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
2022_1	20.01.2022		

Inhaltsverzeichnis

1 Zweck und Anwendungsbereich des Dokuments

Dieses Handbuch beschreibt das Aufbewahrungssystem im Sinne des Art. 44 des Kodex für die digitale Verwaltung und der „Richtlinien über die Erstellung, Verwaltung und Aufbewahrung informatischer Dokumente".

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, welcher der Inhouse-Gesellschaft der Handelskammern InfoCamere K.A.G. anvertraut wird, ist im Handbuch für die Aufbewahrung des verwahrenden Rechtsträgers genauer beschrieben und steht unter https://conservazione.infocamere.it zur Verfügung.

Das vorliegende Handbuch wird vom Verantwortlichen für die Aufbewahrung erstellt und ist durch die Veröffentlichung auf der institutionellen Internetseite im Bereich „Transparente Verwaltung" [https://www.handelskammer.bz.it/de/transparente-verwaltung/weitere-inhalte/handhabung-von-dokumenten] für den verwahrenden Rechtsträger und andere im Aufbewahrungsprozess beteiligte Subjekte einsehbar. Eventuelle Änderungen werden umgehend mitgeteilt.

Zurück zum Inhaltsverzeichnis

2 Begriffsbestimmungen (Glossar und Abkürzungen)

Glossar und Abkürzungen	
AgID	Agenzia per l'Italia Digitale
Dublin Core	ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Metadatensystem des Dublin Core.
Datenschutzkodex	Gesetzesvertretendes Dekret Nr. 196 vom 30. Juni 2003 und darauffolgende Änderung – Kodex über den Schutz personenbezogener Daten
Ersteller des SIP	natürliche oder juristische Person (in der Regel nicht der Verfasser des Dokuments), welche das Übergabepaket (SIP) erstellt und für die Übertragung des Inhalts in das Aufbewahrungssystem verantwortlich ist. In den öffentlichen Verwaltungen ist dies der Verantwortliche für die Dokumentenverwaltung.
GDPR	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
AgID-Richtlininen	Richtlinien über die Erstellung, Verwaltung und Aufbewahrung informatischer Dokumente
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.
Archivierungspaket (AIP)	Informationspaket, das durch die Umwandlung eines oder mehrerer Übergabepakete gemäß den im Aufbewahrungshandbuch festgelegten Verfahren erzeugt wird.
Ausgabepaket (DIP)	Informationspaket, das vom Aufbewahrungssystem an den Benutzer als Antwort auf eine Benutzeranfrage für den Zugriff auf aufbewahrte Daten gesendet wird.
Übergabepaket (SIP)	Informationspaket, das gemäß dem im Aufbewahrungshandbuch beschriebenen Format vom Hersteller an das Aufbewahrungssystem gesendet wird.
Dateipaket (file package)	Endliche Menge mehrerer Dateien (möglicherweise in einer Teilbaumstruktur innerhalb eines Dateisystems organisiert), die sowohl gemeinsam als auch einzeln einen einheitlichen und in sich konsistenten Informationsgehalt bilden.
Sicherheitsplan	Dokument, das im Rahmen des allgemeinen Sicherheitsplanes die Tätigkeiten für den Schutz des Aufbewahrungssystems für informatische Dokumente vor möglichen Risiken im Bereich der Organisation beschreibt und plant
Bestimmungen des CNIPA 2004	Beschluss des CNIPA Nr. 11/2004 vom 19. Februar 2004 - Technische Bestimmungen für die Kopie und Aufbewahrung von Dokumenten auf einem Datenträger, der geeignet ist, um die Konformität mit dem Original zu gewährleisten
Verordnung über die Kriterien für die Bereitstellung von Aufbewahrungssystemen	Verordnung über die Kriterien für die Bereitstellung von Diensten zur Aufbewahrung informatischer Dokumente und deren Anlagen laut Art. 34, Abs. 1bis, Buchstabe B) des Kodex der digitalen Verwaltung
Verantwortlicher für die Aufbewahrung	Verantwortlicher für die Tätigkeiten, die in Absatz 4.5 der Richtlinien über die Erstellung, Verwaltung und Aufbewahrung informatischer Dokumente aufgelistet sind

CNIPA-System 2004	Aufbewahrungssystem, das die technischen Bestimmungen gemäß Beschluss CNIPA Nr. 11/2004 vom 19. Februar 2004 berücksichtigt
Dokumenten-verwaltungssystem	Elektronische Anwendung für die Verwaltung von informatischen Dokumenten
Ersteller	Inhaber des aufzubewahrenden Dokuments
Archiveinheit (UA)	kleinste elementare Einheit aus der ein Archiv besteht, welche aus zusammenhängenden Dokumenten oder aus einem Faszikel bestehen kann.
Dokumenteinheit (UD)	Allgemeiner Begriff für die kleinste unteilbare Einheit eines Archivbestands, der mehrere logisch zusammenhängende Dokumente umfassen kann.
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 informatischen 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;
- Richtlinien über die Erstellung, Verwaltung und Aufbewahrung informatischer Dokumente;
- Dekret des Präsidenten des Ministerrates vom 3. Dezember 2013 - Technische Bestimmungen für das elektronische Protokoll im Sinne der Artikel 40-bis, 41, 47, 57-bis und 71 des Kodex der digitalen Verwaltung gemäß gesetzesvertretendem Dekret Nr. 82/2005;
- Richtlinien, welche die technischen Bestimmungen und Empfehlungen betreffend die Erstellung qualifizierter elektronischer Zertifikate, Unterschriften und qualifizierter elektronischer Siegel sowie qualifizierter elektronischer Zeitstempel beinhalten;
- Dekret des Wirtschafts- und Finanzministeriums vom 17. Juni 2014 - Modalitäten für die Abwicklung der steuerrechtlichen Pflichten in Bezug auf informatische Dokumente und deren Reproduktion auf verschiedenen Datenträgern - 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;
- Verordnung über die Kriterien für die Leistung von Aufbewahrungsdiensten für informatische Dokumente und deren Anhänge, im Sinne des Art. 34, Abs. 1bis, Buchstabe B) des Kodex der digitalen Verwaltung;
- Beschluss des CNIPA vom 21. Mai 2009, Nr. 45 - Bestimmungen für die Anerkennung und die Prüfung

