Handbuch für die Aufbewahrung Handelskammer Bozen

AUSSTELLUNG DES DOKUMENTS

Maßnahme	Datum	Name	Funktion
Abfassung	16.10.2019	Luca Filippi	
Überprüfung		Luca Filippi	
Genehmigung	10.12.2019	Luca Filippi	Verantwortlicher für die Aufbewahrung der Handelskammer Bozen

REGISTER DER FASSUNGEN

Version/Überarbeitung/Entwurf	Ausstellungsdatum	Vorgenommene Änderungen	Anmerkungen

Inhaltsverzeichnis

1 Zweck und Anwendungsbereich des Dokuments

Dieses Handbuch beschreibt das Aufbewahrungssystem im Sinne des Art. 44 des Gesetzbuches für die digitale Verwaltung und Art. 8 der Technischen Bestimmungen.

Im Spezifischen werden in diesem Dokument definiert:

- die Rollen und Verantwortungen im Aufbewahrungsprozess;
- die Aktivierung des Dienstes;
- Dokumente, die der Aufbewahrung unterzogen werden;
- der Aufbewahrungsprozess;
- die Sicherheits- und Schutzmaßnahmen in Bezug auf die personenbezogenen Daten.

Der Teil des Aufbewahrungsprozesses, der einem externen Rechtsträger anvertraut wird, ist im Handbuch für die Aufbewahrung des verwahrenden Rechtsträgers genauer beschrieben.

Zurück zum Inhaltsverzeichnis

2 Begriffsbestimmungen (Glossar und Abkürzungen)

Glossar und Abkürzungen	
AgID	Agenzia per l'Italia Digitale
AIP	Archival Information Package. Definition der OAIS-Normung und sinnverwandt mit Archivierungspaket
AgID-Rundschreiben	Rundschreiben der AgID vom 10. April 2014, Nr. 65 - Modalitäten für die Akkreditierung und Überwachung der öffentlichen und privaten Rechtsträger, die Tätigkeiten der Aufbewahrung von digitalen Dokumenten gemäß Artikel 34 des gesetzesvertretenden Dekrets vom 7. März 2005, Nr. 82 durchführen.
Datenschutzkodex	Gesetzesvertretendes Dekret vom 30. Juni 2003, Nr. 196 i.g.F. - Datenschutzkodex
EU-Verordnung 2016/679	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
Dublin Core	ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Metadatensystem des Dublin Core.
OAIS	Das Open Archival Information System ist der Standard 14721:2003 und definiert Konzepte, Modelle und Funktionen der digitalen Archive und die Aspekte der digitalen Aufbewahrung.
Sicherheitsplan	Dokument, das im Rahmen des allgemeinen Sicherheitsplanes die Tätigkeiten für den Schutz des Aufbewahrungssystems für digitale Dokumente vor möglichen Risiken im Bereich der Organisation beschreibt und plant
Produzierende Körperschaft oder Erzeuger	Natürliche oder juristische Person (in der Regel nicht der Verfasser des Dokuments), welche das Übergabepaket erzeugt und für die Übertragung seines Inhalts in das Aufbewahrungssystem verantwortlich ist. In den öffentlichen Verwaltungen entspricht diese Person dem Verantwortlichen für die Dokumentenverwaltung.
Technische Bestimmungen	Dekret des Präsidenten des Ministerrates vom 3. Dezember 2013 über Aufbewahrungssysteme im Sinne der Artikel 20, Absätze 3 und 5-bis, 23-ter, Absatz 4, 43, Absätze 1 und 3, 44, 34 und 71, Absatz 1 des Kodex der digitalen Verwaltung gemäß gesetzesvertretendem Dekret Nr. 82/2005
Bestimmungen des CNIPA 2004	Beschluss des CNIPA Nr. 11/2004 - Technische Bestimmungen für die Kopie und Aufbewahrung von Dokumenten auf Datenträger, der geeignet ist, um die Konformität mit dem Original zu gewährleisten, vom 19. Februar 2004.

	Der Beschluss des CNIPA Nr. 11/2004 ist ab der Frist gemäß Art. 14, Absätze 2 und 3 der Technischen Bestimmungen nicht mehr wirksam.
Verantwortlicher für die Aufbewahrung	Verantwortlicher für die Tätigkeiten, die in Artikel 8, Absatz 1 der Technischen Bestimmungen des Aufbewahrungssystems angegeben sind
CNIPA-System 2004	Aufbewahrungssystem, das die technischen Bestimmungen gemäß Beschluss CNIPA Nr. 11/2004 vom 19. Februar 2004 berücksichtigt
AgID-System 2013	Aufbewahrungssystem, das die technischen Bestimmungen gemäß Dekret des Präsidenten des Ministerrates vom 3.12.2013 und die von AgID für akkreditierte Verwahrer vorgesehenen Qualitäts- und Sicherheitsvoraussetzungen erfüllt
Dokumentendienste	Applikationen für die Verwaltung von digitalen Dokumenten
UniSincro	UNI 11386:2010 - Support für die Interoperabilität in der Aufbewahrung und Abfrage der digitalen Dokumente
Benutzer	Person, Körperschaft oder System, die bzw. das mit den Diensten eines digitalen Systems zur Verwaltung der Dokumente und/oder einem System für die Aufbewahrung der digitalen Dokumente interagiert, um die gesuchten Informationen zu nutzen

Zurück zum Inhaltsverzeichnis

3 Bezugsnormen und -standards

3.1 Bezugsnormen

Nachfolgend die zum Stichtag bestehende Liste der wichtigsten einschlägigen italienischen Normen, hier hierarchisch geordnet:

