS

1. PRÄAMBEL

Diese Aktualisierung des Zertifizierungsrahmens für Gesundheitsdatenhosts zielt darauf ab, neue Probleme und Verbesserungspunkte gegenüber dem vorherigen Rahmen aus dem Jahr 2018 zu berücksichtigen, die in Abstimmung mit dem Ökosystem ermittelt wurden. Diese Aktualisierung besteht insbesondere aus:

> Verbesserung der Lesbarkeit der von einem zertifizierten Host bereitgestellten Garantien für die Dienstleistungen, die er für einen bestimmten Kunden erbringt;
> Klärung der vertraglichen Verpflichtungen des Hosts im Sinne des Code de la santé publique;
> Strengere Anforderungen an den Schutz personenbezogener Daten im Zusammenhang mit Datenübermittlungen außerhalb der Europäischen Union. In diesem letzten Punkt ist dies ein erster Schritt: bis 2027 werden strengere Anforderungen in Bezug auf die europäische Souveränität hinzugefügt, die mit künftigen europäischen Rahmenbedingungen (EUCS – European Cybersecurity Certification Scheme for Cloud Services) in Einklang stehen.

Für den Fall, dass der Host, der die HDS-Zertifizierung beantragt, bereits eine Zertifizierung auf der Grundlage des ANSSI SecNumCloud 3.2-Frameworks erhalten hat, wird den Hosts in Anhang 1 eine Matrix zur Verfügung gestellt, die die Übereinstimmung zwischen den Maßnahmen in Anhang A der Norm ISO 27001 und den SecNumCloud-Anforderungen zeigt, um die Anwendung eines qualifizierten SecNumCloud-Hosts für HDS-Zertifizierungen zu erleichtern.

1.1. Zweck des Rahmens

Gemäß Artikel R1111-10 des Code de la santé publique legt der HDS-Zertifizierungsrahmen (nachstehend „Anforderungsrahmen“ oder „Rahmen“ genannt) die Anforderungen fest, die ein Host erfüllen muss, um die Zertifizierung als Gesundheitsdatenhost zu erhalten.

1.2. Anwendungsbereich des Rahmens

Der Anforderungsrahmen gilt für die Hosts personenbezogener Gesundheitsdaten gemäß Artikel L. 1111-8 des Code de la santé publique.

2. ALLGEMEINE BEGRIFFSBESTIMMUNGEN UND KONZEPTE

2.1.1. Akteur

Alle Interessenträger, die zur Sicherheit personenbezogener Gesundheitsdaten beitragen, mit Ausnahme des Datenverantwortlichen und der Auftragsverarbeiter eines zertifizierten Hosts, wenn sie in Übereinstimmung mit der Sicherheitspolitik und unter der Aufsicht des genannten Hosts handeln.

2.1.2. Verwaltung und Betrieb des Informationssystems mit Gesundheitsdaten

Die Tätigkeit der Verwaltung und des Betriebs des Informationssystems, das Gesundheitsdaten enthält, besteht darin, die Eingriffe in die Ressourcen zu beherrschen, die dem Kunden des Hosts zur Verfügung gestellt werden. Sie umfasst alle folgenden Nebentätigkeiten:

Festlegung eines Verfahrens für die Zuweisung und jährliche Überprüfung nominativer, gerechtfertigter und notwendiger Zugangsrechte;
Sicherung des Zugangsverfahrens;
Das Sammeln und Bewahren von Spuren der vorgenommenen Zugriffe und deren Gründe;
Vorherige Validierung von Eingriffen (Interventionsplan, Interventionsprozess).

Die Validierung von Interventionen besteht darin, sicherzustellen, dass sie die Sicherheit der gehosteten Informationen weder für den betreffenden Kunden noch für die anderen Kunden des Hosts beeinträchtigen. Diese Validierung kann in folgenden Fällen durchgeführt werden:

A priori für Eingriffe, die der Kunde unabhängig durchführen kann;
Wenn ein Service vom Host angefordert wird.

Die Definition des Zuteilungsverfahrens, der Sicherheit, der Erhebung und Validierung ist für die in Artikel R. 1111-9 Absätze 1 bis 4 des Code de la santé publique definierten Tätigkeiten intrinsisch und obligatorisch. Werden sie ausschließlich durchgeführt, soweit sie mit den Tätigkeiten 1 bis 4 verbunden und substanziell sind, ist der Host nicht verpflichtet, für die Aktivität 5 zertifiziert zu sein. Dies ist nur für den Fall erforderlich, dass er nur Aktivität 5 ausführt.

2.1.3. Kunde des Hosts

Der Kunde des Hosts (auch als „Kunde“ bezeichnet) bezeichnet die natürliche oder juristische Person, die den vom Host bereitgestellten Dienst abonniert.

2.1.4. Host

Der Host, der auch als Organisation in der ISO 27001-Norm bezeichnet wird, ist der Antragsteller für die Zertifizierung als Host von Gesundheitsdaten oder für die Erneuerung seiner Zertifizierung. Er stellt ganz oder teilweise einen Hosting-Dienst für personenbezogene Gesundheitsdaten (oder „Gesundheitsdaten“) im Sinne von Artikel L. 1111-8 des Code de la santé publique zur Verfügung.

2.1.5. Elektronische Identifizierungsmittel

Ein elektronisches Identifizierungsmittel ist ein materielles oder immaterielles Element, das personenbezogene Identifizierungsdaten enthält und zur Authentifizierung bei einem Online-Dienst verwendet wird.

2.1.6. Für die Datenverarbeitung Verantwortlicher

Dieser Begriff bezieht sich auf den für die Verarbeitung Verantwortlichen im Sinne der Verordnung 2016/679, d. h. die natürliche oder juristische Person, Behörde, Dienstleistung oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung bestimmt.

2.2. Abkürzungen und Akronyme

Akronym	
CSP	Code de la santé publique (Gesetzbuch über die öffentliche Gesundheit)
DSCP	Données de Santé à Caractère Personnel (Persönliche Gesundheitsdaten)
HDS	Hébergeur de Données de Santé (Gesundheitsdatenhost)
DSGVO:	Allgemeine Datenschutzverordnung
ISMS	Informationssicherheitsmanagementsystem

3. GELTUNGSBEREICH

3.1. Anwendbarkeit des HDS-Zertifizierungsrahmens

Der Anwendungsbereich des Rahmens wird in den Artikeln L. 1111-8, R. 1111-8-8 und R. 1111-9 des Code de la santé publique festgelegt.

3.1.1. Rolle des Hosts

Die HDS-Zertifizierung gilt für jede natürliche oder juristische Person, die einen Hosting-Dienst ganz oder teilweise für personenbezogene Gesundheitsdaten erbringt und ein Auftragsverarbeiter im Sinne von Artikel 28 der DSGVO ist.

3.1.2. Art der Daten

Die gehosteten Daten müssen personenbezogene Daten sein, die sich auf die Gesundheit beziehen, wie in Artikel 4.15 der DSGVO definiert.

3.1.3. Kontext der Sammlung

Die HDS-Zertifizierung betrifft persönliche Gesundheitsdaten, die während der Prävention, Diagnose, Pflege oder sozialen oder medizinischen Follow-up-Aktivitäten erhoben werden.

Diese personenbezogenen Gesundheitsdaten müssen im Auftrag der natürlichen oder juristischen Personen gespeichert werden, die für die Erstellung oder Erhebung der Daten oder im Auftrag des Patienten verantwortlich sind.

3.1.4. Durchgeführte Tätigkeiten

In Artikel R. 1111-9 des CSP wird die Tätigkeit des Hostings von Gesundheitsdaten festgelegt:

Die Bereitstellung aller oder einiger der folgenden Tätigkeiten im Namen des für die Verarbeitung Verantwortlichen gemäß Artikel R. 1111-8-8 I Absatz 1 oder des Patienten gemäß I Absatz 2 desselben Artikels gilt als das Hosting personenbezogener Gesundheitsdaten im digitalen Format im Sinne von Artikel L. 1111-8 II:

1. Bereitstellung und Aufrechterhaltung der Betriebsfähigkeit von physischen Standorten, an denen die materielle Infrastruktur des für die Verarbeitung der Gesundheitsdaten verwendeten Informationssystems gehostet werden kann;

2. Bereitstellung und Aufrechterhaltung der Betriebsfähigkeit der materiellen Infrastruktur des für die Verarbeitung der Gesundheitsdaten verwendeten Informationssystems;

3. Bereitstellung und Aufrechterhaltung der Betriebsfähigkeit der virtuellen Infrastruktur des für die Verarbeitung der Gesundheitsdaten verwendeten Informationssystems;

4. Bereitstellung und Aufrechterhaltung der Betriebsfähigkeit der Hosting-Plattform für Anwendungen des Informationssystems;

5. Verwaltung und Betrieb des Informationssystems, in dem die Gesundheitsdaten enthalten sind;

6. Sicherung von Gesundheitsdaten.

Aktivität 5 ist in Absatz 2.1.2 festgelegt.

Die Aktivität 6 zur Datensicherung sollte so interpretiert werden, dass sie nur ausgelagerte Backups einschließt. Die Backups, die für die Aktivitäten 1 bis 5 von Natur aus notwendig sind, fallen in den Rahmen der Aktivitäten 1 bis 5.

4. BEDINGUNGEN FÜR DIE ERTEILUNG EINER BESCHEINIGUNG

Anforderung Nr. 01
[EXI 01] Die Zertifizierung eines Hosts erfordert: Dass er ein Informationssicherheitsmanagementsystem (ISMS) implementiert hat, das nach der Norm

ISO 27001 zertifiziert ist, ergänzt durch die in Kapitel 5. definierten Anforderungen;
In der Erwägung, dass der Anwendungsbereich dieses ISMS alle Hosting-Aktivitäten für Gesundheitsdaten des Hosts abdeckt;
Mit seinen Kunden geschlossene Verträge erfüllen die Anforderungen des Kapitels 6.;
Die Einhaltung der in Kapitel 7 festgelegten Souveränitätserfordernisse;
Dass er seinen Kunden die Vorlage der gemäß dem Kapitel formalisierten Garantien übermittelt.

5. ISMS-ANFORDERUNGEN

Die Nummerierung dieses Kapitels entspricht der ISO 27001 und beginnt bei Punkt 5.4, entsprechend Kapitel 4 der Norm.

5.1. Kontext der Organisation

5.1.1. Verstehen der Organisation und ihres Kontextes

Die Anforderungen in Kapitel 4.1 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 02

[EXI 02] Bei der Festlegung seiner externen und internen Fragen muss der Host berücksichtigen, dass sein Auftrag von ihm verlangt, die ihm von seinen Kunden anvertrauten DSCP zu schützen.

5.1.2. Verständnis der Bedürfnisse und Erwartungen der betroffenen Parteien

Die Anforderungen in Kapitel 4.2 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 03

[EXI 03] Bei der Festlegung der Anforderungen der betroffenen Parteien muss der Host den geltenden Rechtsrahmen für den Schutz der DSCP berücksichtigen.

5.1.3. Bestimmung des ISMS-Anwendungsbereichs

Die Anforderungen in Kapitel 4.3 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 04

[EXI 04] Der Anwendungsbereich des ISMS muss die gesamte vom Host bereitgestellte DSCP-Verarbeitung umfassen. Er muss alle Mittel und Prozesse der Verarbeitung von DSCP abdecken, einschließlich Backups und Übertragungen von materiellen Informationsmedien.

5.1.4. Informationssicherheitsmanagementsystem

Es gelten die Anforderungen nach Absatz 4.4 der ISO 27001.

5.2. Kontrolle

Es gelten die Anforderungen in Kapitel 5 der ISO 27001.

5.3. Planung

5.3.1. Maßnahmen, die angesichts von Risiken und Chancen durchzuführen sind

5.3.1.1. Allgemeine Punkte

Es gelten die Anforderungen in Kapitel 6.1.1 der ISO 27001.

5.3.1.2. Risikoabschätzung

Die Anforderungen in Kapitel 6.1.2 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 05

[EXI 05] Bei der Risikoabschätzung muss der Host mindestens folgende Ereignisse berücksichtigen:

A. Ausfall materieller Informationsmedien aufgrund physischer und umweltbedingter Bedrohungen.
B. Verlust der Kontrolle über materielle Informationsmedien, insbesondere während:
    a. Kopieren von DSCP auf tragbaren Medien;
    b. Jede Materialisierung in Papierformat;
    c. Umverteilung von Lagerräumen.
C. Beschädigung, Kompromittierung oder Unterbrechung eines internen oder externen Informationsflusses unter der Verantwortung des Hosts.
D. Nichtbeherrschung des gewährten Zugangs, unabhängig davon, ob es sich um Personal unter der Kontrolle der Organisation handelt, oder Personal, das von ihren Kunden benannt wurde:
    a. Zuteilung, Änderung und Entzug von Zugangsrechten;
    b. Verbreitung elektronischer Identifizierungsmittel;
    c. Rückverfolgbarkeit und Zurechenbarkeit des Zugangs;
    d. Gelegentlicher Zugriff bei Prüfungen und Intrusion-Tests.
E. Nichtbeherrschung von Interventionen, sei es auf Initiative der Organisation oder im Auftrag eines Kunden.
F. Unvorhergesehene Nutzung des Dienstes aufgrund von Ungeschicktheit oder böswilliger Absicht.
G. Hardware- oder Softwarefehler, die es unmöglich machen, die Geschäftskontinuität oder Wiederherstellungsverpflichtungen zu erfüllen.

H. Unterwerfung des Hosts oder eines Auftragsverarbeiters unter außereuropäische Rechtsvorschriften, die zu einem Verstoß gegen die DSCP führen können.

5.3.1.3. Risikobehandlung

Die Anforderungen in Kapitel 6.1.3 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderungen:

Anforderung Nr. 06

[EXI 06] Bei der Verwendung von Unteraufträgen hat der Host sicherzustellen, dass er Änderungen der technischen und organisatorischen Maßnahmen seiner Auftragsverarbeiter zur Bewältigung der festgestellten Risiken kontrolliert.