des informatischen Dokuments.

Zurück zum Inhaltsverzeichnis

3.2 Bezugsstandards

- ISO 14721:2012 OAIS (Open Archival Information System), Offenes System für die digitale Archivierung;
- ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements, Voraussetzungen eines ISMS (Information Security Management System);
- ISO 9001 Management- und Qualitätssysteme - Voraussetzungen
- ETSI TS 101 533-1 V1.3.1 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 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 Standard SInCRO - Support für die Interoperabilität in der Aufbewahrung und Einholung der digitalen Dokumente;
- ISO 15836 Information and documentation - The Dublin Core metadata element set, Metadatensystem des Dublin Core.
- ISO/TS 23081 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 - Managing metadata for records – Part 2: Conceptual and implementation issues, Praktischer Leitfaden für die Implementierung.
- 23081-3 - 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 Organisationsmodell

Die Handelskammer Bozen hat den Aufbewahrungsdienst an die Gesellschaft der italienischen Handelskammern für die digitale Innovation, InfoCamere K.A.G., übertragen, welche im Verzeichnis der akkreditierten Aufbewahrer eingetragen ist und über die Voraussetzungen in den Bereichen Qualität, Sicherheit und Organisation verfügt, welche im Sinne der europäischen Bestimmungen, der Richtlinien laut Art. 71 betreffend die Erstellung, Verwaltung und Aufbewahrung informatischer Dokumente und in der AGID-Verordnung über die Kriterien für die Leistung von Aufbewahrungsdiensten für informatische Dokumente vorgesehen sind.

Die Aufbewahrungstätigkeiten für die obligatorischen Dienste werden aufgrund der Konsortialbindung durchgeführt, gemäß Artikel 2 der Konsortialverordnung, die die wesentlichen Dienste von InfoCamere für die Handelskammern festlegt.

Die Kammer hat sich für das Modell des Outsourcings entschieden, obwohl sie die Aufbewahrungsleistung von einem Inhouse-Subjekt in Anspruch nimmt

Die wichtigsten Merkmale des Organisationsmodells, das in Übereinstimmung mit dem OAIS-Funktionsmodell angenommen wurde, sind nachstehend grafisch dargestellt:

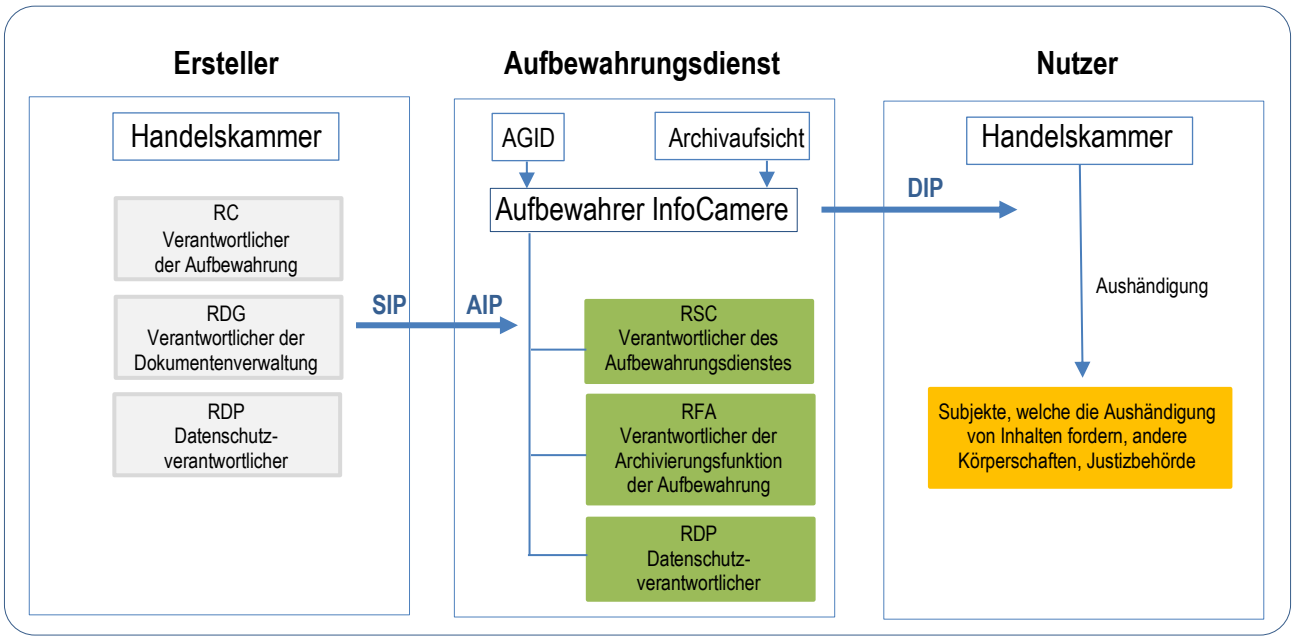

Abbildung 1 – Organisationsmodell

Im Rahmen ihrer institutionellen Tätigkeit kann die Handelskammer InfoCamere auch mit dem Aufbewahrungsdienst für fakultative Dienstleistungen beauftragen, die in Art. 3 der oben genannten Verordnung geregelt sind, sowie mit den Dienstleistungen, die den kleinen und mittleren Unternehmen von den Handelskammern angeboten werden.