- Zivilgesetzbuch [5. Buch, 2. Titel, Arbeit im Unternehmen, 3. Abschnitt Handelsunternehmen und andere registrierungspflichtige Unternehmen, 3. Teil Sonderbestimmungen für Handelsunternehmen, § 2 Rechnungsunterlagen], Artikel 2215 bis - Führung von Unterlagen mittels elektronischer Datenverarbeitung;
- Gesetz 24. Dezember 2007, Nr. 244 - Bestimmungen für die Erstellung des ein- und mehrjährigen Staatshaushaltes;
- Gesetz 7. August 1990, Nr. 241 i.g.F. - Neue Bestimmungen über Verwaltungsverfahren und Zugang zu Verwaltungsunterlagen
- Gesetzesvertretendes Dekret vom 7. März 2005 Nr. 82 i.g.F. – Kodex der digitalen Verwaltung (CAD);
- Gesetzesvertretendes Dekret vom 22. Jänner 2004, Nr. 42 i.g.F. - Kodex der Kultur- und Landschaftsgüter;
- Gesetzesvertretendes Dekret vom 30. Juni 2003, Nr. 196 i.g.F. - Datenschutzkodex;
- Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;
- Dekret des Präsidenten der Republik vom 28. Dezember 2000, Nr. 445 i.g.F. - Vereinheitlichter Text der Gesetze und Verordnungen im Bereich der Verwaltungsunterlagen;
- Dekret des Präsidenten des Ministerrates vom 13. November 2014 - Technische Bestimmungen für die Erstellung, Übermittlung, Kopie, Duplikation, Reproduktion und zeitliche Validierung der digitalen Dokumente sowie Erstellung und Aufbewahrung der digitalen Dokumente der öffentlichen Verwaltung;
- Dekret des Präsidenten des Ministerrates vom 3. Dezember 2013 - Technische Bestimmungen für Aufbewahrungssysteme im Sinne der Artikel 20, Absätze 3 und 5-bis, 23-ter, Absatz 4, 43, Absätze 1 und 3, 44, 44bis und 71, Absatz 1 des Kodex der digitalen Verwaltung gemäß gesetzesvertretendem Dekret Nr. 82/2005;
- Dekret des Präsidenten des Ministerrates vom 3. Dezember 2013 - Technische Bestimmungen für das digitale Protokoll im Sinne der Artikel 40-bis, 41, 47, 57-bis und 71 des Kodex der digitalen Verwaltung gemäß gesetzesvertretendem Dekret Nr. 82/2005;
- Dekret des Präsidenten des Ministerrates vom 22. Februar 2013 - Technische Bestimmungen für die Generierung, Anbringung und Überprüfung der fortgeschrittenen, qualifizierten und digitalen elektronischen Unterschriften im Sinne der Artikel 20, Absatz 3, 24, Absatz 4, 28, Absatz 3, 32, Absatz 3 Buchstabe b), 35, Absatz 2, 36, Absatz 2, und 71;
- Dekret des Wirtschafts- und Finanzministeriums vom 17. Juni 2014 - Modalitäten für die Abwicklung der steuerrechtlichen Pflichten in Bezug auf digitale Dokumente und deren Reproduktion auf verschiedene Träger - Artikel 21, Absatz 5 des gesetzesvertretenden Dekrets

Nr. 82/2005;

- Dekret des Wirtschafts- und Finanzministeriums 3. April 2013, Nr. 55 - Verordnung für die Ausstellung, die Übermittlung und den Erhalt der elektronischen Rechnung, anzuwenden von den öffentlichen Verwaltungen im Sinne des Artikels 1, Absätze 209 - 213 des Gesetzes vom 24. November 2007, Nr. 244;
- Rundschreiben der AgID vom 10. April 2014, Nr. 65 - Modalitäten für die Akkreditierung und Überwachung der öffentlichen und privaten Rechtsträger, die Tätigkeiten der Aufbewahrung von digitalen Dokumenten gemäß Artikel 34 des gesetzesvertretenden Dekrets vom 7. März 2005, Nr. 82 durchführen;
- Beschluss des CNIPA vom 21. Mai 2009, Nr. 45 - Bestimmungen für die Anerkennung und die Prüfung des digitalen Dokuments.

Zurück zum Inhaltsverzeichnis

3.2 Bezugsstandards

- ISO 14721:2012 OAIS (Open Archival Information System), Offenes System für die digitale Archivierung;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Voraussetzungen eines ISMS (Information Security Management System);
- ISO 9001:2008 Management- und Qualitätssysteme - Voraussetzungen
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Voraussetzungen für die Errichtung und Verwaltung von sicheren und zuverlässigen Systemen für die elektronische Aufbewahrung der Informationen;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Leitfaden für die Prüfung sicherer und zuverlässiger Systeme für die elektronische Aufbewahrung der Informationen;
- UNI 11386:2010 Standard SInCRO - Support für die Interoperabilität in der Aufbewahrung und Einholung der digitalen Dokumente;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Metadatensystem des Dublin Core.
- ISO/TS 23081-1:2006 Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Bezugsrahmen für die Entwicklung eines Metadatensystems für die Verwaltung von Dokumenten.
- ISO 23081-2:2009 - Managing metadata for records – Part 2: Conceptual and implementation

issues, Praktischer Leitfaden für die Implementierung.

- 23081-3:2011 Information and documentation -- Managing metadata for records -- Part 3: Self-assessment method, Leitfaden für einen Selbstbewertungsprozess in Bezug auf Metadaten.
- ISAD(G) - International Standard Archival description - vom Komitee übernommener Standard zur Verzeichnung archivischer Unterlagen
- EAD - Encoded Archival Description, XML-Kodierung des Standards ISAD(G)
- ISAAR - International Standard Archival Authority Records - internationaler Standard für Archivierungsnormdateien für Körperschaften, Personen und Familien
- EAC - Encoded Archival Context, XML-Kodierung des ISAAR-Standards

Zurück zum Inhaltsverzeichnis

4 Rollen und Verantwortungen

Erzeuger / Verantwortlicher für die Aufbewahrung

Die Technischen Bestimmungen (Glossar, Anlage 1) definieren den Erzeuger als den Dateninhaber, der das Übergabepaket erzeugt und für die Übermittlung seines Inhaltes in das Aufbewahrungssystem verantwortlich ist.