Anforderung Nr. 07

[EXI 07] Um das Risiko einer unvorhergesehenen Nutzung des Systems zu verringern, muss der Host sicherstellen, dass:

Die Schnittstellen, die den Kunden angeboten werden, mindestens in französischer Sprache verfügbar sind;
Die erste Stufe zumindest auf Französisch unterstützt wird.

Anforderung Nr. 08

[EXI 08] Die Anwendbarkeitserklärung muss den Prüfern auf Anfrage in französischer Sprache zur Verfügung stehen.

5.3.2. Informationssicherheitsziele und Pläne zu deren Erreichung

Die Anforderungen in Kapitel 6.2 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 09

[EXI 09] Die vom Host festgelegten Informationssicherheitsziele müssen den Schutz von DSCP umfassen, die ihm von seinen Kunden anvertraut werden, sowie die Einhaltung der Verpflichtungen aus der DSGVO.

5.3.3. Planung von Änderungen

Es gelten die Anforderungen in Kapitel 6.3 der ISO 27001.

5.4. Medien

5.4.1. Ressourcen

Es gelten die Anforderungen nach Absatz 7.1 der ISO 27001.

5.4.2. Kompetenz

Es gelten die Anforderungen nach Absatz 7.2 der ISO 27001.

5.4.3. Bewusstsein

Die Anforderungen in Kapitel 7.3 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 10

[EXI 10] Personal, das für den Host arbeitet, muss auf die Kritikalität in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität der gehosteten DSCP aufmerksam gemacht werden.

Diese Anforderung gilt auch für das Personal aller Auftragsverarbeiter des Hosts.

5.4.4. Kommunikation

Die Anforderungen in Kapitel 7.4 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderungen:

Anforderung Nr. 11

[EXI 11] Der Host muss:

Eine Liste von Kontaktstellen für jeden Kunden führen. Diese Kontaktstelle muss in der Lage sein, dem Host eine medizinische Fachkraft zu benennen, die befugt ist, erforderlichenfalls Zugang zu den DSCP zu erhalten;
Diese Liste auf Verlangen unverzüglich an die zuständige Behörde übermitteln können, insbesondere im Falle der Aussetzung oder der Rücknahme der Zertifizierung.

.

Anforderung Nr. 12

[EXI 12] Der Host muss seinen Kunden mitteilen:

Eine Kopie der HDS-Konformitätsbescheinigung. Diese Kopie stellt für den Kunden des Hosts eine Garantie dar, dass die Konformitätsanforderungen erfüllt wurden;
Die Bescheinigung seiner Auftragsverarbeiter, die an der Hosting-Aktivität teilnehmen, wenn sie HDS-zertifiziert sind.

5.4.5. Dokumentierte Informationen

Es gelten die Anforderungen in Kapitel 7.5 der ISO 27001.

5.5. Betrieb

5.5.1. Betriebsplanung und -kontrolle

Die Anforderungen in Kapitel 8.1 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 13
[EXI 13] Der Host muss die Verteilung der Informationssicherheitsverantwortung zwischen dem Host und seinem Kunden planen und kontrollieren.

5.5.2. Risikoabschätzung

Es gelten die Anforderungen nach Absatz 8.2 der ISO 27001.

5.5.3. Risikobehandlung

Die Anforderungen in Kapitel 8.3 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 14
[EXI 14] Im Falle des Rückgriffs auf einen zertifizierten Auftragsverarbeiter für die Ausführung des Hosting-Dienstes oder eines Teils des Hosting-Dienstes sieht der Host ein Verfahren vor, um das Risiko des Verlusts oder der Aussetzung der Zertifizierung des Auftragsverarbeiters zu regeln.

5.6. Leistungsbeurteilung

5.6.1. Überwachung, Messung, Analyse und Auswertung

Die Anforderungen in Kapitel 9.1 der ISO 27001 gelten unter Berücksichtigung folgender Anforderung:

Anforderung Nr. 15
[EXI 15] Der Host muss es dem Kunden ermöglichen, die folgenden Überprüfungen des vorgeschlagenen Sicherheitsniveaus durchzuführen: Wenn der Host dem Kunden bestimmte Ressourcen zur Verfügung stellt, kann der Kunde technische Sicherheitsprüfungen nur für diese spezifischen Ressourcen durchführen oder in Auftrag geben. Die Organisation unterstützt den Kunden oder seine beauftragten Interessenträger bei der Aufrechterhaltung der Informationssicherheit während dieser Prüfungen; Auf Wunsch des Kunden muss der Host eine Management-Zusammenfassung eines technischen Prüfungsberichts über die im Rahmen der Dienstleistung gemeinsam genutzten Ressourcen vorlegen. Diese Prüfung muss von einem unabhängigen Prüfer durchgeführt werden und weniger als drei Jahre alt sein; Der Host muss es dem Kunden ermöglichen, die Spuren des Zugriffs auf die DSCP zu konsultieren, die von bestimmten Ressourcen oder von ihm kontrolliertem Personal durchgeführt werden; Der Host muss die Verfahren festlegen, die es seinem Kunden ermöglichen, seinen neuesten Bericht über die Prüfung der HDS-Zertifizierung einzusehen.

5.6.2. Interne Prüfung

5.6.2.1. Allgemeine Punkte

Die Anforderungen in Kapitel 9.2.1 der ISO 27001 gelten unter Berücksichtigung der folgenden Anforderung:

Anforderung Nr. 16

[EXI 16] Die vom Host durchgeführten internen Prüfungen müssen mindestens Folgendes umfassen:

Eine Prüfung, um festzustellen, ob das ISMS den Anforderungen dieses Rahmens entspricht und wirksam umgesetzt und aufrechterhalten wird;
Eine Überprüfung der Spuren des Zugangs von Personen, die im Auftrag der Organisation tätig sind, zu den DSCP oder zu den zu ihrer Verarbeitung verwendeten Systemen.

5.6.2.2. Internes Prüfungsprogramm

Es gelten die Anforderungen in Kapitel 9.2.2 der ISO 27001.

5.6.3. Überprüfung der Leitung

Es gelten die Anforderungen in Kapitel 9.3 der ISO 27001.

5.7. Verbesserung

Es gelten die Anforderungen in Kapitel 5.10 der ISO 27001.

6. ANFORDERUNGEN AN DAS VERTRAGSVERHÄLTNIS

Der Host ist verpflichtet, seinem Kunden einen Mustervertrag gemäß den regulatorischen Anforderungen zur Verfügung zu stellen.

HINWEIS – Insbesondere wird empfohlen, dass der Host, der als Auftragsverarbeiter seines Kunden fungiert, auf die von der Europäischen Kommission vorgeschlagenen Mustervertragsklauseln verweist, um die nach Artikel 28 der DSGVO erforderlichen Klauseln in den Vertrag aufzunehmen (L_2021199EN.01001801.xml (europa.eu)).

6.1. Konformitätsbescheinigung

Anforderung Nr. 17

[EXI 17] Gemäß Artikel R.1111-11 Absatz 11 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel enthalten, in der der Umfang der vom Host erhaltenen Konformitätsbescheinigung sowie seine Ausstellungs- und Erneuerungstermine erwähnt werden.

6.2. Beschreibung der erbrachten Leistungen

Anforderung Nr. 18

[EXI 18] Gemäß Artikel R.1111-11 Absatz 2 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel zur Beschreibung der erbrachten Dienstleistungen enthalten, einschließlich des Inhalts der Dienste und der erwarteten Ergebnisse, insbesondere zur Gewährleistung der Verfügbarkeit, Integrität, Vertraulichkeit und Prüfbarkeit der gehosteten Daten.

6.3. Wahrung der Rechte der betroffenen Personen

Anforderung Nr. 19

[EXI 19] Gemäß Artikel R.1111-11 Absatz 4 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel über die Maßnahmen enthalten, die zur Gewährleistung der Wahrung der Rechte der betroffenen Personen im Gesundheitsbereich durchgeführt werden. Diese Klausel muss folgende Angaben enthalten: die Verfahren zur Ausübung der Rechte auf Zugang, Berichtigung, Einschränkung, Widerspruch, Löschung und Übertragbarkeit von Daten (falls zutreffend), Verfahren für die Meldung einer Verletzung personenbezogener Daten an den für die Verarbeitung Verantwortlichen, die Verfahren für die Durchführung von Prüfungen durch den Datenschutzbeauftragten.

6.4. Bestellung eines Vertragsreferenten

Anforderung Nr. 20

[EXI 20] Gemäß Artikel R.1111-11 Absatz 5 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel enthalten, in der der Vertragsreferent des Kunden des Hosts genannt wird, der für die Behandlung von Vorfällen mit Auswirkungen auf die gehosteten Gesundheitsdaten kontaktiert werden soll.

6.5. Qualitäts- und Leistungsindikatoren

Anforderung Nr. 21

[EXI 21] Gemäß Artikel R. 1111-11 Absatz 6 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel enthalten, in der die Qualitäts- und Leistungsindikatoren festgelegt werden, die die Überprüfung des angekündigten Serviceniveaus, des garantierten Niveaus, der Periodizität ihrer Messung sowie des Vorliegens oder Fehlens von Sanktionen für die Nichteinhaltung dieser Indikatoren ermöglichen.

6.6. Nutzung von Unteraufträgen

Anforderung Nr. 22

[EXI 22] Gemäß Artikel R. 1111-11 Absatz 7 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag Informationen über die Bedingungen für die Nutzung externer technischer Dienstleister und die vom Host

eingegangenen Verpflichtungen enthalten, um sicherzustellen, dass eine solche Nutzung ein gleichwertiges Schutzniveau in Bezug auf die Verpflichtungen des Hosts gemäß Artikel 28.4 der DSGVO gewährleistet.

6.7. Zugriff auf gehostete persönliche Gesundheitsdaten

Anforderung Nr. 23

[EXI 23] Gemäß Artikel R.1111-11 Absatz 8 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag die Methoden zur Regulierung des Zugangs zu gehosteten personenbezogenen Gesundheitsdaten beschreiben.

6.8. Änderungen oder technische Entwicklungen

Anforderung Nr. 24

[EXI 24] Gemäß Artikel R. 1111-11 Absatz 9 des CSP muss der Hosting-Vertrag die Verpflichtungen des Hosts gegenüber seinem Kunden im Falle von Änderungen oder technischen Entwicklungen angeben, die von ihm eingeführt oder durch den geltenden Rechtsrahmen auferlegt werden.

Der Hosting-Vertrag muss auch die vorherige Zustimmung des Kunden für den Fall vorsehen, dass diese vom Host eingeführten Änderungen oder Entwicklungen nicht den folgenden Anforderungen entsprechen:

Die im Kapitel 6.5. geforderten Dienstgrade;
Die Garantien gemäß Kapitel 6.2 und.6.9.

6.9. Garantien

Anforderung Nr. 25

[EXI 25] Gemäß Artikel R.1111-11 Absatz 10 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag Informationen über die Garantien und Verfahren enthalten, die der Host zur Deckung etwaiger Versäumnisse seinerseits eingeführt hat.

6.10. Verbot der Verarbeitung gehosteter Daten

Anforderung Nr. 26

[EXI 26] Gemäß Artikel R.1111-11 Absatz 11 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag an das Verbot erinnern, dass der Host die gehosteten Gesundheitsdaten für andere Zwecke als die Durchführung der Aktivität des Hostings von Gesundheitsdaten verwenden darf.

6.11. Umkehrbarkeit

Anforderung Nr. 27

[EXI 27] Gemäß Artikel R. 1111-11 Absätze 12 bis 14 des CSP muss eine Klausel über die Umkehrbarkeit die Bedingungen für die Umkehrbarkeit am Ende der Dienstleistung oder im Falle einer vorzeitigen Beendigung des Dienstes enthalten, unabhängig von den Gründen, mit mindestens:

Die Verpflichtung, alle im Rahmen der Dienstleistung anvertrauten Informationen zurückzugeben;
Die Verpflichtung, alle Kopien dieser Informationen zu vernichten, sobald sie zurückgegeben wurden;
Die Verfahren zur Berechnung der Kosten und Fristen für die Rücksendung von Kopien;
Die Formate, in denen Gesundheitsdaten zum Zwecke der Übertragbarkeit zurückgegeben, gelesen und verwendet werden können, sowie gegebenenfalls die Modalitäten für den Umzug virtueller Maschinen/Container.

7. DATENHOHEIT

Anforderung Nr. 28

[EXI 28] Egal, welche DSCP-Hosting-Aktivität dem Kunden vom Host oder einem seiner Auftragsverarbeiter angeboten wird, und sofern es um die Speicherung von DSCP geht, muss der Host oder seine Auftragsverarbeiter diese DSCP ausschließlich innerhalb des Europäischen Wirtschaftsraums (EWR) speichern, unbeschadet der in Anforderung Nr. 29 genannten Fälle des Fernzugriffs. Der Host dokumentiert und teilt dem Kunden den Standort dieses Speichers mit.

Anforderung Nr. 29

[EXI 29] Bezieht sich der vom Host oder einem seiner Auftragsverarbeiter angebotene Dienst auf Fernzugriff aus einem Land, das nicht zum Europäischen Wirtschaftsraum (EWR) gehört, so muss dieser Zugang auf einem Angemessenheitsbeschluss der Kommission beruhen, der gemäß Artikel 45 der DSGVO erlassen wurde,[1] oder, falls dies nicht der Fall ist, auf eine der in Artikel 46 der Verordnung vorgesehenen geeigneten Garantien.

Im letzteren Fall unterrichtet der Host seinen Kunden über das Fehlen eines Angemessenheitsbeschlusses einerseits und über die geeigneten Garantien im Sinne von Artikel 46 der DSGVO, die zur Regelung dieses Fernzugriffs geschaffen wurden, andererseits.

Der Host unterrichtet den Kunden und dokumentiert die geeigneten Sicherheitsvorkehrungen sowie gegebenenfalls alle anderen Maßnahmen, um ein Datenschutzniveau zu gewährleisten, das dem durch das Unionsrecht garantierten Niveau entspricht.

In Bezug auf die in Anforderung Nr. 29 genannten zusätzlichen Maßnahmen sollte der Host den Empfehlungen des Europäischen Datenschutzausschusses 01/2020 zu Maßnahmen zur Ergänzung der Übertragungsinstrumente

[1] Die Liste der Länder, die ein angemessenes Schutzniveau gewährleisten, finden sich auf der CNIL-Website: www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

zur Gewährleistung der Einhaltung des EU-Schutzniveaus für personenbezogene Daten Rechnung tragen (Version 2.0, angenommen am 18. Juni 2021).