Um den Digitalisierungsprozess kleiner und mittlerer Unternehmen zu erleichtern, bietet die Kammer Dienstleistungen für die Verwaltung und Aufbewahrung elektronischer Rechnungen, Bücher und digitaler Buchhaltungsunterlagen an. In diesen Fällen übernimmt die Kammer die Rolle des Verantwortlichen für die Aufbewahrung, während das Unternehmen, das die Dienstleistung in Anspruch nimmt, das Eigentum an den in

die IT-Systeme eingegebenen und zur Speicherung übermittelten Dokumenten behält, wie im Folgenden zusammengefasst:

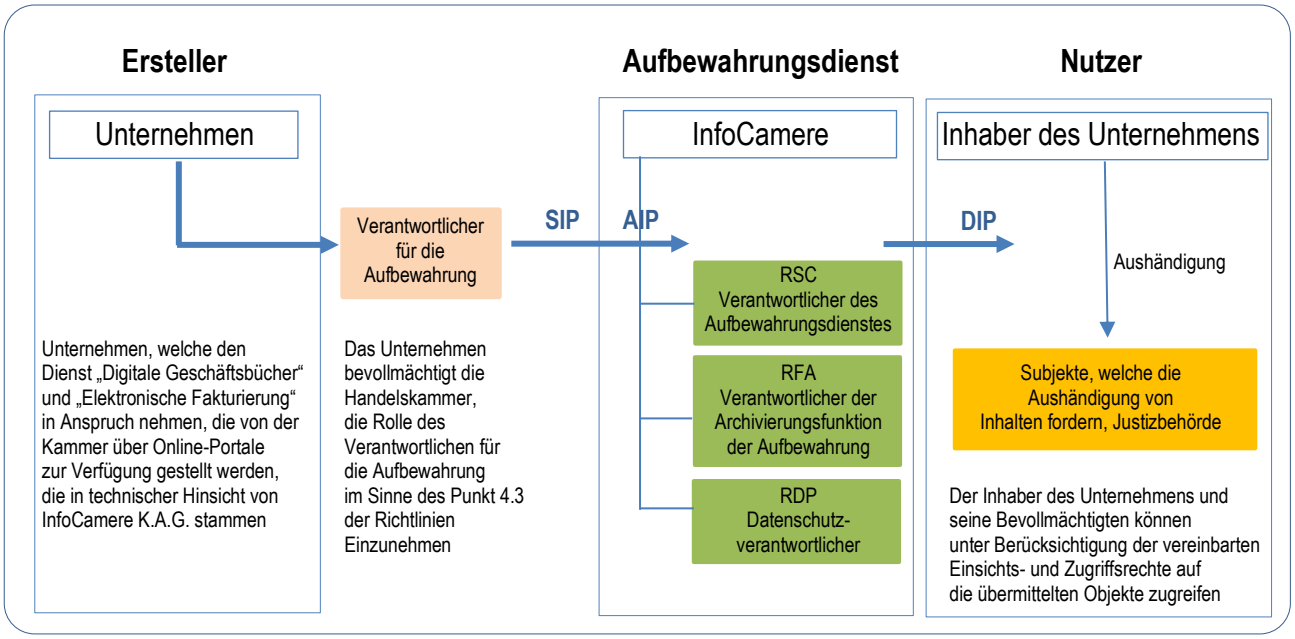

Abbildung 2 – Organisationsmodell für die Aufbewahrung von Dokumenten von Unternehmen

Die Beziehungen zwischen den Unternehmen, welche die betreffenden digitalen Dienste in Anspruch nehmen, und der Kammer werden durch spezifische allgemeine Bedingungen für die Erbringung des Dienstes und durch die damit verbundenen technischen Spezifikationen geregelt. In dem Dokument werden insbesondere die Art der angebotenen Dienstleistungen, die Zuständigkeiten, die wirtschaftlichen Bedingungen und die Modalitäten für die Übermittlung der Datenpakete festgelegt.

Die informatischen Dokumente im Eigentum der Unternehmen werden in zumindest logisch von den aufbewahrten Daten der Kammer getrennten Bereichen aufbewahrt.

Zurück zum Inhaltsverzeichnis

5 Rollen und Verantwortungen

Inhaber der aufbewahrten Objekte

Die Handelskammer ist Eigentümerin der gespeicherten informatischen Dokumente und definiert und implementiert über ihren Verantwortlichen für die Aufbewahrung die allgemeine Politik des Aufbewahrungssystems und regelt dessen Verwaltung mit voller Verantwortung und Autonomie.

Die Kammer, Eigentümerin des aufzubewahrenden Dokuments, übermittelt an InfoCamere K.A.G. die in Punkt 1 dieses Handbuchs genannten, aufzubewahrenden informatischen Dokumente. Diese Übertragung erfolgt laufend mit den begonnenen Verfahren zur Dokumentenverwaltung.