Die produzierende Körperschaft vertraut dem Verantwortlichen für die Aufbewahrung die Aufbewahrung ihrer digitalen Dokumente und Faszikel an. Im Sinne des Art. 7 der Technischen Bestimmungen hat der Verantwortliche für die Aufbewahrung folgende Aufgaben inne:
a) er definiert die Merkmale und die Voraussetzungen des Aufbewahrungssystems je nach Art der aufzubewahrenden Dokumente, über die er eine Liste führt, im Sinne der geltenden Normen;
b) er verwaltet den Aufbewahrungsprozess und garantiert über den gesamten Zeitraum dessen Konformität mit den geltenden Bestimmungen;
c) er generiert den Übergabebericht mit den vom Aufbewahrungshandbuch vorgesehenen Modalitäten;
d) er generiert und unterzeichnet das Ausgabepaket mit digitaler Unterschrift oder qualifizierter digitaler Unterschrift in den vom Aufbewahrungshandbuch vorgesehenen Fällen;
e) er wacht über den korrekten Betrieb des Aufbewahrungssystems;
f) er gewährleistet die periodische Prüfung, die spätestens alle 5 Jahre stattzufinden hat, des Erhalts und der Lesbarkeit der Archive;
g) er ergreift im Sinne der Gewährleistung der Aufbewahrung und des Zugangs zu den digitalen Dokumenten die erforderlichen Maßnahmen, um eine eventuelle Beschädigung der Speichersysteme und der Registrierungen zu erheben und bei Bedarf den korrekten Betrieb wieder herzustellen; er ergreift zudem die entsprechenden Maßnahmen in Bezug auf das Veralten der Formate;
h) er sorgt für die Reduplikation oder Kopie der digitalen Dokumente in Hinblick auf die technologische Entwicklung laut Angaben im Aufbewahrungshandbuch;
i) er ergreift die erforderlichen Maßnahmen für die physische und logische Sicherheit des Aufbewahrungssystems im Sinne des Art. 12 der Technischen Bestimmungen;
j) er gewährleistet die Anwesenheit einer Amtsperson, falls die Betätigung derselben gefordert wird, und liefert ihr den Beistand und die erforderlichen Ressourcen für die Ausführung ihrer Aufgaben;
k) er liefert den von den geltenden Bestimmungen vorgesehenen zuständigen Organen den Beistand und die erforderlichen Ressourcen für die Ausführung der Prüf- und Aufsichtstätigkeiten;
l) er besorgt für die staatlichen Gerichts- und Verwaltungsstellen die Übergabe der Dokumente, die im zentralen Staatsarchiv und in den Staatsarchiven aufbewahrt werden, laut den geltenden Bestimmungen;
m) er bereitet das Aufbewahrungshandbuch gemäß Art. 8 der Technischen Bestimmungen vor und sorgt für dessen regelmäßige Aktualisierung bei bedeutenden rechtlichen, organisatorischen, verfahrensbezogenen oder technologischen Änderungen, in Zusammenarbeit mit dem Verantwortlichen für die Dokumentenverwaltung bzw. mit dem Koordinator der Dokumentenverwaltung, sofern ernannt.

Der Verantwortliche für die Aufbewahrung wird mit formellem Rechtsakt unter den Führungskräften und Beamten mit spezifischer Kompetenz und Erfahrung ernannt (Art. 7, Absatz 3 der Technischen Bestimmungen) und kann dem Verantwortlichen für die Dokumentenverwaltung entsprechen (Art. 7, Absatz 4, Technische Bestimmungen).

Durch eine spezifische Vereinbarung zur Erteilung des Dienstes für die normgerechte Aufbewahrung der digitalen Dokumente (Art. 5, Absatz 3 der Technischen Bestimmungen) hat der Verantwortliche für die Aufbewahrung InfoCamere – einer Gesellschaft der Handelskammern, die bei AgID als Verwahrer akkreditiert ist – folgende Teile des Aufbewahrungsprozesses anvertraut:

i) die Verwaltung des Aufbewahrungsprozesses mit Techniken in Konformität mit den geltenden Bestimmungen und den Angaben von InfoCamere im Aufbewahrungshandbuch sowie mit den technischen Merkmalen;
ii) die Generierung des Übergabeberichtes gemäß den im Aufbewahrungshandbuch vorgesehenen Modalitäten;
iii) die Generierung und die Unterzeichnung des Ausgabepaketes mit digitaler Unterschrift oder qualifizierter digitaler Unterschrift in den vom Aufbewahrungshandbuch vorgesehenen Fällen;
iv) die Überwachung der korrekten Funktionalität des Aufbewahrungssystems;
v) die Gewährleistung der periodischen Überprüfung, die spätestens alle 5 Jahre stattzufinden hat, des Erhalts und der Lesbarkeit der Archive;
vi) die Anwendung der erforderlichen Maßnahmen, um eine eventuelle Beschädigung der Speichersysteme und der Registrierungen rechtzeitig zu erheben und bei Bedarf den korrekten Betrieb wieder herzustellen; die Anwendung analoger Maßnahmen in Bezug auf das Veralten der Formate;
vii) die Produktion von digitalen Duplikaten gemäß den im Aufbewahrungshandbuch enthaltenen Anleitungen;
viii) die Anwendung der erforderlichen Maßnahmen für die physische und logische Sicherheit des Aufbewahrungssystems;
ix) die Lieferung des Beistandes und der erforderlichen Ressourcen für die Ausführung der Prüf- und Aufsichtstätigkeiten an die von den geltenden Bestimmungen vorgesehenen zuständigen Organe.