Anforderung Nr. 30

[EXI 30] Wenn der Host oder einer seiner am Hosting-Dienst beteiligten Auftragsverarbeiter den Rechtsvorschriften eines Drittlandes unterliegt, das kein angemessenes Schutzniveau im Sinne von Artikel 45 DSGVO bietet, muss der Host in dem Vertrag, der ihn an seinen Kunden bindet, angeben und die Vergabestelle darüber informieren:

- Die Liste der außereuropäischen Vorschriften, nach denen der Host oder einer seiner am Hosting-Dienst beteiligten Auftragsverarbeiter verpflichtet wäre, nach Unionsrecht unberechtigten Zugang zu den DSCP im Sinne von Artikel 48 der DSGVO zu ermöglichen;
- Die vom Host ergriffenen Maßnahmen zur Minderung der Risiken des unbefugten Zugangs zu DSCP, die durch diese außereuropäischen Vorschriften verursacht werden;
- Eine Beschreibung der Restrisiken des unbefugten Zugangs zu DSCP durch außereuropäische Regelungen, die trotz dieser Maßnahmen bestehen bleiben.

In Bezug auf diese Maßnahmen zur Minderung der in Anforderung Nr. 30 genannten Zugangsrisiken berücksichtigt der Host die Leitlinien des Europäischen Datenschutzausschusses 01/2020 über Maßnahmen zur Ergänzung von Übertragungsinstrumenten, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten sicherzustellen (Version 2.0, angenommen am 18. Juni 2021).

Anforderung Nr. 31

[EXI 31] Der Host veröffentlicht und aktualisiert die Kartierung der Übermittlungen von DSCP in ein Land außerhalb des Europäischen Wirtschaftsraums, einschließlich aller in Anforderung Nr. 29 genannten Fernzugriffe sowie der Beschreibung der Risiken des unbefugten Zugangs, die unter die Anforderung Nr. 30 fallen. Die Unterrichtung der Öffentlichkeit muss in folgender Form erfolgen:

- Wenn die zertifizierte Aktivität SecNumCloud-qualifiziert ist (Version 3.2), muss der Host folgende Informationen bereitstellen: „ Kein Risiko des Zugangs, das durch die Rechtsvorschriften eines Drittlandes unter Verstoß gegen EU-Recht auferlegt wird“;

- Wenn die zertifizierte Tätigkeit nicht von einer SecNumCloud-Qualifikation (Version 3.2) profitiert und keine Übertragung von DSCP in ein Land außerhalb des Europäischen Wirtschaftsraums beinhaltet, muss der Host folgende Informationen bereitstellen: „ Keine Übermittlung personenbezogener Gesundheitsdaten in ein Land außerhalb des Europäischen Wirtschaftsraums“;

- Wenn die zertifizierte Tätigkeit nicht von einer SecNumCloud-Qualifikation (Version 3.2) profitiert und eine oder mehrere Übertragungen von DSCP in ein Land außerhalb des Europäischen Wirtschaftsraums oder die Gefahr eines unbefugten Zugriffs gemäß Anforderung Nr. 30 umfasst, muss der Host die Informationen in der Tabelle in Kapitel 8 angeben.

Der Host muss diese Informationen der Öffentlichkeit auf einer speziellen Seite einer zugänglichen Website lesbar zugänglich machen und der Vergabestelle die URL der Seite mitteilen. Diese URL wird in der Liste der zertifizierten Hosts auf der ANS-Website veröffentlicht.

8. DARSTELLUNG DER GARANTIEN

Ziel dieses Kapitels ist es, Kunden von Gesundheitsdatenhosts mehr Transparenz in Bezug auf den Umfang des Dienstes zu bieten, der von der HDS-Zertifizierung abgedeckt wird. Es ermöglicht den Kunden eines Dienstes, sich über die verschiedenen Akteure zu informieren, auf die ihr Dienstleister angewiesen ist, um seine Dienstleistung zu erbringen.

Daher wird diese Standardbeschreibung verwendet, um die Akteure aufzulisten, die an der Verarbeitung von DSCP im Rahmen des vorgeschlagenen Hosting-Dienstes beteiligt sind.

Geschäftsbezeichnung des Akteurs	Rolle im Hosting-Dienst (Host/Auftragsverarbeiter des Hosts)	HDS-zertifiziert (ja/nein/ausgenommen)	SecNumCloud 3.2-qualifiziert	Hosting-Aktivitäten, an denen der Akteur beteiligt ist	Zugang zu personenbezogenen Gesundheitsdaten aus Ländern außerhalb des Europäischen Wirtschaftsraums durch den Host oder einen seiner Auftragsverarbeiter (Anforderung Nr. 29 des HDS-Rahmens)	Host oder Auftragsverarbeiter, für den das Risiko des Zugangs zu personenbezogenen Gesundheitsdaten aus Ländern außerhalb des Europäischen Wirtschaftsraums besteht, das durch die Rechtsvorschriften eines Drittlands unter Verstoß gegen EU-Recht auferlegt wird (Anforderung Nr. 30 des HDS-Rahmens)
	◻ Host ◻ Auftragsverarbeiter	◻ Ja ◻ Nein ◻ Ausgenommen	◻ Ja, kein Risiko eines unbefugten Zugriffs auf Daten, das unter die Anforderung Nr. 30 des HDS-Rahmens fallen ◻ Nein		◻ Ja ◻ Nein, kein Zugriff auf Daten aus einem Land außerhalb des Europäischen Wirtschaftsraums Falls ja, geben Sie das betreffende Land an: —von einem Angemessenheitsbeschluss im Sinne von Artikel 45 DSGVO abgedeckt: XX (Geben Sie das Land an) — nicht von einem Angemessenheitsbeschluss im Sinne von Artikel 45 DSGVO abgedeckt: XX (Geben Sie das Land an)	◻ Ja ◻ Nein Falls ja, geben Sie das betreffende Land an:

9. ZUSAMMENFASSUNG DER ANFORDERUNGEN

Anforderung Nr. 01

[EXI 01] Die Zertifizierung eines Hosts erfordert:

Dass er ein Informationssicherheitsmanagementsystem (ISMS) implementiert hat, das nach der Norm ISO 27001 zertifiziert ist, ergänzt durch die in Kapitel 5. definierten Anforderungen;
In der Erwägung, dass der Anwendungsbereich dieses ISMS alle Hosting-Aktivitäten für Gesundheitsdaten des Hosts abdeckt;
Mit seinen Kunden geschlossene Verträge erfüllen die Anforderungen des Kapitels6.;
Die Einhaltung der in Kapitel 7 festgelegten Souveränitätserfordernisse;
Dass er seinen Kunden die Vorlage der gemäß dem Kapitel formalisierten Garantien übermittelt.

Anforderung Nr. 02

[EXI 02] Bei der Festlegung seiner externen und internen Fragen muss der Host berücksichtigen, dass sein Auftrag von ihm verlangt, die ihm von seinen Kunden anvertrauten DSCP zu schützen.

Anforderung Nr. 03

[EXI 03] Bei der Festlegung der Anforderungen der betroffenen Parteien muss der Host den geltenden Rechtsrahmen für den Schutz der DSCP berücksichtigen.

Anforderung Nr. 04

[EXI 04] Der Anwendungsbereich des ISMS muss die gesamte vom Host bereitgestellte DSCP-Verarbeitung umfassen. Er muss alle Mittel und Prozesse der Verarbeitung von DSCP abdecken, einschließlich Backups und Übertragungen von materiellen Informationsmedien.

Anforderung Nr. 05

[EXI 05] Bei der Risikoabschätzung muss der Host mindestens folgende Ereignisse berücksichtigen:

A. Ausfall materieller Informationsmedien aufgrund physischer und umweltbedingter Bedrohungen.
B. Verlust der Kontrolle über materielle Informationsmedien, insbesondere während:
    a. Kopieren von DSCP auf tragbaren Medien;
    b. Jede Materialisierung in Papierformat;
    c. Umverteilung von Lagerräumen.
C. Beschädigung, Kompromittierung oder Unterbrechung eines internen oder externen Informationsflusses unter der Verantwortung des Hosts.

D. Nichtbeherrschung des gewährten Zugangs, unabhängig davon, ob es sich um Personal unter der Kontrolle der Organisation handelt, oder Personal, das von ihren Kunden benannt wurde:
   a. Zuteilung, Änderung und Entzug von Zugangsrechten;
   b. Verbreitung elektronischer Identifizierungsmittel;
   c. Rückverfolgbarkeit und Zurechenbarkeit des Zugangs;
   d. Gelegentlicher Zugriff bei Prüfungen und Intrusion-Tests.

E. Nichtbeherrschung von Interventionen, sei es auf Initiative der Organisation oder im Auftrag eines Kunden.

F. Unvorhergesehene Nutzung des Dienstes aufgrund von Ungeschicktheit oder böswilliger Absicht.

G. Hardware- oder Softwarefehler, die es unmöglich machen, die Geschäftskontinuität oder Wiederherstellungsverpflichtungen zu erfüllen.

H. Unterwerfung des Hosts oder eines Auftragsverarbeiters unter außereuropäische Rechtsvorschriften, die zu einem Verstoß gegen die DSCP führen können.

Anforderung Nr. 06

[EXI 06] Bei der Verwendung von Unteraufträgen hat der Host sicherzustellen, dass er Änderungen der technischen und organisatorischen Maßnahmen seiner Auftragsverarbeiter zur Bewältigung der festgestellten Risiken kontrolliert.

Anforderung Nr. 07

[EXI 07] Um das Risiko einer unvorhergesehenen Nutzung des Systems zu verringern, muss der Host sicherstellen, dass:

Die Schnittstellen, die den Kunden angeboten werden, mindestens in französischer Sprache verfügbar sind;
Die erste Stufe zumindest auf Französisch unterstützt wird. .

Anforderung Nr. 08

[EXI 08] Die Anwendbarkeitserklärung muss den Prüfern auf Anfrage in französischer Sprache zur Verfügung stehen.

Anforderung Nr. 09

[EXI 09] Die vom Host festgelegten Informationssicherheitsziele müssen den Schutz von DSCP umfassen, die ihm von seinen Kunden anvertraut werden, sowie die Einhaltung der Verpflichtungen aus der DSGVO.

Anforderung Nr. 10

[EXI 10] Personal, das für den Host arbeitet, muss auf die Kritikalität in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität der gehosteten DSCP aufmerksam gemacht werden.

Diese Anforderung gilt auch für das Personal aller Auftragsverarbeiter des Hosts.

Anforderung Nr. 11

[EXI 11] Der Host muss:

Eine Liste von Kontaktstellen für jeden Kunden führen. Diese Kontaktstelle muss in der Lage sein, dem Host eine medizinische Fachkraft zu benennen, die befugt ist, erforderlichenfalls Zugang zu den DSCP zu erhalten;
Diese Liste auf Verlangen unverzüglich an die zuständige Behörde übermitteln können, insbesondere im Falle der Aussetzung oder der Rücknahme der Zertifizierung.

.

Anforderung Nr. 12

[EXI 12] Der Host muss seinen Kunden mitteilen:

Eine Kopie der HDS-Konformitätsbescheinigung. Diese Kopie stellt für den Kunden des Hosts eine Garantie dar, dass die Konformitätsanforderungen erfüllt wurden;
Die Bescheinigung seiner Auftragsverarbeiter, die an der Hosting-Aktivität teilnehmen, wenn sie HDS-zertifiziert sind.

Anforderung Nr. 13

[EXI 13] Der Host muss die Verteilung der Informationssicherheitsverantwortung zwischen dem Host und seinem Kunden planen und kontrollieren.

Anforderung Nr. 14

[EXI 14] Im Falle des Rückgriffs auf einen zertifizierten Auftragsverarbeiter für die Ausführung des Hosting-Dienstes oder eines Teils des Hosting-Dienstes sieht der Host ein Verfahren vor, um das Risiko des Verlusts oder der Aussetzung der Zertifizierung des Auftragsverarbeiters zu regeln.

Anforderung Nr. 15

[EXI 15] Der Host muss es dem Kunden ermöglichen, die folgenden Überprüfungen des vorgeschlagenen Sicherheitsniveaus durchzuführen:

Wenn der Host dem Kunden bestimmte Ressourcen zur Verfügung stellt, kann der Kunde technische Sicherheitsprüfungen nur für diese spezifischen Ressourcen durchführen oder in Auftrag geben. Die Organisation unterstützt den Kunden oder seine beauftragten Interessenträger bei der Aufrechterhaltung der Informationssicherheit während dieser Prüfungen;
Auf Wunsch des Kunden muss der Host eine Management-Zusammenfassung eines technischen Prüfungsberichts über die im Rahmen der Dienstleistung gemeinsam genutzten Ressourcen vorlegen. Diese Prüfung muss von einem unabhängigen Prüfer durchgeführt werden und weniger als drei Jahre alt sein;
Der Host muss es dem Kunden ermöglichen, die Spuren des Zugriffs auf die DSCP zu konsultieren, die von bestimmten Ressourcen oder von ihm kontrolliertem Personal durchgeführt werden;
Der Host muss die Verfahren festlegen, die es seinem Kunden ermöglichen, seinen neuesten Bericht über die Prüfung der HDS-Zertifizierung einzusehen.

Anforderung Nr. 16

[EXI 16] Die vom Host durchgeführten internen Prüfungen müssen mindestens Folgendes umfassen:

Eine Prüfung, um festzustellen, ob das ISMS den Anforderungen dieses Rahmens entspricht und wirksam umgesetzt und aufrechterhalten wird;
Eine Überprüfung der Spuren des Zugangs von Personen, die im Auftrag der Organisation tätig sind, zu den DSCP oder zu den zu ihrer Verarbeitung verwendeten Systemen.

Anforderung Nr. 17

[EXI 17] Gemäß Artikel R.1111-11 Absatz 11 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel enthalten, in der der Umfang der vom Host erhaltenen Konformitätsbescheinigung sowie seine Ausstellungs- und Erneuerungstermine erwähnt werden.