Die Beziehungen zwischen Ersteller und Aufbewahrer werden anhand einiger grundlegender Dokumente geregelt:

1. Vereinbarung für die Beauftragung mit dem Dienst zur Aufbewahrung der informatischen Dokumente.
2. Vereinbarung über die Bearbeitung der personenbezogenen Daten im Sinne des Art. 28 der EU-Verordnung 2016/679 im Bereich der Aufbewahrungsdienste informatischer Dokumente.
3. die auf dem Portal https://conservazione.infocamere.it veröffentlichten technische Bestimmungen.

Die Namen der anderen beteiligten Personen und eine Beschreibung der wichtigsten Tätigkeiten, die von den Personen mit organisatorischen Aufgaben innerhalb der Handelskammer ausgeführt werden, sind im Handbuch für die Dokumentenverwaltung angeführt.

Die von Punkt 4.5 der Richtlinien vorgesehenen Phasen des Aufbewahrungsprozesses werden an InfoCamere K.A.G. übertragen.

Der Verantwortliche für die Aufbewahrung der Handelskammer muss weiterhin folgende Aufgaben erfüllen:

- die Aufbewahrungspolitik und die funktionellen Anforderungen an das Aufbewahrungssystem unter Beachtung der geltenden Rechtsvorschriften und unter Berücksichtigung der internationalen Normen auf der Grundlage der Besonderheiten der aufzubewahrenden Inhalte (informatische Dokumente, Datenpakete, informatische Archive), der Art der vom Eigentümer der Inhalte durchgeführten Tätigkeiten und der Merkmale des angewandten informatischen Dokumentenverwaltungssystems festzulegen;

- die Anwesenheit einer Amtsperson zu gewährleisten, falls deren Intervention notwendig sein sollte, und dieser die notwendige Hilfestellung und Ressourcen für die Durchführung der ihr zugewiesenen Aufgaben zu garantieren.

Die Handelskammer ist weiterhin Inhaber und Eigentümer der aufbewahrten Dokumente.
Die Kammer ist für den Inhalt der Übergabepakete verantwortlich und verpflichtet, diese gemäß den in diesem Handbuch und seinem Anhang beschriebenen Modalitäten an das Aufbewahrungssystem zu übermitteln.
Die zu übertragenden Dokumententypen und -formate, die Methoden der Übermittlung und die Metadaten werden im Anhang dieses Handbuchs und in den technischen Bestimmungen vereinbart und festgelegt.
Die Kammer ist nicht Eigentümerin der Unterlagen, die über die Dienste "Elektronische Faktuierung" und "Digitale Geschäftsbücher" zur Aufbewahrung übermittelt werden.

Ersteller der Übergabepakete (SIP)

Die AGID-Richtlinien sehen vor, dass der Verantwortliche der Dokumentenverwaltung die Übergabepakete (SIP) erstellt. Der Ersteller der Übergabepakete ist für die Erstellung und Übermittlung des Inhalts an das Aufbewahrungssystem verantwortlich. Er prüft auch den Erfolg der Übermittlung an das Aufbewahrungssystem, indem er den vom Aufbewahrungssystem selbst erstellten Übermittlungsbericht einsieht.

Bei den Diensten "Digitale Geschäftsbücher" und "Elektronische Fakturierung", die den Unternehmen angeboten werden, fungiert die Kammer als Verantwortlicher des Aufbewahrungsdienstes (unter Nutzung der von InfoCamere bereitgestellten IT-Dienste) und die Erstellung der Übergabepakete erfolgt automatisch. Die technischen Bestimmungen und ihre Aktualisierungen werden dem Unternehmen durch die Aushändigung derselben bei Vertragsunterzeichnung bekannt gegeben.
Das Unternehmen hat immer einen direkten Überblick über die Erstellung des aufzubewahrenden Datenpakets und Einsicht in den zeitlichen Ablauf, kann aber auch die Ergebnisse vorwegnehmen, wobei es stets Eigentümer des Verfahrens und des Inhalts bleibt und die Automatisierung der Aktivitäten zur Erstellung des aufzubewahrenden Pakets verwalten kann.

Verwahrer / InfoCamere

InfoCamere fungiert gemäß den AgID-Richtlinien als externe Verwahrungsstelle und übernimmt die Rolle des Verantwortlichen für die Datenverarbeitung, wie sie im Datenschutzgesetz vorgesehen ist, garantiert die Einhaltung der Anforderungen, die in den jeweils geltenden Vorschriften für die Aufbewahrungssysteme festgelegt sind und führt alle in Absatz 4.7 der AgID-Richtlinien aufgelisteten Tätigkeiten aus.

Als akkreditierter Verwahrer und in Übereinstimmung mit den vorgesehenen Bestimmungen:

- 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 Erstellers vor.

Benutzer

Die AGID-Richtlinien bezeichnen den Benutzer als eine Person, eine Körperschaft oder ein System, die oder das mit den Diensten eines Aufbewahrungssystems informatischer Dokumente interagiert. Der Benutzer kann intern oder außerhalb der produzierenden Körperschaft tätig sein. Die befähigten Nutzer des Aufbewahrungssystems sind in der Handelskammer tätig.
Der Benutzer ersucht das Aufbewahrungssystem um Zugang zu den informatischen Dokumenten, um die ihn interessierenden Informationen im Rahmen der gesetzlichen Bestimmungen einzuholen. Das Aufbewahrungssystem gestattet den ermächtigten Subjekten den auch im Fernzugriff möglichen Zugang zu den aufbewahrten digitalen Dokumenten und ermöglicht die Produktion eines Ausgabepaketes (DIP), das direkt von den ermächtigten Benutzern übernommen werden kann.