Der Verantwortliche für die Aufbewahrung teilt das Aufbewahrungshandbuch mit dem Verwahrer und mit allen Subjekten, die am Aufbewahrungsprozess beteiligt sind und denen er rechtzeitig jede Änderung mitteilt.

Verwahrer / InfoCamere

InfoCamere ist kraft der abgeschlossenen Vereinbarung als externer Verwahrer im Sinne des Absatzes 8 des Art. 6 der Technischen Bestimmungen tätig und übernimmt die Rolle des Verantwortlichen für die Verarbeitung der Daten laut Datenschutzkodex.

Aufgrund der geltenden Bestimmungen sieht das Aufbewahrungssystem von InfoCamere die materielle Aufbewahrung der Daten und der Sicherheitskopien im Inland und den Zugriff auf die Daten in den Strukturen, die für die Abwicklung des Dienstes vorgesehen sind, oder am Sitz des Erzeugers vor.

Als akkreditierter Verwahrer:

- befolgt InfoCamere die von AgID vorgesehenen organisatorischen, Qualitäts- und Sicherheitsvoraussetzungen und bietet angemessene organisatorische und technologische Garantien für die Abwicklung der ihr anvertrauten Funktionen;
- übt InfoCamere ihre Aufgaben durch Einsatz von Personen aus, die aufgrund ihrer Kompetenz und Erfahrung die korrekte Ausführung der Arbeit gewährleisten;
- sieht InfoCamere die materielle Aufbewahrung der Daten und der Sicherheitskopien im Inland und den Zugriff auf die Daten in den Strukturen, die für die Abwicklung des Dienstes vorgesehen sind, oder am Sitz des Erzeugers vor.

Benutzer

Die Technischen Bestimmungen (Glossar, Anlage 1) bezeichnen den Benutzer als eine Person, eine Körperschaft oder ein System, die oder das mit den Diensten eines Systems zur Aufbewahrung digitaler Dokumente interagiert. Der Benutzer kann intern oder außerhalb der produzierenden Körperschaft tätig sein.

Der Benutzer ersucht das Aufbewahrungssystem um Zugang zu den digitalen Dokumenten, um die ihn interessierenden Informationen im Rahmen der gesetzlichen Bestimmungen einzuholen. Das Aufbewahrungssystem gestattet den ermächtigten Subjekten den direkten Zugang, auch von entfernten Positionen aus, zu den aufbewahrten digitalen Dokumenten und ermöglicht die Produktion eines Ausgabepaketes, das direkt von den ermächtigten Subjekten übernommen werden kann.

Gemäß OAIS kann die Gemeinschaft der Benutzer als Bezugsgemeinschaft definiert werden.

4.1 Rollen

In der nachfolgenden Tabelle werden die Namen der natürlichen und/oder juristischen Personen angeführt, welche die im Aufbewahrungssystem angegebenen Rollen bekleiden.

Rolle	Name	Zeitraum in der Rolle	etwaige Vollmachten
Verantwortlicher für die Aufbewahrung	Luca Filippi	ab 01.01.2019	
Stellvertreter	Ivo Morelato	ab 01.01.2019	
Verwahrer	InfoCamere	ab 01.10.2015	

Zurück zum Inhaltsverzeichnis

5 Aktivierung des Dienstes

5.1 Zuteilung des Dienstes

Der Verantwortliche für die Aufbewahrung hat InfoCamere, die von AgID als Verwahrer akkreditiert wurde, den Aufbewahrungsprozess mit Unterzeichnung der Vereinbarung für die Erteilung des normgerechten Aufbewahrungsdienstes für digitale Dokumente gemäß den entsprechenden technischen Merkmalen am 07.02.2017 mit Fälligkeit 31.12.2021 anvertraut.
InfoCamere verfügt über ein eigenes Aufbewahrungshandbuch, dessen Inhalt Art. 8 der Technischen Bestimmungen entspricht. Die aktuelle Fassung des Aufbewahrungshandbuches von InfoCamere als akkreditierter Verwahrer steht auf der Website der Agenzia per l'Italia digitale zur Verfügung.

5.2 Zugang zum Dienst

Die produzierende Körperschaft hat durch die Dokumentendienste von InfoCamere Zugang zum Aufbewahrungssystem. Diese Dienste:

- generieren die Übergabepakete;
- ergänzen die Applikation für die Vorlegung der aufbewahrten Inhalte, welche die Ausgabepakete generiert.

5.3 Beschreibung des Dienstes

Die Beschreibung des Aufbewahrungsdienstes samt allen technologischen, physischen und logischen Komponenten ist im Aufbewahrungshandbuch des Verwahrers enthalten.

5.4 Technische Bestimmungen und Bestimmungen des CNIPA 2004

Nach Maßgabe des Art. 14 Abs. 3 der Technischen Bestimmungen hat es die Körperschaft für angemessen befunden, die bereits nach den Bestimmungen des CNIPA 2004 aufbewahrten Dokumente im System CNIPA 2004 beizubehalten und bis zur Aufbewahrungsfrist der im System enthaltenen Dokumente unverändert zu belassen.

Zurück zum Inhaltsverzeichnis

6 Dokumente, die der Aufbewahrung unterzogen werden

Die aufbewahrungsgegenständlichen Dokumente umfassen alle digitalen Dokumente, die von der produzierenden Körperschaft gemäß dem Handbuch für die Dokumentenverwaltung der Körperschaft, dem Gesetz oder dem Archivierungsverfahren vorgesehen sind. Die Liste der Arten der aufbewahrten Dokumente und der Aufbewahrungsfristen ist in Anlage 1 „Aufbewahrungsfristen, Inhaltsklassen, Formate und Dateibetrachter“ enthalten.