Anforderung Nr. 18

[EXI 18] Gemäß Artikel R.1111-11 Absatz 2 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel zur Beschreibung der erbrachten Dienstleistungen enthalten, einschließlich des Inhalts der Dienste und der erwarteten Ergebnisse, insbesondere zur Gewährleistung der Verfügbarkeit, Integrität, Vertraulichkeit und Prüfbarkeit der gehosteten Daten.

Anforderung Nr. 19

[EXI 19] Gemäß Artikel R.1111-11 Absatz 4 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel über die Maßnahmen enthalten, die zur Gewährleistung der Wahrung der Rechte der betroffenen Personen im Gesundheitsbereich durchgeführt werden. Diese Klausel muss folgende Angaben enthalten: die Verfahren zur Ausübung der Rechte auf Zugang, Berichtigung, Einschränkung, Widerspruch, Löschung und Übertragbarkeit von Daten (falls zutreffend), Verfahren für die Meldung einer Verletzung personenbezogener Daten an den für die Verarbeitung Verantwortlichen, die Verfahren für die Durchführung von Prüfungen durch den Datenschutzbeauftragten.

Anforderung Nr. 20

[EXI 20] Gemäß Artikel R.1111-11 Absatz 5 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel enthalten, in der der Vertragsreferent des Kunden des Hosts genannt wird, der für die Behandlung von Vorfällen mit Auswirkungen auf die gehosteten Gesundheitsdaten kontaktiert werden soll.

Anforderung Nr. 21

[EXI 21] Gemäß Artikel R. 1111-11 Absatz 6 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag eine Klausel enthalten, in der die Qualitäts- und Leistungsindikatoren festgelegt werden, die die Überprüfung des angekündigten Serviceniveaus, des garantierten Niveaus, der Periodizität ihrer Messung sowie des Vorliegens oder Fehlens von Sanktionen für die Nichteinhaltung dieser Indikatoren ermöglichen.

Anforderung Nr. 22

[EXI 22] Gemäß Artikel R. 1111-11 Absatz 7 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag Informationen über die Bedingungen für die Nutzung externer technischer Dienstleister und die vom Host eingegangenen Verpflichtungen enthalten, um sicherzustellen, dass eine solche Nutzung ein gleichwertiges Schutzniveau in Bezug auf die Verpflichtungen des Hosts gemäß Artikel 28.4 der DSGVO gewährleistet.

Anforderung Nr. 23

[EXI 23] Gemäß Artikel R.1111-11 Absatz 8 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag die Methoden zur Regulierung des Zugangs zu gehosteten personenbezogenen Gesundheitsdaten beschreiben.

Anforderung Nr. 24

[EXI 24] Gemäß Artikel R. 1111-11 Absatz 9 des CSP muss der Hosting-Vertrag die Verpflichtungen des Hosts gegenüber seinem Kunden im Falle von Änderungen oder technischen Entwicklungen angeben, die von ihm eingeführt oder durch den geltenden Rechtsrahmen auferlegt werden.

Der Hosting-Vertrag muss auch die vorherige Zustimmung des Kunden für den Fall vorsehen, dass diese vom Host eingeführten Änderungen oder Entwicklungen nicht den folgenden Anforderungen entsprechen:

Die im Kapitel 6.5. geforderten Dienstgrade;
Die Garantien gemäß Kapitel 6.2 und 6.9.

Anforderung Nr. 25

[EXI 25] Gemäß Artikel R.1111-11 Absatz 10 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag Informationen über die Garantien und Verfahren enthalten, die der Host zur Deckung etwaiger Versäumnisse seinerseits eingeführt hat.

Anforderung Nr. 26

[EXI 26] Gemäß Artikel R.1111-11 Absatz 11 des CSP muss der zwischen dem Host und seinem Kunden geschlossene Hosting-Vertrag an das Verbot erinnern, dass der Host die gehosteten Gesundheitsdaten für andere Zwecke als die Durchführung der Aktivität des Hostings von Gesundheitsdaten verwenden darf.

Anforderung Nr. 27

[EXI 27] Gemäß Artikel R. 1111-11 Absätze 12 bis 14 des CSP muss eine Klausel über die Umkehrbarkeit die Bedingungen für die Umkehrbarkeit am Ende der Dienstleistung oder im Falle einer vorzeitigen Beendigung des Dienstes enthalten, unabhängig von den Gründen, mit mindestens:

Die Verpflichtung, alle im Rahmen der Dienstleistung anvertrauten Informationen zurückzugeben;
Die Verpflichtung, alle Kopien dieser Informationen zu vernichten, sobald sie zurückgegeben wurden;
Die Verfahren zur Berechnung der Kosten und Fristen für die Rücksendung von Kopien;
Die Formate, in denen Gesundheitsdaten zum Zwecke der Übertragbarkeit zurückgegeben, gelesen und verwendet werden können, sowie gegebenenfalls die Modalitäten für den Umzug virtueller Maschinen/Container.

Anforderung Nr. 28

[EXI 28] Egal, welche DSCP-Hosting-Aktivität dem Kunden vom Host oder einem seiner Auftragsverarbeiter angeboten wird, und sofern es um die Speicherung von DSCP geht, muss der Host oder seine Auftragsverarbeiter diese DSCP ausschließlich innerhalb des Europäischen Wirtschaftsraums (EWR) speichern, unbeschadet der in Anforderung Nr. 29 genannten Fälle des Fernzugriffs. Der Host dokumentiert und teilt dem Kunden den Standort dieses Speichers mit.

Anforderung Nr. 29

[EXI 29] Bezieht sich der vom Host oder einem seiner Auftragsverarbeiter angebotene Dienst auf Fernzugriff aus einem Land, das nicht zum Europäischen Wirtschaftsraum (EWR) gehört, so muss dieser Zugang auf einem Angemessenheitsbeschluss der Kommission beruhen, der gemäß Artikel 45 der DSGVO[2] erlassen wurde, oder, falls dies nicht der Fall ist, auf eine der in Artikel 46 der Verordnung vorgesehenen geeigneten Garantien.

Im letzteren Fall unterrichtet der Host seinen Kunden über das Fehlen eines Angemessenheitsbeschlusses einerseits und über die geeigneten Garantien im Sinne von Artikel 46 der DSGVO, die zur Regelung dieses Fernzugriffs geschaffen wurden, andererseits.

Der Host unterrichtet den Kunden und dokumentiert die geeigneten Sicherheitsvorkehrungen sowie gegebenenfalls alle anderen Maßnahmen, um ein Datenschutzniveau zu gewährleisten, das dem durch das Unionsrecht garantierten Niveau entspricht.

[2] Die Liste der Länder, die ein angemessenes Schutzniveau gewährleisten, finden sich auf der CNIL-Website: www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Anforderung Nr. 30

[EXI 30] Wenn der Host oder einer seiner am Hosting-Dienst beteiligten Auftragsverarbeiter den Rechtsvorschriften eines Drittlandes unterliegt, das kein angemessenes Schutzniveau im Sinne von Artikel 45 DSGVO bietet, muss der Host in dem Vertrag, der ihn an seinen Kunden bindet, angeben und die Vergabestelle darüber informieren:

- Die Liste der außereuropäischen Vorschriften, nach denen der Host oder einer seiner am Hosting-Dienst beteiligten Auftragsverarbeiter verpflichtet wäre, nach Unionsrecht unberechtigten Zugang zu den DSCP im Sinne von Artikel 48 der DSGVO zu ermöglichen;
- Die vom Host ergriffenen Maßnahmen zur Minderung der Risiken des unbefugten Zugangs zu DSCP, die durch diese außereuropäischen Vorschriften verursacht werden;
- Eine Beschreibung der Restrisiken des unbefugten Zugangs zu DSCP durch außereuropäische Regelungen, die trotz dieser Maßnahmen bestehen bleiben würden
- .

Anforderung Nr. 31

[EXI 31] Der Host veröffentlicht und aktualisiert die Kartierung der Übermittlungen von DSCP in ein Land außerhalb des Europäischen Wirtschaftsraums, einschließlich aller in Anforderung Nr. 29 genannten Fernzugriffe sowie der Beschreibung der Risiken des unbefugten Zugangs, die unter die Anforderung Nr. 30 fallen. Die Unterrichtung der Öffentlichkeit muss in folgender Form erfolgen:

- Wenn die zertifizierte Aktivität SecNumCloud-qualifiziert ist (Version 3.2), muss der Host folgende Informationen bereitstellen: „Kein Risiko des Zugangs, das durch die Rechtsvorschriften eines Drittlandes unter Verstoß gegen EU-Recht auferlegt wird“

- Wenn die zertifizierte Tätigkeit nicht von einer SecNumCloud-Qualifikation (Version 3.2) profitiert und keine Übertragung von DSCP in ein Land außerhalb des Europäischen Wirtschaftsraums beinhaltet, muss der Host folgende Informationen bereitstellen: „Keine Übermittlung personenbezogener Gesundheitsdaten in ein Land außerhalb des Europäischen Wirtschaftsraums“;

- Wenn die zertifizierte Tätigkeit nicht von einer SecNumCloud-Qualifikation (Version 3.2) profitiert und eine oder mehrere Übertragungen von DSCP in ein Land außerhalb des Europäischen Wirtschaftsraums oder die Gefahr eines unbefugten Zugriffs gemäß Anforderung Nr. 30 umfasst, muss der Host die Informationen in der Tabelle in Kapitel 8 angeben.

Der Host muss diese Informationen der Öffentlichkeit auf einer speziellen Seite einer zugänglichen Website lesbar zugänglich machen und der Vergabestelle die URL der Seite mitteilen. Diese URL wird in der Liste der zertifizierten Hosts auf der ANS-Website veröffentlicht.

Anhang 1: Korrespondenzmatrix mit SecNumCloud

In der folgenden Matrix wird die Übereinstimmung zwischen den einzelnen Maßnahmen in Anhang A der ISO 27001 und dem Anforderungskapitel des SecNumCloud v3.2-Rahmens erläutert. Beachten Sie, dass die Übereinstimmung nicht bedeutet, dass es eine Gleichwertigkeit zwischen einer ISO 27001-Maßnahme und einer SecNumCloud 3.2-Anforderung gibt.

Die Wirksamkeit der Maßnahmen ist für die HDS-Zertifizierung noch zu bewerten.

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
5.1 – Informationssicherheitsrichtlinien	5.2 – Informationssicherheitspolitik
5.2 – Funktionen und Verantwortlichkeiten im Zusammenhang mit der Informationssicherheit	6.1 – Funktionen und Verantwortlichkeiten im Zusammenhang mit der Informationssicherheit.
5.3 – Trennung der Pflichten	6.2 – Trennung der Pflichten
5.4 – Verantwortlichkeiten der Geschäftsführung	Keine entsprechende Anforderung
5.5 – Kontakte zu den Behörden	6.3 – Beziehungen zu den Behörden
5.6 – Kontakte zu bestimmten Interessengruppen	6.4 – Beziehungen zu besonderen Interessengruppen
5.7 – Bedrohungsüberwachung	Keine entsprechende Anforderung
5.8 – Informationssicherheit im Projektmanagement	6.5 – Informationssicherheit im Projektmanagement
5.9 – Bestandsaufnahme von Informationen und sonstigen damit verbundenen Vermögenswerten	8.1 – Inventar und Eigentum an Vermögenswerten
5.10 – Korrekte Verwendung von Informationen und anderen damit verbundenen Vermögenswerten	8.4 – Kennzeichnung und Handhabung von Informationen

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
5.11 – Rückgabe von Vermögenswerten	8.2 – Rückgabe von Vermögenswerten
5.12 – Klassifizierung von Informationen	8.3 – Identifikation
5.13 – Kennzeichnung von Informationen	8.4 – Kennzeichnung und Handhabung von Informationen
5.14 – Übermittlung von Informationen	10.2 – Fluss-Verschlüsselung
5.15 – Zugangskontrolle	9.1 – Zugriffsrichtlinien und -kontrolle
5.16 – Identitätsmanagement	9.2 – Benutzerregistrierung und Abmeldung
5.17 – Authentifizierungsinformationen	10.3 – Hashing von Passwörtern
5.18 – Zugangsrechte	9.2 – Benutzerregistrierung und Abmeldung 9.4 – Überprüfung der Benutzerzugangsrechte
5.19 – Informationssicherheit in Lieferantenbeziehungen	15.1 – Identifizierung Dritter
5.20 – Informationssicherheit in Lieferantenverträgen	15.2 – Sicherheit in Drittverträgen 15.5 – Vertraulichkeitsverpflichtungen
5.21 – Informationssicherheitsmanagement in der Lieferkette der Informations- und Kommunikationstechnologie (TIC)	15.1 – Identifizierung Dritter 15.3 – Überwachung und Überprüfung von Diensten Dritter

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
5.22 – Überwachung, Überprüfung und Verwaltung von Änderungen bei Lieferantendienstleistungen	15.3 – Überwachung und Überprüfung von Diensten Dritter
5.23 – Informationssicherheit bei der Nutzung von Cloud-Diensten	15.1 – Identifizierung Dritter 15.3 – Überwachung und Überprüfung von Diensten Dritter 19.6 – Immunität von Nicht-EU-Recht (d)
5.24 – Planung und Vorbereitung des Managements von Informationssicherheitsvorfällen	16.1 – Zuständigkeiten und Verfahren
5.25 – Bewertung von Informationssicherheitsereignissen und Entscheidungsfindung	16.3 – Bewertung von Informationssicherheitsereignissen und Entscheidungsfindung
5.26 – Reaktion auf Informationssicherheitsvorfälle	16.4 – Reaktion auf Vorfälle im Zusammenhang mit der Informationssicherheit
5.27 – Aus Informationssicherheitsvorfällen lernen	16.5 – Aus Vorfällen im Zusammenhang mit der Informationssicherheit lernen
5.28 – Sammlung von Beweismitteln	16.6 – Sammeln von Beweismitteln
5.29 – Informationssicherheit bei Störungen	Keine entsprechende Anforderung
5.30 – Vorbereitung von TICs für die Geschäftskontinuität	17.4 – Verfügbarkeit von Informationsverarbeitungsressourcen
5.31 – Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	18.1 – Ermittlung der anwendbaren Rechtsvorschriften und vertraglichen Anforderungen
5.32 – Rechte des geistigen Eigentums	Keine entsprechende Anforderung