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

Der Verantwortliche für die Aufbewahrung

Der Verantwortliche für die Aufbewahrung ist eine in der öffentlichen Verwaltung vorgesehene Funktion, die im Organisationsplan des Eigentümers der aufzubewahrenden, informatischen Dokumente vorgesehen ist; sie wird durch einen Verwaltungsakt aus dem Kreis der Führungskräfte und Beamten ernannt, die über geeignete juristische, informationstechnische und archivarische Kenntnisse verfügen, und kann vom Leiter der Dokumentenverwaltung oder vom Koordinator der Dokumentenverwaltung, sofern ernannt, wahrgenommen werden.
Für andere Subjekte (also nicht öffentliche Körperschaften) kann die Rolle des Verantwortlichen für die Aufbewahrung von einer organisationsfremden Person mit geeigneten juristischen, IT- und Archivierungskenntnissen wahrgenommen werden. Es darf sich jedoch nicht direkt um den Aufbewahrer selbst handeln, um die Funktion des Eigentümers der aufzubewahrenden Dokumente in Verhältnis zum Verwahrer getrennt zu halten.

Der Verantwortliche für die Aufbewahrung muss mit Unterstützung des Verantwortlichen des Aufbewahrungssystems:
a) die Aufbewahrungspolitik und die funktionellen Anforderungen an das Aufbewahrungssystem in Übereinstimmung mit den geltenden Rechtsvorschriften und unter Berücksichtigung internationaler Normen festlegen, und zwar auf der Grundlage der Besonderheiten der aufzubewahrenden Inhalte (informatische Dokumente, Datensätze, informatische Archive), der Art der vom Inhaber der aufbewahrten Inhalte ausgeübten Tätigkeiten und der Merkmale des eingesetzten informatischen Dokumentenverwaltungssystems;
b) den Aufbewahrungsprozess verwalten und über den gesamten Zeitraum dessen Konformität mit den geltenden Bestimmungen garantieren;
c) den Übergabebericht mit den vom Aufbewahrungshandbuch vorgesehenen Modalitäten generieren und unterzeichnen;
d) das Ausgabepaket (DIP) generieren und mit digitaler Unterschrift oder qualifizierter digitaler Unterschrift in den vom Aufbewahrungshandbuch vorgesehenen Fällen unterzeichnen;
e) über den korrekten Betrieb des Aufbewahrungssystems wachen;
f) mindestens alle 5 Jahre die periodische Prüfung der Integrität und Lesbarkeit der informatischen Dokumente und der Faszikel in den Archiven durchführen;
g) im Sinne der Gewährleistung der Aufbewahrung und des Zugangs zu den digitalen Dokumenten die erforderlichen Maßnahmen ergreifen, 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) für die Duplikation oder Kopie der digitalen Dokumente in Hinblick auf die technologische Entwicklung laut Angaben im Aufbewahrungshandbuch sorgen;
i) die erforderlichen Maßnahmen für die physische und logische Sicherheit des Aufbewahrungssystems im Sinne des Art. 4.1 der AGID-Richtlinien ergreifen;
j) die Anwesenheit einer Amtsperson gewährleisten, falls die Betätigung derselben gefordert wird, und ihr die erforderliche Hilfestellung und die Ressourcen für die Ausführung ihrer Aufgaben liefern;
k) den von den geltenden Bestimmungen vorgesehenen zuständigen Organen die Hilfestellung und die erforderlichen Ressourcen für die Ausführung der Prüf- und Aufsichtstätigkeiten liefern;
l) die informatischen Dokumente, die Datensätze und informatischen Archive sowie die zu deren Lesbarkeit notwendigen Instrumente im Sinne des Art. 41, Abs. 1 des Kodex der Kulturgüter für die staatlichen und territorialen Stellen an das Staatsarchiv und die jeweils zuständigen territorialen Archive (bzw. Landesarchiv) übermitteln;
m) das Aufbewahrungshandbuch gemäß Abs. 4.7 verfassen und anlässlich von gesetzlichen, organisatorischen, verfahrenstechnischen oder bedeutenden technologischen Änderungen regelmäßig aktualisieren.

Die Handelskammer hat den Vizegeneralsekretär Luca Filippi mit Beschluss des Kammerausschusses Nr. 158 vom 25.11.2019 zum Verantwortlichen für die Aufbewahrung ernannt.

Der Verantwortliche für die Aufbewahrung stellt das vorliegende Handbuch dem beauftragten Aufbewahrer und allen an der Aufbewahrung beteiligten Subjekten zur Verfügung und informiert diese umgehend über eventuelle Neuerungen.

Der Verantwortliche für die Aufbewahrung der Handelskammer übt diese Rolle auch für die Unternehmen aus, welche die von der Kammer zur Verfügung gestellten Dienste „Digitale Geschäftsbücher“ oder „Elektronische Fakturierung“ in Anspruch nehmen.

5.1 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	

5.2 Amtsperson

Die Funktion der Amtsperson, welche wie von Art. 23 bis, Abs. 2 des G.v.D. Nr. 82 vom 7. März 2005 – Kodex der digitalen Verwaltung vorgesehen die Übereinstimmung der Kopien mit den informatischen Dokumenten bestätigt, die in dem von InfoCamere K.A.G. verwalteten System aufbewahrt werden, wird vom Verantwortlichen für die Aufbewahrung oder dessen Stellvertreter übernommen.