Die digitalen Dokumente müssen statisch sein, d.h. sie dürfen keine dynamischen Elemente wie Makroanleitungen, externe Bezüge oder ausführbare Kodes und Informationen für die Abfassung wie Anmerkungen, Überarbeitungen, Lesezeichen, die von der für die Erstellung des Dokuments verwendete Software eingesetzt werden, enthalten.

Der Aufbewahrungsdienst gestattet die Aufbewahrung von digital unterschriebenen PDF- und XML-Dateien mit Zeitstempelung in folgenden Formaten: P7M (CAdES), PAdES (für PDF-Dateien), M7M, TSD. Die Dokumentendienste von InfoCamere gewährleisten die Gültigkeit der digital unterzeichneten Dokumente und die Zeitstempelung, deren Gültigkeit vom Aufbewahrungssystem nicht überprüft wird.

6.1 Formate

Die Formattypen, die von der produzierenden Körperschaft angewandt und verwaltet und zur Aufbewahrung übermittelt werden, sind in Anlage 1 „Aufbewahrungsfristen, Inhaltsklassen, Formate und Dateibetrachter“ detailliert angeführt.

Der Aufbewahrungsdienst InfoCamere garantiert die normgerechte Aufbewahrung nur für die Formate, die für die Aufbewahrung als angemessen erachtet werden und in Anlage 2 der Technischen Bestimmungen enthalten sind.

Die produzierende Körperschaft hat die Formate eingeführt, die für die Aufbewahrung tauglich und in Anlage 2 der Technischen Bestimmungen angeführt sind, da sie die Merkmale der Öffnung, Sicherheit, Übertragbarkeit, Funktionalität, Verbreitung, langfristigen Lesbarkeit und Unterstützung in der Entwicklung gewährleisten.

In außerordentlichen Fällen verwendet die produzierende Körperschaft Formate, die nicht auf der Liste aufscheinen, und zwar aus folgenden Gründen:

- wegen technischer Auflagen;
- wegen des spezifischen Formats;
- wegen der für das Dokument erforderlichen Dauer der Aufbewahrung.

Für diese Formate liefert die Körperschaft InfoCamere Hinweise in Bezug auf den verwendbaren Dateibetrachter, unter Berücksichtigung der Rechte des geistigen Eigentums und eventueller Einschränkungen in der Verwendung der Software.

6.2 Inhaltsklasse

Es werden die Modalitäten für die Aufbewahrung der Dokumente genehmigt, die im Aufbewahrungshandbuch von InfoCamere gemäß der archivischen Logik der ‚Dokumenteneinheit‘ und ‚Archiveinheit‘ beschrieben sind.

Mit Inhaltsklasse ist die Gesamtheit der Daten (Metadaten) gemeint, die der ‚Dokumenteneinheit' und der ‚Archiveinheit' zugeordnet wird, um sie zu identifizieren und den Kontext, Inhalt und Aufbau zu umschreiben. Diese Informationen sind in den Übergabe-, Archivierungs- und Ausgabepaketen des Aufbewahrungssystems enthalten.

Die Liste der Arten der aufbewahrten Dokumente und der Aufbewahrungsfristen ist in Anlage 1 „Aufbewahrungsfristen, Inhaltsklassen, Formate und Dateibetrachter" enthalten.

Sie wird aufgrund der von den Dokumentendiensten von InfoCamere verwendeten Inhaltsklassen aktualisiert.

Zurück zum Inhaltsverzeichnis

7 Der Aufbewahrungsprozess

Die Hauptprozesse des Aufbewahrungsdienstes sind:

- Aufbewahrung;
- Vorlegung;
- Produktion von Duplikaten und digitalen Kopien;
- Skartierungsverfahren.

7.1 Aufbewahrung

Der Aufbewahrungsprozess sieht folgende Phasen vor:

- Erstellung und Übermittlung des Übergabepakets seitens der produzierenden Körperschaft;
- Übernahme des übergebenen Paketes durch das Aufbewahrungssystem;
- Indexierung und Generierung des Archivierungspaketes.

Es folgen die Details der obengenannten Phasen.

7.1.1 Erstellung und Übermittlung des Übergabepakets

Die produzierende Körperschaft erzeugt die Übergabepakete durch die Dokumentendienste InfoCamere und übermittelt sie an das Aufbewahrungssystem. Die Übergabepakete enthalten eine Archiveinheit oder eine Dokumenteneinheit und entsprechen den Vorgaben des Aufbewahrungshandbuches von InfoCamere.

7.1.2 Übernahme des übergebenen Paketes durch das Aufbewahrungssystem

Das Aufbewahrungssystem führt die Kontrolle über das erhaltene Übergabepaket durch. Die Liste der automatischen Kontrollen am Übergabepaket ist im Aufbewahrungshandbuch von InfoCamere und in den technischen Merkmalen im Anhang zur Vereinbarung für die Erteilung des Dienstes enthalten.

Bei negativem Ausgang der Kontrollen teilt das Aufbewahrungssystem dem Dokumentendienst InfoCamere den erhobenen Fehler mit.

Bei positivem Ausgang der Kontrollen generiert das Aufbewahrungssystem einen Übergabebericht an den Dokumentendienst von InfoCamere, und das Paket wird vom System übernommen.

7.1.3 Indexierung und Generierung des Archivierungspaketes

Die Indexierung der Inhalte und die Generierung des Archivierungspaketes sind im Aufbewahrungshandbuch von InfoCamere beschrieben.