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
5.33 – Schutz von Aufzeichnungen	Keine entsprechende Anforderung
5.34 – Schutz der Privatsphäre und personenbezogener Daten (DCP)	19.5 – Schutz der personenbezogenen Daten.
5.35 – Unabhängiges Prüfung der Informationssicherheit	18.2 – Unabhängige Überprüfung der Informationssicherheit
5.36 – Einhaltung von Informationssicherheitsrichtlinien, -regeln und -normen	18.3 – Einhaltung von Sicherheitsrichtlinien und -normen 18.4 – Prüfung der technischen Übereinstimmung
5.37 – Dokumentierte Betriebsabläufe	12.1 – Dokumentierte Betriebsabläufe
6.1 – Auswahl der Kandidaten	7.1 – Auswahl der Kandidaten
6.2 – Arbeits- und Beschäftigungsbedingungen	7.2 – Bedingungen für die Einstellung
6.3 – Sensibilisierung, Ausbildung und Schulung im Bereich der Informationssicherheit	7.3 – Sensibilisierung, Ausbildung und Schulung im Bereich der Informationssicherheit
6.4 – Disziplinarverfahren	7.4 – Disziplinarverfahren
6.5 – Verantwortlichkeiten nach Beendigung oder dem Wechsel der Beschäftigung	7.5 – Verletzung, Beendigung oder Änderung des Arbeitsvertrags
6.6 – Vertraulichkeits- oder Geheimhaltungsvereinbarungen	15.5 – Vertraulichkeitsverpflichtungen
6.7 – Fernarbeit	12.12 – Verwaltung (c) 12.13 – Ferndiagnose und Fernwartung von Infrastrukturkomponenten

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
6.8 – Meldung von Informationen Sicherheitsereignisse	16.2 – Warnungen im Zusammenhang mit der Informationssicherheit
7.1 – Physische Sicherheitsumstände	11.1 – Physische Sicherheitsumstände
7.2 – Physikalische Eingaben	11.2 – Physische Zutrittskontrolle 11.5 – Liefer- und Verladebereiche
7.3 – Absicherung von Büros, Räumen und Geräten	Keine entsprechende Anforderung
7.4 – Physische Sicherheitsüberwachung	11.2.1 – Private Bereiche (h) 11.2.2 – Empfindliche Bereiche (h)
7.5 – Schutz vor äußeren und ökologischen Bedrohungen	11.3 – Schutz vor äußeren und ökologischen Bedrohungen
7.6 – Arbeiten in sicheren Bereichen	11.4 – Arbeit in privaten und sensiblen Bereichen
7.7 – Sauberer Schreibtisch und leerer Bildschirm	Keine entsprechende Anforderung
7.8 – Standort und Schutz der Ausrüstung	11.10 – Ausrüstung, die auf Gebrauch wartet
7.9 – Sicherheit von Vermögenswerten außerhalb des Gebäudes	Keine entsprechende Anforderung
7.10 – Speichermedien	11.8 – Beseitigung von Vermögenswerten

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
7.11 – Unterstützungsdienste	11.3 – Schutz vor äußeren und ökologischen Bedrohungen 11.7 – Wartung der Ausrüstung
7.12 – Verkabelungssicherheit	11.6 – Verkabelungssicherheit
7.13 – Wartung der Geräte	11.7 – Wartung der Ausrüstung
7.14 – Sichere Entsorgung oder Recycling von Geräten	11.9 – Sicheres Recycling von Geräten
8.1 – Endgeräte von Nutzern	12.12 – Verwaltung
8.2 – Privilegierte Zugangsrechte	9.3 – Verwaltung von Zugangsrechten
8.3 – Beschränkung des Zugriffs auf Daten	9.7 – Beschränkung des Zugriffs auf Daten
8.4 – Zugriff auf Quellcodes	Keine entsprechende Anforderung
8.5 – Sichere Authentifizierung	9.5 – Verwalten von Benutzerauthentifizierungen
8.6 – Bemessung	Keine entsprechende Anforderung
8.7 – Schutz vor Malware	12.4 – Maßnahmen gegen Schadcode

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
8.8 – Management von technischen Schwachstellen	12.11 – Management von technischen Schwachstellen
8.9 – Konfigurationsmanagement	18.2.1 – Erste Überprüfung 18.2.2 – Überprüfung der wichtigsten Änderungen
8.10 – Löschung von Informationen	11.9 – Sicheres Recycling von Geräten 19.4 – Vertragsende
8.11 – Maskierung von Daten	Keine entsprechende Anforderung
8.12 – Vermeidung von Datenlecks	12.14 – Überwachung von Infrastrukturabflüssen 19.6 – Immunität gegen Nicht-EU-Recht
8.13 – Sicherung von Informationen	12.5 – Sicherung von Informationen 17.5 – Sicherung der Konfiguration der technischen Infrastruktur 17.6 – Bereitstellung eines Backup-Systems der Daten des Sponsors
8.14 – Redundanz von Datenverarbeitungsressourcen	17.1 – Organisation der Geschäftskontinuität 17.2 – Umsetzung der Geschäftskontinuität 17.3 – Überprüfung, Überarbeitung und Bewertung der Geschäftskontinuität
8.15 – Protokollierung	12.6 – Ereignisprotokolle 12.7 – Schutz von protokollierten Informationen 12.9 – Analyse und Korrelation von Ereignissen
8.16 – Überwachungstätigkeiten	13.3 – Überwachung des Netzes
8.17 – Synchronisation der Uhren	12.8 – Synchronisation der Uhren

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
8.18 – Nutzung privilegierter Dienstprogramme	Keine entsprechende Anforderung
8.19 – Installation von Software auf Betriebssystemen	12.10 – Installation von Software auf in Betrieb befindlichen Systemen
8.20 – Netzwerksicherheit	13.1 – Kartierung des Informationssystems 13.2 – Netzwerkpartitionierung
8.21 – Sicherheit von Netzwerkdiensten	9.6 – Zugang zu Verwaltungsdiensten 13.2 – Netzwerkpartitionierung (d, e)
8.22 – Netzwerkpartitionierung	13.2 – Netzwerkpartitionierung
8.23 – Webfilterung	13.2 – Netzwerkpartitionierung (c)
8.24 – Verwendung von Kryptographie	10.4 – Nichtabstreitbarkeit 10.5 – Verwaltung von Geheimnissen 10.6 – Wurzeln des Vertrauens
8.25 – Sicherer Entwicklungslebenszyklus	14.1 – Sichere Entwicklungspolitik
8.26 – Anforderungen an die Anwendungssicherheit	5.3 – Risikoabschätzung
8.27 – Technische und architektonische Grundsätze für sichere Systeme	Keine entsprechende Anforderung
8.28 – Sichere Codierung	18.2.2 – Erste Überprüfung 18.2.3 – Überprüfung der wichtigsten Änderungen

Maßnahme Anhang A	Anwendbare SecNumCloud-Anforderungen
8.29 – Sicherheitstests in Entwicklung und Akzeptanz	14.6 – Sicherheitstests und Systemkonformität
8.30 – Ausgelagerte Entwicklung	14.5 – Ausgelagerte Entwicklung
8.31 – Trennung von Entwicklungs-, Test- und Betriebsumgebungen	12.3 – Trennung von Entwicklungs-, Test- und Betriebsumgebungen 14.4 – Sichere Entwicklungsumgebung
8.32 – Änderungsmanagement	12.2 – Änderungsmanagement 14.2 – Systemänderungskontrollverfahren 14.3 – Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform
8.33 – Prüfinformationen	14.7 – Schutz der Prüfdaten
8.34 – Schutz von Informationssystemen bei Kontrolltesten	Keine entsprechende Anforderung

Zwei SecNumCloud-Anforderungen sind nicht mit ISO 27001-Referenzmaßnahmen korreliert, sondern teilweise in den vertraglichen oder zusätzlichen ISMS-Anforderungen zu finden:

- Anforderungen an den Inhalt der Dienstleistungsvereinbarung (19.1 von SecNumCloud);
- Datenlokalisierungsanforderungen (19.2 von SecNumCloud).

AGENCE DU NUMÉRIQUE EN SANTÉ

HDS-Akkreditierungsrahmen

Status: Validierung im Gange | *Klassifikation: Öffentlich* | *Fassung: v2023 – zu validieren*

Agence du numérique en santé (Agentur für digitale Gesundheit)
2-10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Referenzdokumente

Referenznummer 1: NF EN ISO/IEC 17021-1:2015

Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme prüfen und zertifizieren

Referenznummer 2: NF ISO/IEC 27001:2022

Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen

Referenznummer 3: HDS-Zertifizierungsrahmenanforderungen v2023

Referenznummer 4: IAF MD1-Version in Kraft

IAF-Anforderungendokument für Multi-Site-Zertifizierung durch Probenahme

Referenznummer 5: IAF MD2-Version in Kraft

IAF-Anforderungendokument für die Übertragung der Zertifizierung des Managementsystems unter Akkreditierung

Referenznummer 6: IAF MD4-Version in Kraft

IAF-Anforderungendokument für den Einsatz computergestützter Prüfungstechniken („CAAT“) für akkreditierte Managementsystemzertifizierungen

Referenznummer 7: IAF MD5-Version in Kraft

Ermittlung der Prüfzeit von Qualitätsmanagementsystemen und Umweltmanagementsystemen

Referenznummer 8: IAF MD11-Version in Kraft

IAF-Anforderungsdokument für die Anwendung von ISO/IEC 17021 für Prüfung von integrierten Verwaltungssystemen (IMS)

Die IAF-Anforderungen sind auf der IAF-Website abrufbar.

INHALT

10. EINLEITUNG

10.1. Zweck des Dokuments

Dieses Dokument richtet sich an Zertifizierungsstellen, die für die Zertifizierung von Gesundheitsdatenhosts akkreditiert werden möchten. Es beschreibt das Akkreditierungsverfahren für Zertifizierungsstellen und das Zertifizierungsverfahren für Hosts.

10.2. Struktur des Dokuments

Dieses Dokument besteht aus sieben Teilen und zwei Anhängen:

- Einführung des Dokuments;
- Beschreibung des Anwendungsbereichs des Akkreditierungsrahmens;
- Beschreibung der im Rahmen des Akkreditierungsrahmens geltenden Normen;
- Liste der im Akkreditierungsrahmen verwendeten Akronyme;
- Beschreibung der Bedingungen, Kriterien und Verfahren für die Akkreditierung von Zertifizierungsstellen;
- Festlegung der Zuständigkeiten der Akkreditierungsstellen;
- Beschreibung der Bedingungen, Kriterien und Verfahren für die Zertifizierung von Hosts.

Anhänge

- Anhang A mit den erforderlichen Elementen zur Bestimmung der Prüfdauer für die HDS-Zertifizierung;
- Anhang B mit den Mustern für Dokumente, die von den Zertifizierungsstellen für die Übermittlung von Informationen an die zuständige Behörde zu verwenden sind.
- .

10.2.1. Begriffsbestimmungen

10.2.1.1. Akteur

Alle Interessenträger, die zur Sicherheit personenbezogener Gesundheitsdaten beitragen, mit Ausnahme des Verantwortlichen und der Auftragsverarbeiter eines zertifizierten Hosts, wenn sie in Übereinstimmung mit der Sicherheitspolitik und unter der Aufsicht des genannten Hosts handeln

10.2.1.2. Verwaltung und Betrieb des Informationssystems mit Gesundheitsdaten

Die Tätigkeit der Verwaltung und des Betriebs des Informationssystems, das Gesundheitsdaten enthält, besteht darin, die Eingriffe in die Ressourcen zu beherrschen, die dem Kunden des Hosts zur Verfügung gestellt werden. Es umfasst alle folgenden Nebentätigkeiten:

- Festlegung eines Verfahrens für die Zuweisung und jährliche Überprüfung nominativer, gerechtfertigter und notwendiger Zugangsrechte;
- Sicherung des Zugangsverfahrens;
- das Sammeln und Bewahren von Spuren der vorgenommenen Zugriffe und der Gründe dafür;
- vorherige Validierung von Interventionen (Interventionsplan, Interventionsprozess).

Die Validierung von Interventionen besteht darin, sicherzustellen, dass sie die Sicherheit der gehosteten Informationen weder für den betreffenden Kunden noch für die anderen Kunden des Hosts beeinträchtigen. Diese Validierung kann in folgenden Fällen durchgeführt werden:

- a priori für Eingriffe, die der Kunde unabhängig durchführen kann;
- wenn vom Host ein Service angefordert wird.

Die Definition des Zuteilungsverfahrens, der Sicherheit, der Erhebung und Validierung ist für die in Artikel R. 1111-9 Absätze 1 bis 4 des Code de la santé publique definierten Tätigkeiten intrinsisch und obligatorisch. Werden sie ausschließlich durchgeführt, soweit sie mit den Tätigkeiten 1 bis 4 verbunden und substanziell sind, ist der Host nicht verpflichtet, für die Aktivität 5 zertifiziert zu sein. Dies ist nur für den Fall erforderlich, dass er nur Aktivität 5 ausführt.

10.2.1.3. Kunde des Hosts

Der Kunde des Hosts (auch als „Kunde“ bezeichnet) bezeichnet die natürliche oder juristische Person, die den vom Host bereitgestellten Dienst abonniert.

10.2.1.4. Host

Der Host, der auch als Organisation in der ISO 27001-Norm bezeichnet wird, ist der Antragsteller für die Zertifizierung als Host von Gesundheitsdaten oder für die Erneuerung seiner Zertifizierung. Er bietet ganz oder teilweise einen Hosting-Dienst für persönliche Gesundheitsdaten (oder „Gesundheitsdaten“).

10.2.1.5. Elektronische Identifizierungsmittel

Ein elektronisches Identifizierungsmittel ist ein materielles oder immaterielles Element, das personenbezogene Identifizierungsdaten enthält und zur Authentifizierung bei einem Online-Dienst verwendet wird.