Zurück zum Inhaltsverzeichnis

6 Schutz- und Aufsichtsorgane

Die Archive und die einzelnen, von den Handelskammern erstellten Dokumente bilden Kulturgut und unterliegen somit den vom Kodex der Kultur- und Landschaftsgüter vorgesehenen Schutzbestimmungen.

Die Aufsicht über die Einhaltung der Bestimmungen betreffend die korrekte Archivierung obliegt dem Kulturministerium durch die Generaldirektion der Archive bzw. dem Südtiroler Landesarchiv.

Was das Aufbewahrungssystem der Handelskammer Bozen anbelangt, kann die zuständige Stelle vor allem überprüfen, dass die Aufbewahrung im Einklang mit den Rechtsvorschriften und den Grundsätzen der ordnungsgemäßen und ununterbrochenen Aufbewahrung erfolgt, und genehmigt die Aussonderung und Weitergabe der aufbewahrten Dokumente.

Der Gesetzgeber hat eine weitere Körperschaft vorgesehen, welche die zuständigen Organe im Rahmen der digitalen Aufbewahrung unterstützt, aber eine andere Rolle einnimmt: die Agenzia per l'Italia Digitale (AgID).

Die AgID hat die Aufgabe, im Hinblick auf die digitalen Systeme zur Aufbewahrung von Archiven und informatischen Dokumenten, die notwendigen Überprüfungen hinsichtlich der Einhaltung der Anforderungen für Einrichtungen durchzuführen, die beabsichtigen, den Aufbewahrungsdienst im Auftrag der öffentlichen Verwaltungen zu erbringen.

Die Anforderungen sind in der Verordnung über die Kriterien für die Erbringung von Dienstleistungen im Bereich der Aufbewahrung von informatischen Dokumenten festgelegt, die den bisherigen Akkreditierungsmechanismus für diese Anbieter ersetzt.

Die Aufsichtstätigkeit der AgID betrifft daher die Stelle, welche den Aufbewahrungsdienst erbringt, und das Aufbewahrungssystem als Ganzes, d. h. die Gesamtheit der Regeln, Verfahren und Technologien, die die ordnungsgemäße Aufbewahrung von informatischen Dokumenten und Faszikeln und der zugehörigen Metadaten in jeder Phase des Lebenszyklus eines Dokuments - von der Übernahme bis zur Vernichtung - gewährleisten sollen.

7 Aktivierung des Dienstes

7.1 Anvertrauung des Dienstes

Mit der im Februar 2022 erfolgten Unterzeichnung der Vereinbarung für die Erteilung des normgerechten Aufbewahrungsdienstes für informatische Dokumente hat der Verantwortliche für die Aufbewahrung das Verfahren zur Aufbewahrung der informatischen Dokumente, die sich im Eigentum der Kammer befinden, InfoCamere anvertraut. Der Dienst endet mit 31.12.2026.

Der Verantwortliche für die Aufbewahrung hat InfoCamere auch damit beauftragt, die Inhalte aufzubewahren, welche von Unternehmen durch die Dienste „Digitale Geschäftsbücher“ und „Elektronische Fakturierung“ übermittelt werden.

7.2 Zugang zum Dienst

Laut dem von der Kammer angewandten Organisationsmodell können die zum Zugriff auf das Dokumentenverwaltungssystem der Körperschaft berechtigten Nutzer in das Aufbewahrungssystem einsehen. Die Einsichtnahme ist auf die vom Zugehörigkeitsbereich erstellten oder zugeteilten Dokumente bzw. auf die Dokumente, zu deren Einsichtnahme sie befähigt waren, beschränkt. Diese Dienste:

- generieren die Übergabepakete;
- ergänzen die Anwendung für die Aushändigung der aufbewahrten Inhalte, welche die Ausgabepakete generiert.

Die befähigten Nutzer können auch durch das Aufbewahrungsportal http://conservazione.infocamere.it auf das Aufbewahrungssystem zugreifen.
Auch der Verantwortliche für die Aufbewahrung und dessen Stellvertreter können auf das Aufbewahrungsportal zugreifen.
Der Zugang zu Dokumenten, welche im Rahmen der Dienste „Elektronische Fakturierung“ und „Digitale Geschäftsbücher“ erstellt worden sind, ist auf den Inhaber der Dokumente und/oder seine Bevollmächtigte beschränkt, welche mittels SPID oder CNS auf die jeweiligen Portale zugreifen können.

7.3 Beschreibung des Dienstes

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

7.4 Technische Bestimmungen und Bestimmungen des CNIPA 2004

Die Körperschaft hat es 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

8 Dokumente, die der Aufbewahrung unterzogen werden

Die Dokumente, welche aufbewahrt werden, umfassen alle informatischen 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 Systeme zur Einsichtnahme in Dokumente“ 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 Dokumentenverwaltungsdienste von InfoCamere gewährleisten die Gültigkeit der digital unterzeichneten Dokumente und die Zeitstempelung, deren Gültigkeit vom Aufbewahrungssystem nicht überprüft wird.

Als Eigentümerin des aufzubewahrenden Inhalts bestimmt die Kammer die Beziehung zwischen den Dokumenten, welche eine dokumentarische Einheit bilden, und der jeweiligen Archiveinheit, während InfoCamere K.A.G. in seiner Eigenschaft als Aufbewahrer diese Informationen im Laufe der Zeit unveränderbar, einsehbar und kontextbezogen aufbewahrt, und zwar gemäß den im Handbuch für die Aufbewahrung und in der Vereinbarung festgelegten Parametern.