7.2 Vorlegung

Die Vorlegung der vom Aufbewahrungssystem aufbewahrten Dokumente erfolgt durch die eigens vorgesehene Webapplikation in Verbindung mit dem Dokumentendienst von InfoCamere. Die Vorlegung eines Dokuments durch diese Funktion ist den Mitarbeitern der produzierenden Körperschaft, die im Dokumentendienst für die Verwaltung/Verarbeitung des Dokuments zugelassen sind, gestattet.

Wird von einem körperschaftsinternen oder -externen Benutzer, der nicht zur Generierung der Ausgabepakete befugt ist, die normgerechte Vorlegung der aufbewahrten Dokumente gefordert, so muss der Verantwortliche für die Aufbewahrung:

- den Antrag prüfen und die Ausgabepakete aufgrund der geforderten Daten generieren, indem er sich direkt in das System einloggt oder befugte Benutzer der produzierenden Körperschaft mit der Generierung der Pakete betraut;
- dem Antragsteller den Inhalt der Ausgabepakete zur Verfügung stellen.

7.3 Produktion von digitalen Duplikaten

Die Produktion von Duplikaten erfolgt durch die spezifische Webapplikation zur Vorlegung der aufbewahrten Dokumente, welche die Ausgabepakete liefert.

7.4 Produktion von digitalen Kopien

Die produzierende Körperschaft muss:

- die Fälle prüfen, in denen originalkonforme Kopien erzeugt werden müssen;
- die Kopien erzeugen und bei Bedarf die Anwesenheit einer Amtsperson anfordern. Die Konformitätsbescheinigung obliegt der produzierenden Körperschaft, auch wenn eine Formatänderung erforderlich sein sollte.

Das Aufbewahrungssystem sieht eigene Metadaten für die Rückverfolgbarkeit der Übergabe von digitalen Kopien vor, die auch die Speicherung der Verbindung zwischen den einzelnen Fassungen der Dokumenteinheiten ermöglichen.

7.5 Skartierung der Archivierungspakete

Der Verantwortliche für die Dokumentenverwaltung führt im Einvernehmen mit dem Verantwortlichen für die Aufbewahrung nach Auslauf der vorgesehenen Aufbewahrungsfristen das Verfahren zur Skartierung der Dokumente und Faszikel, die in den Archivierungspaketen enthalten sind, gemäß den Angaben im Aufbewahrungsplan des Handbuches der Körperschaft, den geltenden Bestimmungen oder den Archivierungsverfahren durch.

Unter Beachtung des Dekrets 42/2004 obliegt es dem Verantwortlichen für die Dokumentenverwaltung, der zuständigen Aufsichtsbehörde die Liste der skartierbaren Inhalte zu liefern. Der Verantwortliche für die Dokumentenverwaltung passt nach Erhalt der entsprechenden Ermächtigung bei Bedarf die Skartierungsliste und die entsprechenden Modalitäten an die Beschlüsse der Behörde an.

Der Verantwortliche für die Dokumentenverwaltung liefert dem Aufbewahrungssystem die Liste der Identifikationsdaten der skartierbaren Inhalte; er kann dem Skartierungsantrag auch die Datei der

Skartierungsermächtigung beilegen, die von der Aufsichtsbehörde ausgestellt wird, damit sie auf diese Weise vom Aufbewahrungssystem aufbewahrt wird.

7.6 Überprüfung des Erhalts

Die produzierende Körperschaft erteilt dem Verwahrer die Aufgabe, den Erhalt der Archive regelmäßig zu prüfen. Der Verantwortliche für die Aufbewahrung kann vom Verwahrer über eine zertifizierte E-Mail die Auflistung der durchgeführten Kontrollen anfordern.

7.7 Rücktritt

Sollte die produzierende Körperschaft beabsichtigen, von der Vereinbarung für die Erteilung des Dienstes zurückzutreten, muss dies der Verantwortliche für die Aufbewahrung dem Verwahrer mittels zertifizierter E-Mail mitteilen.
Es ist Aufgabe des Verantwortlichen für die Aufbewahrung oder einer von ihm bevollmächtigten Person, die Archivierungspakete innerhalb der von der Vereinbarung für die Diensterteilung vorgesehenen Fristen herunterzuladen.

Zurück zum Inhaltsverzeichnis

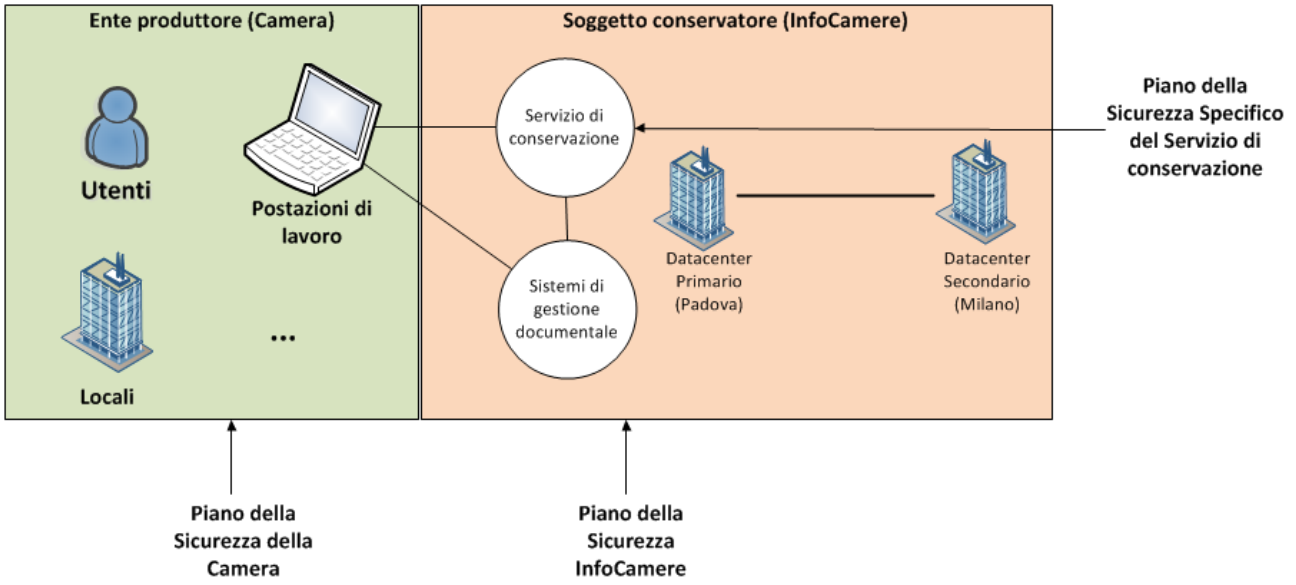
8 Plan für die Sicherheit des Aufbewahrungssystems