10.2.1.6. Für die Datenverarbeitung Verantwortlicher

Der Verantwortliche im Sinne der Verordnung 2016/679 bezeichnet die natürliche oder juristische Person, Behörde, Dienstleistung oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung bestimmt.

11. GELTUNGSBEREICH

11.1. Anwendbarkeit des HDS-Zertifizierungsrahmens

Der Anwendungsbereich des Rahmens wird in den Artikeln L. 1111-8, R. 1111-8-8 und R. 1111-9 des Code de la santé publique festgelegt.

11.1.1. Rolle des Hosts

Die HDS-Zertifizierung gilt für jede natürliche oder juristische Person, die einen Hosting-Dienst ganz oder teilweise für personenbezogene Gesundheitsdaten erbringt und ein Auftragsverarbeiter im Sinne von Artikel 28 der DSGVO ist.

11.1.2. Art der Daten

Die gehosteten Daten müssen personenbezogene Daten sein, die sich auf die Gesundheit beziehen, wie in Artikel 4.15 der DSGVO definiert.

11.1.3. Kontext der Sammlung

Die HDS-Zertifizierung betrifft persönliche Gesundheitsdaten, die während der Prävention, Diagnose, Pflege oder sozialen oder medizinischen Follow-up-Aktivitäten erhoben werden.

Diese personenbezogenen Gesundheitsdaten müssen im Auftrag folgender Personen gespeichert werden:

die natürlichen oder juristischen Personen, die für die Erstellung oder Erhebung der Daten verantwortlich sind;

oder den Patienten selbst.

11.1.4. Durchgeführte Tätigkeiten

Artikel R. 1111-9 des CSP definiert die Tätigkeit des Hostings von Gesundheitsdaten.

Die Bereitstellung aller oder einiger der folgenden Tätigkeiten im Namen des für die Verarbeitung Verantwortlichen gemäß Artikel R. 1111-8-8 I Absatz 1 oder des Patienten gemäß I Absatz 2 desselben Artikels gilt als das Hosting personenbezogener Gesundheitsdaten im digitalen Format im Sinne von Artikel L. 1111-8 II:

1. Bereitstellung und Aufrechterhaltung der Betriebsfähigkeit von physischen Standorten, an denen die materielle Infrastruktur des für die Verarbeitung der Gesundheitsdaten verwendeten Informationssystems gehostet werden kann;

2. Bereitstellung und Aufrechterhaltung der Betriebsfähigkeit der materiellen Infrastruktur des für die Verarbeitung der

Gesundheitsdaten verwendeten Informationssystems;

3. Bereitstellung und Aufrechterhaltung der Betriebsfähigkeit der virtuellen Infrastruktur des für die Verarbeitung der Gesundheitsdaten verwendeten Informationssystems;

4. Bereitstellung und Aufrechterhaltung der Betriebsfähigkeit der Hosting-Plattform für Anwendungen des Informationssystems;

5. Verwaltung und Betrieb des Informationssystems, in dem die Gesundheitsdaten enthalten sind;

6. Sicherung von Gesundheitsdaten.

Aktivität 5 ist in Absatz 2.1.2 festgelegt.

Die Aktivität 6 zur Datensicherung sollte so interpretiert werden, dass sie nur ausgelagerte Backups einschließt. Die Backups, die für die Aktivitäten 1 bis 5 von Natur aus notwendig sind, fallen in den Rahmen der Aktivitäten 1 bis 5.

12. NORMATIVE VERWEISE

Die unten aufgeführten Dokumente werden in diesem Rahmen normativ referenziert und sind für ihre Anwendung unabdingbar.

NF IN ISO 27001:2023, *Informationssicherheit, Cybersicherheit und Datenschutz – Managementsysteme für Informationssicherheit – Anforderungen*

NF IN ISO/IEC 17021-1:2015, *Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1: Anforderungen*

Im Rest des Dokuments werden Verweise auf diese Normen wie folgt gemacht:

- NF ISO 27001 für die Norm NF EN ISO 27001:2023;
- NF ISO 17021-1 für die Norm NF EN ISO/IEC 17021-1:2015.

13. VERWENDETE AKRONYME

COFRAC	Comité Français d'Accréditation (Französischer Akkreditierungsausschuss)
DDA	Déclaration d'Applicabilité documentée – Dokumentierte Erklärung über die Anwendbarkeit der Sicherheitsziele sowie geeignete und anwendbare Maßnahmen für das Informationssicherheitsmanagementsystem einer Organisation
HDS	Hébergeur de Données de Santé (Gesundheitsdatenhost)
IAF	International Accreditation Forum
CEI/IEC	Internationale Elektrotechnische Kommission/International Electrotechnical Commission
ISO	International Organization for Standardization
OC	Organisme de Certification (Zertifizierungsstelle)

14. BEDINGUNGEN, KRITERIEN UND VERFAHREN FÜR DIE AKKREDITIERUNG

Die Bedingungen, Kriterien und Verfahren für die Akkreditierung basieren auf den Standards der NF ISO 17021-1. Die Akkreditierung bescheinigt die Kompetenz, Unparteilichkeit und Zuverlässigkeit einer Stelle, um die Einhaltung der festgelegten und formalisierten Anforderungen zu überprüfen. Die Akkreditierung ist eine sogenannte Prüfung der zweiten Ebene, die darauf abzielt, die Funktionsweise des Kontrolleurs zu kontrollieren.

14.1. Akkreditierungsbedingungen und -kriterien

Zertifizierungsstellen, die zur Ausstellung von HDS-Konformitätsbescheinigungen zugelassen sind, müssen von einer nationalen Akkreditierungsstelle im Sinne der Verordnung (EG) Nr. 765/2008 (COFRAC in Frankreich oder deren Äquivalent in anderen Ländern, die multilaterale internationale Anerkennungsabkommen unterzeichnet haben) gemäß diesem Akkreditierungsrahmen akkreditiert werden, der regelmäßig überprüft wird, um technologische Entwicklungen in Gesundheitsinformationssysteme sowie Änderungen in den Hostingberufen einzubeziehen.

Der Antrag und die Einhaltung der Anforderungen des Akkreditierungsrahmens stellen sicher, dass akkreditierte Stellen für die Ausstellung von HDS-Zertifizierungen zuständig sind.

Die Akkreditierung umfasst die Bewertung von Stellen, die als Host personenbezogener Gesundheitsdaten zertifiziert werden möchten.

Damit eine Stelle für die Erteilung von HDS-Zertifizierungen akkreditiert werden kann, muss sie gemäß den Anforderungen der NF ISO 17021-1 akkreditiert sein und die geltenden Regeln für die Prüfung und Zertifizierung von Sicherheitsmanagementsystemen von Informationssystemen gemäß ISO 27001 anwenden. Darüber hinaus definiert dieser Akkreditierungsrahmen die spezifischen Anforderungen, die für die HDS-Zertifizierung gelten.

14.2. Akkreditierungsanforderungen

14.2.1. Allgemeine Anforderungen

14.2.1.1. Vertrags- und Rechtsbereich

Es gelten die Anforderungen des § 5.1 der NF ISO 17021-1.

14.2.1.2. Unparteilichkeitsmanagement

Es gelten die Anforderungen des § 5.2 der NF ISO 17021-1.

14.2.1.3. Verantwortung und Finanzierung

Es gelten die Anforderungen des § 5.3 der NF ISO 17021-1.

14.2.2. Strukturelle Anforderungen:

14.2.2.1. Kompetenz des Personals

Es gelten die Anforderungen des § 7.1 der NF ISO 17021-1.

Bei der Auswahl des Prüfungsteams stellt die Zertifizierungsstelle sicher, dass die für jeden Auftrag vermittelten Fähigkeiten angemessen sind. Das Team muss über ausreichende Kenntnisse der Informationssicherheit, des Hostings sensibler Daten und der Dienste verfügen, die von Gesundheitsdatenhosts angeboten werden.

Insbesondere müssen die Prüfer der Zertifizierungsstelle, die an HDS-Zertifizierungstätigkeiten beteiligt ist, nachweisen können, dass sie über Fähigkeiten im Bereich der Sicherheit der Informationssysteme und insbesondere der Gesundheitsinformationssysteme verfügen.

Die Leitung der Zertifizierungsstelle muss die Prozesse definieren und über die erforderlichen Ressourcen verfügen, um festzustellen, ob die Prüfer für die im Rahmen der HDS-Zertifizierung zu erfüllenden Aufgaben kompetent sind oder nicht. Die Zertifizierungsstelle muss in der Lage sein, ihren Kunden die Fähigkeiten ihres an den Zertifizierungstätigkeiten beteiligten Personals mitzuteilen.

14.2.2.2. An Zertifizierungsmaßnahmen beteiligtes Personal

Es gelten die Anforderungen des § 7.2 der NF ISO 17021-1.

Das Prüfungsteam kann durch Sachverständige verstärkt werden. Diese Sachverständigen ersetzen nicht die Prüfer, sondern unterstützen sie bei Fragen der Angemessenheit der Sicherheit und der Geräte, die zum Hosting von Gesundheitsdaten verwendet werden.

Es wird empfohlen, dass Sachverständige über spezifische Fähigkeiten im Bereich der Gesundheit verfügen, die durch Schulungen oder ein Projekt erworben werden.

Die Zertifizierungsstelle muss über ein Verfahren verfügen, das Folgendes ermöglicht:

- Auswahl von Prüfern und technischen Sachverständigen auf der Grundlage ihrer Fähigkeiten, Schulungen, Qualifikationen und Erfahrungen;
- Bewertung des Verhaltens von Prüfern und Sachverständigen bei Zertifizierungs- und Überwachungsprüfungen.

14.2.2.3. Intervention einzelner externer Prüfer und Sachverständiger

Es gelten die Anforderungen des § 7.3 der NF ISO 17021-1.

14.2.2.4. Personalaufzeichnungen

Es gelten die Anforderungen des § 7.4 der NF ISO 17021-1.

14.2.2.5. Auslagerung

Es gelten die Anforderungen des § 7.5 der NF ISO 17021-1.

14.2.3. Informationspflichten

14.2.3.1. Öffentlich zugängliche Informationen

Es gelten die Anforderungen des § 8.1 der NF ISO 17021-1.

14.2.3.2. Zertifizierungsunterlagen

Es gelten die Anforderungen des § 8.2 der NF ISO 17021-1.

Die Zertifizierungsstelle stellt jedem ihrer zertifizierten Kunden, die personenbezogene Gesundheitsdaten beherbergen, Unterlagen zur Verfügung, die ihre Zertifizierung bescheinigen.

Diese Dokumente müssen:

- den Umfang der zertifizierten Dienstleistung in Bezug auf die Tätigkeiten gemäß Kapitel 2 „Anwendungsbereich“, insbesondere die Liste der zertifizierten Tätigkeiten, spezifizieren;
- die ISO-Normen angeben, für die die Organisation bereits zertifiziert ist und die geltenden Anforderungen erfüllt (NF ISO 27001).
- den Standort (zumindest das Land) aller Standorte im Rahmen der Zertifizierung angeben.

Wird eine ISO 27001-Zertifizierung von einer anderen OC als der, die die HDS-Zertifizierung ausstellt, ausgestellt, so muss in dem Zertifikat ausdrücklich angegeben werden, dass es gültig ist, vorbehaltlich der Erlangung einer gültigen ISO 27001-Zertifizierung für denselben Umfang.

Hinweis

Wenn Auftragsverarbeiter beauftragt werden, erscheinen ihre Standorte nicht auf der Bescheinigung.

14.2.3.3. Hinweis auf Zertifizierung und Verwendung von Marken

Es gelten die Anforderungen des § 8.3 der NF ISO 17021-1.

14.2.3.4. Geheimhaltung

Es gelten die Anforderungen des § 8.4 der NF ISO 17021-1.

Vor einem Eingreifen des Prüfungsteams muss die Zertifizierungsstelle gemeinsam mit dem Antragsteller sicherstellen, dass die während der Prüfung bereitzustellenden Informationen keine personenbezogenen Gesundheitsdaten oder vertrauliche oder sensible Daten enthalten. Gegebenenfalls müssen die

Zertifizierungsstelle und der Antragsteller festlegen, wie auf das zu prüfende System zuzugreifen ist (Vertraulichkeitsverpflichtung usw.).

Im Falle der Unfähigkeit, das Informationssystem ohne Zugang zu personenbezogenen Gesundheitsdaten oder anderen vertraulichen oder sensiblen Daten zu überprüfen, muss die Zertifizierungsstelle den Antragsteller informieren, eine Vertraulichkeitsvereinbarung erstellen und einen Gesundheitsfachmann, der unter der Verantwortung des Kunden handelt, informieren.

Kapitel 8.4.2 der Norm NF ISO 17021-1 wird wie folgt ergänzt: personenbezogene Gesundheitsdaten und sonstige vertrauliche oder sensible Daten, auf die die Zertifizierungsstelle im Rahmen der Prüfung Zugriff haben kann, dürfen weder von der Zertifizierungsstelle noch vom Zertifizierungsantragsteller offengelegt oder wiederverwendet werden.

14.2.3.5. Informationsaustausch mit der zuständigen Behörde

14.2.3.5.1. HDS-Aussetzungsbericht

Die Zertifizierungsstelle teilt der zuständigen Behörde in französischer oder englischer Sprache jede Entscheidung zur Aussetzung der Zertifizierung eines Hosts von Gesundheitsdaten mit.

Die nachstehenden Informationen über den Gesundheitsdatenhost, dessen Zertifizierung ausgesetzt wurde, sind mitzuteilen:

- Bezeichnung oder Geschäftsbezeichnung des Gesundheitsdatenhosts, für den die Zertifizierung ausgesetzt wurde;
- Kennnummer der ausgesetzten Bescheinigung;
- Datum der Aussetzung der Bescheinigung;
- Gründe für die Aussetzung der HDS-Zertifizierung.

Die Informationen sind auf elektronischem Wege unter Verwendung des Musters in Anhang B zu übermitteln: Informationsaustausch zwischen der Zertifizierungsstelle und der zuständigen Behörde.

14.2.3.5.2. HDS-Rücknahmebericht

Die Zertifizierungsstelle teilt der zuständigen Behörde in französischer oder englischer Sprache jede Entscheidung mit, die Zertifizierung eines Gesundheitsdatenhosts zurückzunehmen.