8.1 Formate

Gemäß den Bestimmungen der Vereinbarung überträgt die Kammer die digitalen Inhalte, welche aufbewahrt werden müssen, in der von InfoCamere K.A.G. festgelegten Art und Weise und Form über das Dokumentenverwaltungssystem GeDoc, über das Handelsregister, das SUAP-Portal und die Dienste "Elektronische Fakturierung" und "Digitale Geschäftsbücher". Die Kammer garantiert die Authentizität und Integrität der Dokumentation in der Produktions- und der laufenden Archivierungsphase, die unter Einhaltung der Richtlinien durchgeführt wird. Sie stellt insbesondere sicher, dass die Übertragung von informatischen Dokumenten in Formaten erfolgt, die mit der Aufbewahrungsfunktion kompatibel sind und den geltenden Rechtsvorschriften entsprechen.

In Absprache mit dem Verwahrer ist die Aufbewahrung von Nicht-Standardformaten vorgesehen, aber eine langfristige Aufbewahrung ist nicht garantiert. Eine Liste dieser Formate ist im Anhang zu diesem Handbuch enthalten.

Die Formattypen, die von der produzierenden Körperschaft angewandt und verwaltet und zur Aufbewahrung übermittelt werden, sind in Anlage 1 „Aufbewahrungsfristen, Inhaltsklassen, Formate und Systeme zur Einsichtnahme in Dokumente“ 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 Kammer 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 Kammer Formate, die nicht auf der Liste aufscheinen, und zwar aus folgenden Gründen:

- technische Auflagen;
- spezifische Formate;
- für das Dokument erforderlichen Dauer der Aufbewahrung.

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

8.2 Inhaltsklasse

Es werden die Modalitäten für die Aufbewahrung der Dokumente genehmigt, die im Aufbewahrungshandbuch von InfoCamere gemäß der archivistischen 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 Systeme zur Einsichtnahme in Dokumente" enthalten.

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

Zurück zum Inhaltsverzeichnis

9 Der Aufbewahrungsprozess

Die Hauptprozesse des Aufbewahrungsdienstes sind:

- Aufbewahrung;
- Aushändigung;
- Produktion von Duplikaten und digitalen Kopien;
- Aussonderungsverfahren.

9.1 Aufbewahrung

Der Aufbewahrungsprozess sieht folgende Phasen vor:

- Erstellung und Übermittlung des Übergabepakets (SIP) seitens der produzierenden Körperschaft;
- Annahme des Übergabepaketes (SIP) durch das Aufbewahrungssystem;
- Indexierung und Generierung des Archivierungspaketes (AIP).

Es folgen die Details der obengenannten Phasen.

9.1.1 Erstellung und Übermittlung des Übergabepakets

Der Verantwortliche für die Dokumentenverwaltung der Handelskammer erstellt das Übergabepaket durch das Dokumentenverwaltungssystem von InfoCamere und übermittelt es an das Aufbewahrungssystem.

Die mit Hilfe des Dienstes „Digitale Geschäftsbücher“ von den Unternehmen erstellten Dokumente werden im Sinne der geltenden Bestimmungen innerhalb des automatisch vom System errechneten Datums an das Aufbewahrungssystem übermittelt und zwar aufgrund:

- des vom Nutzer angegeben Steuerjahres;
- der Kategorie und Art von Geschäftsbuch;
- und eventuell unter Berücksichtigung außerordentlicher Operationen oder Konkursverfahren, die im Laufe des Geschäftsjahres eingetreten sind.

Der Eigentümer kann beantragen, dass die digitalen Geschäftsbücher vor dem vom System berechneten Datum zur Aufbewahrung übermittelt werden. Im letzteren Fall erfolgt die Aufbewahrung innerhalb von zwei Tagen nach dem Antrag, außer bei besonderen technischen Anforderungen.
B2B-Rechnungen, die im Rahmen des Dienstes "Elektronische Fakturierung" erstellt werden, werden innerhalb von 5 Tagen nach Versand/Empfang zur Aufbewahrung übermittelt. PA-Rechnungen werden innerhalb von 15 Tagen nach ihrer Ausstellung zur Aufbewahrung übermittelt.

Die Übergabepakete enthalten eine Archiveinheit oder eine Dokumenteneinheit und entsprechen den Vorgaben des Aufbewahrungshandbuches von InfoCamere. Die Fristen für die Übermittlung der Archiveinheiten und Dokumenteneinheiten an das Aufbewahrungssystem variieren je nach Art des Inhalts und des Systems, aus dem sie übermittelt werden.

System für die Übermittlung	Art des Inhalts	Fristen für die Übermittlung[1]
GEDOC	Dokumenteneinheit	60 Tage nach deren Registrierung
	Archiveinheit	30 Tage nach Schließung des Faszikels
	Tägliches Protokollregister	innerhalb des nächsten Werktages

System für die Übermittlung	Art des Inhalts	Fristen für die Übermittlung[1]
HANDELSREGISTER	Dokumenteneinheit	bei Abschluss der Überprüfung
	Archiveinheit	30 Tage nach Schließung des Faszikels
SUAP	Dokumenteneinheit	nach erfolgter Protokollierung
	Archiveinheit	bei Schließung des Faszikels
DIGITALE GESCHÄFTSBÜCHER	Dokumenteneinheit	innerhalb von zwei Tage nach Anfrage[1]
ELEKTRONISCHE FAKTURIERUNG	Dokumenteneinheit	Rechungen B2B innerhalb von 5 Tagen ab Versand/Erhalt Rechnungen PA innerhalb von 15 Tagen ab Ausstellung

[1] Sonderfälle aufgrund technischer Erfordernisse werden in den angeführten Fristen nicht berücksichtigt.