Im Einklang mit Art. 12 der Technischen Bestimmungen sorgt der Verantwortliche für die Aufbewahrung, im Einvernehmen mit dem Verantwortlichen für die Sicherheit, für die Erstellung des Sicherheitsplanes des Aufbewahrungssystems im Rahmen des allgemeinen Sicherheitsplanes und unter Beachtung der Sicherheitsmaßnahmen gemäß Art. 32 ff. der EU-Verordnung 2016/679 und der Vorgaben des Artikels 51 des Kodex für die digitale Verwaltung.

Der Sicherheitsplan des Aufbewahrungssystems gewährleistet, dass:

- die Dokumente und Informationen, die vom Aufbewahrungssystem verarbeitet werden, unversehrt und vertraulich zur Verfügung stehen;
- die gemeinen, sensiblen und/oder gerichtlichen personenbezogenen Daten so aufbewahrt werden, dass die Risiken der Beschädigung oder des auch nur zufälligen Verlustes, des unbefugten Zuganges oder der unerlaubten oder nicht den Sammelzwecken entsprechenden Behandlung mit Bezug auf den technischen Fortschritt, auf ihre Beschaffenheit und auf die spezifischen Merkmale der Behandlung durch die Anwendung geeigneter und vorab ergriffener Sicherheitsmaßnahmen auf ein Mindestmaß reduziert werden.

Die gesamte Sicherheit des Aufbewahrungssystems wird durch die Gesamtheit der Sicherheitsmaßnahmen gewährleistet, die von der produzierenden Körperschaft oder vom Verwahrer innerhalb der entsprechenden Verantwortung ergriffen werden, wie im nachfolgenden Schema dargestellt:



Der Verwahrer bestimmt und setzt angemessene Sicherheitsmaßnahmen für die Lieferung des Aufbewahrungsdienstes um. Die Zuweisung des Dienstes an InfoCamere als akkreditierten Verwalter gewährleistet zudem, dass das Aufbewahrungssystem:

- die Voraussetzungen gemäß Sicherheitsstandard ISO 27001:2013, einschließlich der anwendbaren Kontrollen gemäß Standard ISO 27002:3013, erfüllt;
- den geltenden einschlägigen Vorschriften, insbesondere der Verordnung (EU) 2016/679 entspricht;
- die Qualitäts- und Sicherheitsvoraussetzungen erfüllt, die von AgID für die akkreditierten Verwahrer festgelegt werden;
- über einen spezifischen Sicherheitsplan verfügt, der regelmäßig aktualisiert wird.

Der Verwahrer verpflichtet sich, der produzierenden Körperschaft eventuelle bedeutende Änderungen an der eigenen Sicherheitspolitik mitzuteilen.

Die produzierende Körperschaft definiert und setzt angemessene Sicherheitsmaßnahmen für die unter ihre Verantwortung fallenden Bereiche um, insbesondere für:

- die eigenen Räumlichkeiten und die Betriebskontinuität der produzierenden Körperschaft bei Katastrophen (siehe 8.1.2 und 8.1.9);
- die vom Personal der produzierenden Körperschaft verwendeten Arbeitsplätze für die Verwaltung der digitalen Dokumente (siehe 8.1.3-8);
- die Ausbildung und Verhaltensweisen des Personals der produzierenden Körperschaft (siehe 8.1.1).

8.1 Sicherheitsmaßnahmen der produzierenden Körperschaft

Die produzierende Körperschaft sieht Maßnahmen zur Gewährleistung der Sicherheit des Aufbewahrungssystems im Rahmen der allgemeinen Sicherheit der eigenen Prozesse und Arbeitsflüsse vor. Die Sicherheitsmaßnahmen sind im Dokument „Anweisung für die Verwendung der digitalen Ausrüstungen“ enthalten, das mit Beschluss des Handelskammerausschusses vom 25.05.2009, Nr. 76 genehmigt wurde. Zudem wurden dem gesamten Personal der Körperschaft und den betroffenen Dritten Sicherheitsmaßnahmen mitgeteilt; diese Maßnahmen sehen folgende einzuhaltende Regeln vor:

8.1.1 Ausbildung des Personals

Mit Bezug auf die Pläne für die Ausbildung des Personals der produzierenden Körperschaft garantiert die Körperschaft für das an der Aufbewahrung beteiligte Personal Folgendes:

- die Aus- und Fortbildungsinitiativen dienen der Erhaltung und Entwicklung der Kenntnisse der Körperschaft im Sinne der Weiterbildung und sollen dem Ausbildungsbedarf und den rechtlichen, institutionellen und technologischen Entwicklungen gerecht werden;
- Die Ausbildung jeder einzelnen Person erfolgt auf der Grundlage einer Planung, welche den befolgten Bildungsweg, die Berufsfigur und die Tätigkeiten, welche die Person ausübt oder ausüben wird, sowie die Kompetenzen und das erwiesene Personal berücksichtigt.