Die nachstehenden Informationen über den Gesundheitsdatenhost, dessen Zertifizierung zurückgenommen wurde, sind mitzuteilen:

- Bezeichnung oder Geschäftsbezeichnung des Gesundheitsdatenhosts, für den die Zertifizierung zurückgenommen wurde;
- Kennnummer der zurückgenommenen Bescheinigung;
- Datum der Rücknahme der Bescheinigung;
- Gründe für die Rücknahme der HDS-Zertifizierung.

Die Informationen sind elektronisch unter Verwendung des Musters in Anhang B zu übermitteln: Informationsaustausch zwischen der Zertifizierungsstelle und der zuständigen Behörde.

14.2.3.5.3. HDS-Kundenverzeichnis

Mindestens einmal im Monat übermittelt die Zertifizierungsstelle der zuständigen Behörde einen Bericht über gültige, ausgesetzte und zurückgenommene Zertifizierungen. Dieser Bericht muss auf Französisch oder Englisch die folgenden Daten für jeden Gesundheitsdatenhost enthalten:

- Bezeichnung oder Geschäftsbezeichnung des Gesundheitsdatenhosts;
- Kennnummer der Bescheinigung;
- Umfang der Zertifizierung (Liste der Tätigkeiten);
- Anschrift des zertifizierten Standorts und im Falle einer Mehrstandortzertifizierung die Anschrift des Hauptsitzes sowie die Anschrift aller angeschlossenen Standorte;
- Status der Zertifizierung (gültig, ausgesetzt oder zurückgenommen);
- Datum der Zertifizierung.
- URL oder Kontakt, um die Überprüfung der Bescheinigung mit der OC zu ermöglichen.
- URL der DSCP-Übertragungsdeklaration gemäß Anforderung 31 des Zertifizierungsrahmens

Das Verzeichnis ist unter Verwendung des Musters in Anhang B elektronisch zu übermitteln: Informationsaustausch zwischen der Zertifizierungsstelle und der zuständigen Behörde.

14.2.3.5.4. HDS-Jahresbericht

Es gelten die Anforderungen des § 8.5 der NF ISO 17021-1.

Jedes Jahr legt die Zertifizierungsstelle der zuständigen Behörde einen Jahresbericht in französischer oder englischer Sprache vor, einschließlich:

- eine anonymisierte Zusammenfassung der HDS-Zertifizierungen, durchgeführte Prüfungen und festgestellte Nichtkonformitäten.
- eine Zusammenfassung der Schwierigkeiten bei der Zertifizierung von Hosting-Anbietern und etwaige Vorschläge für Änderungen der Zertifizierungs- und Akkreditierungsnormen;
- Indikatoren für das HDS-Zertifizierungsverfahren, wie z. B.:
- Anzahl der Gesundheitsdatenhosts, die sich im Prozess der Zertifizierung befinden;
- Anzahl der Gesundheitsdatenhosts, die die Zertifizierung nicht bestanden haben;
- Anzahl der Zertifizierungserneuerungen;
- durchschnittliche Dauer der Prüfungen.

Der Jahresbericht ist zwischen dem 1. und dem 31. Januar des folgenden Jahres unter Verwendung des in Anhang B vorgeschlagenen Musters elektronisch zu übermitteln: Informationsaustausch zwischen der Zertifizierungsstelle und der zuständigen Behörde.

14.2.4. Die Anforderungen des Zertifizierungsprozesses

14.2.4.1. Vorzertifizierungstätigkeiten

14.2.4.1.1. Antrag auf Zertifizierung

Es gelten die Anforderungen des § 9.1.1 der NF ISO 17021-1.

Im Falle einer Übertragung von Bescheinigungen gilt der Leitfaden IAF MD 2. Darüber hinaus unterrichtet die empfangende Zertifizierungsstelle die zuständige Behörde über jede Übertragung von Bescheinigungen und gibt den Namen der ausstellenden Zertifizierungsstelle an.

14.2.4.1.2. Überprüfung des Antrags

Es gelten die Anforderungen des § 9.1.2 der NF ISO 17021-1.

14.2.4.1.3. Prüfprogramm

Es gelten die Anforderungen des § 9.1.3 der NF ISO 17021-1.

Kapitel 9.1.3.1 wird durch folgende Anforderung ergänzt: in der Beschreibung des Geltungsbereichs der Zertifizierung ist die Liste der in Kapitel 11. aufgeführten Tätigkeiten anzugeben, für die der Antragsteller eine Zertifizierung beantragt, um die Art der HDS-Zertifizierung zu bestimmen.

14.2.4.1.4. Ermittlung der Prüfzeit

Es gelten die Anforderungen des § 9.1.4 der NF ISO 17021-1. Darüber hinaus gelten die Anforderungen der Leitfäden IAF MD 4 und MD 5.

Die Prüfdauer wird anhand der Methode und der Tabellen in „Anhang A: Prüfdauertabelle für die HDS-Zertifizierung“ dieses Dokuments bestimmt.

Wenn das Ergebnis nach der Berechnung nicht eine ganze Zahl ist, muss die Anzahl der Tage auf den nächsten halben Tag gerundet werden (z. B.: 5,3 Prüfungstage werden 5,5 Prüfungstage und 5,2 Prüfungstage werden zu 5 Prüftagen).

14.2.4.1.5. Mehrfachprobenahme

Es gelten die Anforderungen des § 9.1.5 der NF ISO 17021-1. Darüber hinaus gilt der IAF MD 1-Leitfaden.

14.2.4.1.6. Standards für mehrere Managementsysteme

Es gelten die Anforderungen des § 9.1.6 der NF ISO 17021-1 sowie der IAF MD 11-Leitfaden.

14.2.4.2. Prüfungsplanung

Es gelten die Anforderungen des § 9.2 der NF ISO 17021-1.

14.2.4.3. Erstzertifizierung

Es gelten die Anforderungen des § 9.3 der NF ISO 17021-1.

14.2.4.4. Durchführung von Prüfungen

Es gelten die Anforderungen des § 9.4 der NF ISO 17021-1.

Vertreter der Agentur für digitale Gesundheit können als Beobachter an einer Prüfung teilnehmen.

14.2.4.5. Zertifizierungsentscheidung

Es gelten die Anforderungen des § 9.5 der NF ISO 17021-1.

14.2.4.6. Beibehaltung der Zertifizierung

Es gelten die Anforderungen des § 9.6 der NF ISO 17021-1.

Die Zertifizierung wird für einen Zeitraum von 3 Jahren ausgestellt. Zertifizierte Hosts müssen spätestens 3 Monate vor Ablauf der Zertifizierung einen Antrag auf Rezertifizierung bei der Zertifizierungsstelle einreichen.

14.2.4.7. Rechtsbehelf

Es gelten die Anforderungen des § 9.7 der NF ISO 17021-1.

14.2.4.8. Beschwerden

Es gelten die Anforderungen des § 9.8 der NF ISO 17021-1.

14.2.4.9. Kundendatensätze

Es gelten die Anforderungen des § 9.9 der NF ISO 17021-1.

14.2.4.10. Anforderungen an das Managementsystem für Zertifizierungsstellen

14.2.4.10.1. Optionen

Es gelten die Anforderungen des § 10.1 der NF ISO 17021-1.

14.2.4.10.2. Anforderungen an das Managementsystem gemäß ISO 9001

Es gelten die Anforderungen des § 10.2 der NF ISO 17021-1.

14.2.4.10.3. Allgemeine Anforderungen an das Managementsystem

Es gelten die Anforderungen des § 10.3 der NF ISO 17021-1.

14.2.5. Bewertungsverfahren

Anhang B der Norm NF ISO 17021-1 findet Anwendung.

15. ZUSTÄNDIGKEITEN DER AKKREDITIERUNGSSTELLEN

Die Akkreditierungsstellen (COFRAC in Frankreich und ihre europäischen Partner) haben die Aufgabe sicherzustellen, dass die von ihnen akkreditierten Stellen kompetent und unparteiisch sind und dass sie dies im Laufe der Zeit unabhängig vom Kontext beibehalten.

Um diese Kompetenz zu bescheinigen, nimmt die Akkreditierungsstelle regelmäßige Bewertungen der Arbeitsweise dieser akkreditierten Stellen vor. Die Bewertungen bestehen aus einer Dokumentenprüfung sowie einer Intervention der Gutachter als Zeugen einer Prüfung, um sowohl die Qualität der Verfahren als auch die Art und Weise ihrer Anwendung zu überprüfen.

15.1. Akkreditierungsverfahren

Das Akkreditierungsverfahren muss NF ISO 17021-1 entsprechen.

Wenn die Zertifizierungsstelle bereits für die Norm NF ISO 17021-1 akkreditiert ist, wird eine wesentliche Erweiterung des Akkreditierungsumfangs auf eine neue Domäne vorgenommen. Dies führt zu einer Beurteilung am Sitz des Körpers und mindestens zu einer Aktivitätsbeobachtung.

Wenn die Zertifizierungsstelle noch nicht für NF ISO 17021-1 akkreditiert ist, ist das erste Akkreditierungsverfahren anzuwenden.

Nach positiver Zulässigkeit des Antrags auf Akkreditierung durch die nationale Akkreditierungsstelle für die HDS-Zertifizierung (operative Zulässigkeit) sind Zertifizierungsstellen, die bei der Antragstellung eine Akkreditierung beantragen, für zwölf (12) Monate berechtigt, Bescheinigungen auszustellen.

Die Akkreditierung muss innerhalb von höchstens zwölf (12) Monaten nach Bekanntgabe der positiven Entscheidung über die Betriebszulässigkeit erfolgen.

Wird innerhalb dieser Frist keine Akkreditierung erteilt, so unterrichtet die Zertifizierungsstelle ihre Kunden, um sich an eine andere Zertifizierungsstelle zu wenden, um eine neue Bescheinigung zu erhalten.

Bescheinigungen, die während der zwölf (12) Monate ausgestellt wurden, müssen im Rahmen der Akkreditierung neu ausgestellt werden, wenn sie ursprünglich unter den gleichen Bedingungen wie für die Erteilung der Akkreditierung ausgestellt wurden.

Der Umfang der Akkreditierung wird wie folgt ausgedrückt:

Gegenstand der Zertifizierung	Zertifizierungsreferenz	Akkreditierungsrahmen
Sicherheitsmanagementsysteme für Gesundheitsdatenhosts	Rahmen für HDS-Zertifizierungsanforderungen (aktuelle	HDS-Akkreditierungsrahmen (aktuelle Version)

	Version)	

15.2. Verfahren zur Aussetzung der Akkreditierung

15.2.1. Aussetzungsbeschluss

Im Falle einer Aussetzung der Akkreditierung auf Initiative der Akkreditierungsstelle unterrichtet diese unverzüglich die Zertifizierungsstelle und die zuständige Behörde und legt Folgendes fest: Name der Zertifizierungsstelle, Datum der Aussetzung, Gründe für die Aussetzungsentscheidung und Datum des Widerrufs der Akkreditierung, wenn die Voraussetzungen für die Aufhebung der Aussetzung nicht erfüllt sind.

Die Aussetzungsentscheidung wird per Einschreiben mit Rückschein mitgeteilt und legt den Umfang der Aussetzung der Akkreditierung, die Gründe für die Entscheidung über die Aussetzung der Akkreditierungsstelle und die Bedingungen fest, unter denen die Stelle die Aussetzung der Zertifizierungsstelle aufheben kann.

Übermittelt die Zertifizierungsstelle die von der Akkreditierungsstelle angeforderten Antworten nicht innerhalb der in der Aussetzungsentscheidung festgelegten Fristen, so wird die Akkreditierung für Zertifizierungstätigkeiten des Hosts personenbezogener Gesundheitsdaten zurückgezogen.

Sobald sie die Entscheidung erhält, ihre Akkreditierung auszusetzen, muss die Zertifizierungsstelle ihre Kunden darüber informieren und darf nicht mehr auf die Akkreditierung verweisen. Eine Stelle, deren Akkreditierung ausgesetzt wurde, darf keine Zertifizierungsprüfung mehr durchführen oder Entscheidungen über die Bescheinigung des Gesundheitsdatenhosts erlassen.

15.2.2. Aufhebung der Aussetzung

Im Falle einer Aussetzung auf Initiative der Akkreditierungsstelle werden die Bedingungen für die Aufhebung der Aussetzung in der der Zertifizierungsstelle übermittelten Aussetzungsentscheidung festgelegt.

Die Entscheidung über die Aufhebung der Aussetzung kann nur nach einer Vor-Ort-Bewertung durch die Zertifizierungsstelle oder nach Prüfung eines von der Zertifizierungsstelle übermittelten internen Prüfungsberichts durch die Akkreditierungsstelle erlassen werden. Enthält der Bericht keine ausreichenden Nachweise, um die Einhaltung der Akkreditierungsanforderungen nachzuweisen, wird die Zertifizierungsstelle per Schreiben darüber unterrichtet, dass ihre Aussetzung nur auf der Grundlage der Ergebnisse einer Vor-Ort-Bewertung aufgehoben werden kann. Die Entscheidung über die Aufhebung der Aussetzung wird von der Akkreditierungsstelle notifiziert. Es wird eine neue Akkreditierungsbescheinigung erstellt, aus der der Zeitpunkt der Aufhebung der Aussetzung hervorgeht, und der technische Anhang mit den Tätigkeiten, für die die Akkreditierung erteilt wurde, wird aktualisiert. Das Ablaufdatum der Akkreditierung ist gegenüber der ursprünglichen Akkreditierung unverändert.

Die Mitteilung über die Aufhebung der Aussetzung wird der zuständigen Behörde elektronisch übermittelt und muss folgende Angaben enthalten: Name der Zertifizierungsstelle, das Datum der Aussetzung (falls zutreffend), die Gründe für die Aussetzungsentscheidung und das Datum, an dem die Aussetzung aufgehoben wurde.

Im Falle der Weigerung, die Aussetzung aufzuheben, kann die Zertifizierungsstelle gegen die Entscheidung bei der Akkreditierungsstelle Berufung einlegen.

15.3. Akkreditierungsrücknahmeverfahren

Im Falle der Rücknahme der Akkreditierung unterrichtet die Akkreditierungsstelle die Zertifizierungsstelle und die zuständige Behörde unverzüglich über alle Maßnahmen zur Rücknahme der Akkreditierung.

Die Mitteilung über die Rücknahme wird der zuständigen Behörde auf elektronischem Wege übermittelt und muss folgende Angaben enthalten: den Namen der Zertifizierungsstelle, das Datum der Rücknahme (falls zutreffend), die Gründe für die Rücknahme der Akkreditierung und das Datum, an dem die Akkreditierung zurückgenommen wurde.

Die Rücknahme der Akkreditierung tritt am Tag der Mitteilung über die Rücknahme durch die Akkreditierungsstelle in Kraft. Die Entscheidung wird der Zertifizierungsstelle durch Einschreiben mit Rückschein unter Angabe der Gründe für die Entscheidung mitgeteilt.

Die Organisation ist nicht mehr berechtigt, Bescheinigungen auszustellen oder bestehende Bescheinigungen zu pflegen.

Die Zertifizierungsstelle, deren Akkreditierung zurückgenommen wurde, muss alle Tätigkeiten im Zusammenhang mit der Zertifizierung des Gesundheitsdatenhosts einstellen und unverzüglich die zuständige Behörde und ihre Kunden informieren, damit sie sich an eine zu diesem Zweck akkreditierte Zertifizierungsstelle wenden können, um gegebenenfalls die Zertifizierung zu übertragen.

Die Akkreditierungsstelle hat die Möglichkeit, am Standort der Zertifizierungsstelle einzugreifen, um sicherzustellen, dass die Tätigkeiten im Zusammenhang mit der Zertifizierung von Gesundheitsdatenhosts ausgesetzt und die zuständige Behörde und die Kunden darüber unterrichtet wurden.

15.4. Übertragung der Zertifizierung an eine neue Zertifizierungsstelle nach Rücknahme

Die neue Zertifizierungsstelle, die einen Übertragungsantrag erhält, muss die in § 16. dieses Dokuments beschriebenen Bestimmungen anwenden. Insbesondere gilt der Leitfaden für die IAF MD2. Wenn es unmöglich ist, die Akte des Kunden von der vorherigen Stelle zu erhalten, wird der Antrag des Kunden als Erstzertifizierung behandelt. In jedem Fall obliegt es der „empfangenden“ Zertifizierungsstelle, die bereitgestellten Elemente zu bewerten und festzustellen, ob der Zertifizierungszyklus in der gleichen Zertifizierungsphase wie bei der ursprünglichen Zertifizierungsstelle wiederaufgenommen werden kann.

15.5. Einstellung der Tätigkeit einer Zertifizierungsstelle

Die Akkreditierungsstelle unterrichtet die zuständige Behörde unverzüglich über jede Ankündigung der Einstellung der Tätigkeit einer Zertifizierungsstelle.

Die Zertifizierungsstelle ist ferner verpflichtet, die zuständige Behörde sowie die betreffenden Kunden so bald wie möglich darüber zu unterrichten, damit sie sich bei einer anderen zu diesem Zweck akkreditierten Zertifizierungsstelle bewerben können, um die erteilte Zertifizierung gegebenenfalls zu übertragen.

16. BEDINGUNGEN, KRITERIEN UND VERFAHREN FÜR DIE ZERTIFIZIERUNG

16.1. Zertifizierungsbedingungen und -kriterien

Ein Antragsteller, der eine HDS-Zertifizierung beantragt, muss die Anforderungen des HDS-Zertifizierungsrahmens erfüllen und eine Zertifizierung bei einer akkreditierten Zertifizierungsstelle gemäß dem HDS-Akkreditierungsrahmen beantragen.

Die Zertifizierung eines Hosts erfordert:

- die vorherige Implementierung eines gemäß der Norm ISO 27001 zertifizierten Informationssicherheitsmanagementsystems (ISMS), das durch die Anforderungen in Kapitel 5 des Zertifizierungsrahmens ergänzt wird;
- dass der Anwendungsbereich dieses ISMS alle Hosting-Aktivitäten für Gesundheitsdaten des Hosts abdeckt;
- dass die mit seinen Kunden geschlossenen Verträge die in Kapitel 6 des Zertifizierungsrahmens festgelegten Anforderungen erfüllen;
- dass er die in Kapitel 7 des Zertifizierungsrahmens festgelegten Souveränitätsanforderungen erfüllt;
- dass er seinen Kunden die Vorlage der gemäß Kapitel 8 des Zertifizierungsrahmens formalisierten Garantien mitteilt.

Ein Host, der bereits eine ISO 27001-Zertifizierung erhalten hat, kann diese Zertifizierung in Anspruch nehmen, wenn er die Bedingungen des Kapitels 16.2. erfüllt.

Ein Antragsteller, der bereits über diese Zertifizierung verfügt, wird im Rahmen der Anforderungen des Zertifizierungsrahmens bewertet, der nicht von der Zertifizierung abgedeckt ist. Die bereits erhaltene Bescheinigung wird nach den Verfahren des Kapitels 16.2. überprüft.

Die HDS-Bescheinigung wird für 3 Jahre ausgestellt: das Ablaufdatum kann vom Ablaufdatum der ISO 27001-Bescheinigung abweichen.

Die HDS-Bescheinigung muss ausdrücklich angeben, dass sie vorbehaltlich einer gültigen ISO 27001-Zertifizierung für denselben Umfang gültig ist.

Im Vertrag zwischen der OC und ihren Kunden müssen folgende Angaben enthalten sein:

- Der Kunde wird darüber informiert, dass bei Nichteinhaltung einer im Rahmen einer HDS-Prüfung festgestellten Anforderung von ISO 27001 diese Informationen an die OC übermittelt werden, die den Kunden nach ISO 27001 zertifiziert hat.
- Der Kunde ist verpflichtet, der OC unverzüglich alle Maßnahmen zur Aussetzung, Rücknahme, Beendigung oder Übertragung seiner ISO 27001-Bescheinigung mitzuteilen.

Diese Verpflichtungen werden im Rahmen von Überwachungsprüfungen überprüft.

16.2. Gleichwertigkeit

Wenn der Antragsteller die Zertifizierung nach der Norm NF ISO 27001, die er bereits erhalten hat, verwenden möchte, muss diese Zertifizierung alle folgenden Bedingungen erfüllen:

- der Anwendungsbereich der Zertifizierung, die dem Host zur Verfügung steht, muss den Anwendungsbereich umfassen, für den der Antragsteller eine HDS-Zertifizierung beantragt;
- Prüfberichte: der erste Prüfbericht und die Prüfberichte zur Zertifizierungsüberwachung, für die die Gleichwertigkeit beantragt wird, müssen auf Antrag der Zertifizierungsstelle vorgelegt werden;
- für einen Antragsteller mit einer ISO 27001-Zertifizierung muss die Anwendbarkeitserklärung (DdA) des Informationssicherheitsmanagementsystems der Organisation ausdrücklich Folgendes enthalten:
- die detaillierte Begründung für einen Ausschluss von ISO 27001-Kontrollen;
- die detaillierte Begründung für nicht anwendbare Kontrollen;
- die Zertifizierung muss:
- gültig sein;
- von einer Zertifizierungsstelle ausgestellt worden sein, die von einer nationalen Akkreditierungsstelle im Sinne der Verordnung (EG) Nr. 765/2008 für die Ausstellung solcher Bescheinigungen akkreditiert ist und deren Akkreditierung gültig sein muss (COFRAC in Frankreich oder gleichwertig in anderen Ländern, die multilaterale internationale Anerkennungsabkommen unterzeichnet haben);
- nicht Gegenstand eines Aussetzungs- oder Rücknahmeverfahrens sein;
- nicht Gegenstand eines Übertragungsantrags sein.

Die oben genannten Bedingungen müssen von der Zertifizierungsstelle, die den HDS-Zertifizierungsantrag erhält, überprüft werden, die die erhaltenen Informationen (einschließlich Kopien von Bescheinigungen) aufzeichnet und die Ergebnisse dieser Überprüfung durch Angabe begründen muss, indem sie angibt, welche Zertifizierung(en) von der OC vor der ersten Prüfung des Antragstellers akzeptiert wird/werden.

Zertifizierungen, die nach internationalen Normen erworben wurden, die den oben genannten französischen Normen gleichwertig sind, können unter denselben Bedingungen anerkannt werden. Dazu gehören Zertifizierungen zur Einhaltung der Normen ISO 27001 und ISO 17021 in anderen Sprachen als Französisch.

16.3. Vergabe von Unteraufträgen

Im Falle der Verwendung von Auftragsverarbeitern durch den Host gilt die Darstellung der in Kapitel 8 des HD-Zertifizierungsrahmens beschriebenen Garantien.

ANHANG A Prüfdauertabelle für die HDS-Zertifizierung

Die nachstehende Prüfdauertabelle bietet den Rahmen, der für die Planung des HDS-Zertifizierungsprüfungen verwendet werden sollte, indem ein Ausgangspunkt ermittelt wird, der auf der Gesamtzahl der Personen basiert, die unter der Kontrolle der Organisation für alle Positionen am Hosting-Dienst für Gesundheitsdaten arbeiten und die wichtigen Faktoren anpassen.

Die OC hat dem Kunden die Festlegung der Prüfzeit und der Belege zur Verfügung zu stellen. Diese sind Bestandteil des Vertrags und müssen der Akkreditierungsstelle auf Anfrage zur Verfügung gestellt werden.

Der Ausgangspunkt für die Bestimmung der Prüfzeit einer HDS-Zertifizierung muss auf der tatsächlichen Anzahl des am Hosting-Dienst für Gesundheitsdaten beteiligten Personals basieren und kann dann um signifikante Faktoren angepasst werden, die für den zu prüfenden Kunden zutreffen.

Anzahl der Personen, die am Hosting-Dienst für Gesundheitsdaten beteiligt sind	Dauer der HDS-Zertifizierungsprüfung (Schritt 1 + Schritt 2) A+B		
	(A) Prüfdauer NF ISO 27001	(B) Dauer der Prüfung von Anforderungen außerhalb von NF ISO 27001	Gesamtdauer der HDS-Zertifizierungsprüfung
0			0,5[3]
1 – 10	5	2	7
11 - 15	6	2	8
16 - 25	7	2	9
26 - 45	8,5	2	10,5
46 - 65	10	3	13
66 - 85	11	3	14
86 - 125	12	3	15
126 - 175	13	3	16
176 - 275	14	3	17
276 - 425	15	3	18
426 - 625	16,5	4	20,5
626 - 875	17,5	4	21.5
876 - 1175	18,5	4	22,5
1176 - 1550	19,5	4	23,5

[3] Auf dieser Linie darf kein Reduktionsfaktor angewendet werden.

Anzahl der Personen, die am Hosting-Dienst für Gesundheitsdaten beteiligt sind	Dauer der HDS-Zertifizierungsprüfung (Schritt 1 + Schritt 2) A+B		
	(A) Prüfdauer NF ISO 27001	(B) Dauer der Prüfung von Anforderungen außerhalb von NF ISO 27001	Gesamtdauer der HDS-Zertifizierungsprüfung
1551 – 2025	21	4	25
2026 – 2675	22	4	26
2676 – 3450	23	4	27
3451 – 4350	24	5	29
4351 – 5450	25	5	30
5451 – 6800	26	5	31
6801 – 8500	27	5	32
8501 - 10700	28	5	33
10700	Folgen Sie dem oben genannten Fortschritt	Folgen Sie dem oben genannten Fortschritt	Folgen Sie dem oben genannten Fortschritt

Die HDS-Prüfdauer kann je nach den derzeitigen bewährten Verfahren zur Berechnung der ISMS-Prüfdauer nach oben oder unten angepasst werden. Zu diesen Faktoren gehören die Komplexität des ISMS, die Art des betreffenden Dienstes, der Nachweis der vorherigen Implementierung eines ISMS, die implementierte technologische Komplexität, die Verwendung von Auftragsverarbeitern, die Art der Entwicklungen und die Anzahl der Standorte. Änderungen am ISMS sind ein Faktor, der bei der Berechnung der Dauer der Überwachungs- und Rezertifizierungsprüfung zu berücksichtigen ist.

Nach den geltenden Regeln der bewährten Praktiken für die Berechnung der ISMS-Prüfdauer beträgt die maximale Verkürzung der Prüfdauer 30 % und die maximale Erhöhung der Prüfdauer 100 %. Diese Grenzen gelten für die Berechnung der HDS-Prüfdauer.

Anhang B: Informationsaustausch zwischen der Zertifizierungsstelle und der zuständigen Behörde

HDS-Jahresbericht

Name der Zertifizierungsstelle	Datum (*TT/MM/JJJJ*)

Zusammenfassung der HDS-Zertifizierungen, der durchgeführten Prüfungen und der festgestellten Nichtkonformitäten

Zusammenfassung der Schwierigkeiten, die bei der HDS-Zertifizierung aufgetreten sind

Vorschläge zur Verbesserung der HDS-Zertifizierung

Indikatoren für das HDS-Zertifizierungsverfahren

Anzahl der ausgestellten	Anzahl der Ausfälle	Anzahl der	Anzahl der	Anzahl der	Anzahl der

Zertifizierungen		Erneuerungen	Aussetzungen	Rücknahmen	übertragenen Zertifizierungen
XXXX	*XXXX*	*XXXX*	*XXXX*	*XXXX*	*XXXX*

HDS-Kundenverzeichnis

Name der Zertifizierungsstelle: *XXXX*	Datum (*TT/MM/JJJJ*)

Bescheinigungs-Identifikator	Name des Gesundheitsdatenhosts	Umfang der Zertifizierung (Liste der Tätigkeiten)	URL der DSCP-Übertragungsrisikodeklaration gemäß Anforderung Nr. 31	Adresse der Standorte	Datum der Zertifizierung	Bescheinigungstatus	URL der Bescheinigungspublikation oder Kontakt zur OC

esante.gouv.fr

Das Portal, um auf alle von der digitalen Gesundheitsagentur angebotenen Dienstleistungen und Produkte zuzugreifen und über Informationen über elektronische Gesundheitsdienste auf dem Laufenden zu bleiben.

esante.gouv.fr