8.1.2 Kontrolle über die physischen Zugänge

Die Kontrolle über die physischen Zugänge ist für die Sitze und Räumlichkeiten vorgesehen, in denen Verarbeitungen in Verbindung mit dem Aufbewahrungsdienst durchgeführt werden; daher wird der Zugang zu den Sitzen und Räumlichkeiten der produzierenden Körperschaft geregelt und kontrolliert.

8.1.3 Kontrolle über die logischen Zugriffe

Die Kontrolle über die logischen Zugriffe findet auch im spezifischen Fall der Aufbewahrung Anwendung; daher ist auch in diesem Bereich die Einschränkung des Zugangs zu den Informationen und Diensten für die Ausarbeitung der Informationen aufgrund des Prinzips „need to access“, das heißt nur für die tatsächlichen und berechtigten betrieblichen Notwendigkeiten ein wesentliches Ziel der Sicherheit der Informationen in der Körperschaft.
Zu diesem Zweck werden das gesamte Personal der Körperschaft und betroffene Dritte über das Bestehen spezifischer Maßnahmen für die Verwaltung und die Kontrolle der logischen Zugriffe informiert und sind je nach Verantwortung oder Kompetenz verpflichtet, die Vorschriften einzuhalten, insbesondere in Bezug auf:

- **Verwaltung der Zugangsdaten**
- **Verwendung der Passwörter**

- **Verantwortung der Benutzer**

Die Mittel und Anweisungen für die Kontrolle der Zugänge werden durchgehend an die Dienstbedürfnisse der Körperschaft und an die Anforderungen an die Sicherheit der Zugänge, auch in Bezug auf die organisatorischen und technologischen Entwicklungen, angepasst.

8.1.4 Verwaltung der in den aufbewahrten Dokumenten enthaltenen personenbezogen Daten

Die produzierende Körperschaft gewährleistet die Sicherheit der personenbezogenen Daten, die im Aufbewahrungssystem enthalten sind, im Sinne der Vorgaben des GvD 196/03 i.g.F. und der EU-Verordnung 2016/679.

8.1.5 Verwaltung der Arbeitsplätze

Die Verarbeitung der Informationen und der digitalen Dokumente an den Arbeitsplätzen der produzierenden Körperschaft hat unter Beachtung der guten Sicherheitspraktiken zu erfolgen; daher werden dem zuständigen Personal Regeln zu folgenden Themen mitgeteilt:

- **Software-Upgrades;**
- **Einschränkung der Verbindungen zu externen Datenträgern;**
- **Änderung der Einstellungen der Arbeitsplätze;**
- **Konfiguration der Arbeitsplätze.**

8.1.6 Verwaltung, Stilllegung und Entsorgung der mobilen Geräte und der Datenträger

In Bezug auf die Verwaltung, die Stilllegung und Entsorgung der Arbeitsplätze der produzierenden Körperschaft (einschließlich der mobilen Geräte) und der Datenträger (auch abnehmbarer Art) müssen dem zuständigen Personal Regeln zu folgenden Themen mitgeteilt werden:

- **Verwaltung der Geräte und Datenträger;**
- **Stilllegung der Geräte und Datenträger;**
- **Verwaltung der Unterlagen auf Papier;**
- **Vernichtung der Unterlagen auf Papier.**

8.1.7 Schutz vor Malware

Der Schutz vor Malware erfordert die Beachtung folgender Regeln:

- Die Informationen, die Eigentum der Körperschaft sind oder von ihr verwaltet werden, und die für ihre Verarbeitung zuständigen IT-Strukturen sind vor Malware geschützt.
- In Bezug auf Malware sind Kontrollen zur Ermittlung, Vorbeugung und Wiederherstellung vorgesehen.

Die produzierende Körperschaft fördert ein angemessenes Bewusstsein der Benutzer, um den Gefahren und der Verwundbarkeit durch Malware vorzubeugen und sieht **geeignete Gegenmaßnahmen zum Schutz vor Malware vor, die nachfolgend angeführt werden:**

- Die Software zum Schutz vor Malware (sog. Antivirenprogramm) wird auf allen Geräten installiert, die vom Personal der Körperschaft verwendet werden, unabhängig davon, ob es sich um Server für die Lieferung von Diensten oder Arbeitsplätze, von denen aus der Zugriff auf die Dienste getätigt wird, handelt; das Antivirenprogramm wird sei es in physische Systeme (Server, PC) als auch in virtuelle Systeme, welche die Körperschaft verwendet, installiert.

- In den „Endpoint“-Systemen, in denen das Antivirenprogramm installiert wird, ist dieses immer aktiv; dabei wird jede Dateienbewegung in Echtzeit überprüft, um das Gerät vor Malware zu schützen.
- Die oben beschriebenen Komponenten werden periodisch aktualisiert, um angemessene Sicherheitsmaßnahmen zu gewährleisten.

8.1.8 Sauberer Schreibtisch und Bildschirm

Um unbefugte Zugriffe auf vertrauliche Informationen zu vermeiden, werden dem gesamten Personal der produzierenden Körperschaft Regeln zu folgenden Themen mitgeteilt:

- **sauberer Schreibtisch;**
- **sauberer Bildschirm.**

8.1.9 Wiederherstellung des Dienstes und Betriebskontinuität

Die produzierende Körperschaft gewährleistet, im Rahmen ihrer Zuständigkeit, die Betriebskontinuität des Aufbewahrungssystems.

Zurück zum Inhaltsverzeichnis