9.1.2 Annahme des Übergabepaketes (SIP) durch das Aufbewahrungssystem

Das Aufbewahrungssystem führt die Kontrolle über das erhaltene Übergabepaket (SIP) 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 Dokumentenverwaltungssystem von InfoCamere den erhobenen Fehler mit.

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

9.1.3 Indexierung und Generierung des Archivierungspaketes (AIP)

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

9.2 Aushändigung

Die Aushändigung der vom Aufbewahrungssystem aufbewahrten Dokumente erfolgt durch die eigens vorgesehene Webapplikation in Verbindung mit dem Dokumentenverwaltungssystem von InfoCamere. Die Aushändigung eines Dokuments durch diese Funktion ist den Mitarbeitern der Körperschaft gestattet, die im Dokumentenverwaltungssystem zur Verwaltung/Verarbeitung des Dokuments ermächtigt sind.

Wird von einem körperschaftsinternen oder -externen Benutzer, der nicht zur Generierung der Ausgabepakete befugt ist, die normgerechte Aushändigung 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.

9.3 Produktion von digitalen Duplikaten

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

9.4 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.

9.5 Aussonderung der digitalen Inhalte

Der dem Handbuch für die Dokumentenverwaltung beiliegende „Faszikulierungs- und Aussonderungsplan“ der Handelskammer legt die Fristen fest, nach Ablauf derer die verschiedenen Arten von informatischen Dokumenten ausgesondert werden können. Der Verantwortliche für die Aufbewahrung erstellt das Verzeichnis der Archivierungspakete, welche die auszusondernden Dokumente beinhalten und teilt diese nach Überprüfung der Einhaltung der vom Aussonderungskatalog vorgesehenen Zeitrahmen dem Verantwortlichen für die Dokumentenverwaltung mit.

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

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

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

Nach Abschluss der Löschung der ausgesonderten Archivpakete aus dem Aufbewahrungssystem, teilt die Handelskammer den zuständigen Behörden das Ergebnis der Aussonderung mit.

Die Aussonderung tritt erst nach Aktualisierung sämtlicher Sicherheitskopien des Systems in Kraft. Die Dokumente und informatischen Gruppierungen von Dokumenten, welche vom Aufbewahrungssystem ausgesondert werden, werden auch von allen von der Handelskammer genutzten Anwendungen gelöscht.

9.6 Überprüfung der Integrität

Die Handelskammer beauftragt den Verwahrer, die Integrität der Archive regelmäßig zu prüfen. Der Verantwortliche für die Aufbewahrung kann die Ergebnisse der durchgeführten Kontrollen vom Verwahrer anfordern.

9.7 Rücktritt

Sollte die Handelskammer beabsichtigen, von der Vereinbarung für die Erteilung des Dienstes zurückzutreten, muss dies der Verantwortliche für die Aufbewahrung dem Verwahrer mindestens dreißig Tage vorher 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

10 Sicherheit des Aufbewahrungssystems

Dieser Abschnitt gibt einen allgemeinen Überblick über die Richtlinien der Kammer zur IT-Sicherheit und zum Schutz personenbezogener Daten, die eingeführt wurden, um eine angemessene Verwaltung der Sicherheit des Systems zur Aufbewahrung von informatischen Dokumenten zu gewährleisten.
Der Abschnitt gilt als Ergänzung zu den technischen und organisatorischen Sicherheitsmaßnahmen, die im Aufbewahrungshandbuch und im Sicherheitsplan von InfoCamere als beauftragter Verwahrer beschrieben sind und auf die sich die Kammer bezieht.

10.1 Gesetzlicher Bezugsrahmen

Wie im Beschluss der AgID Nr. 407/2020 - Richtlinien für die Erstellung, Verwaltung und Aufbewahrung elektronischer Dokumente vorgesehen, erstellt der Verantwortliche für die Aufbewahrung im Einvernehmen mit dem Sicherheitsverantwortlichen und dem Verantwortlichen für die Digitalisierung der Körperschaft und nach Stellungnahme des Datenschutzverantwortlichen den Teil des allgemeinen Sicherheitsplans, welcher das Aufbewahrungssystems betrifft und sieht geeignete technische und organisatorische Maßnahmen vor, um ein angemessenes Sicherheitsniveau zu gewährleisten, das dem Risiko in Bezug auf den Schutz personenbezogener Daten gemäß Art. 32 der Verordnung (EU) 2016/679 und unter Bezugnahme auf die IKT-Mindestsicherheitsmaßnahmen "Minimum ICT security measures for public administrations" entgegenwirkt.

In diesem Zusammenhang hat die Kammer zur Aufbewahrung von informatischen Dokumenten eine Vereinbarung mit einer externen Partei getroffen, welche die gesetzlich vorgeschriebenen organisatorischen und technischen Garantien bietet (Artikel 44. Voraussetzungen für die Verwaltung und Aufbewahrung informatischer Dokumente im Sinne des G.V.D. Nr. 82 vom 07.03.2005). Die Rolle des Aufbewahrers (also des Verantwortlichen des Aufbewahrungssystems) sowie die entsprechende Aufbewahrung der informatischen Dokumente ist damit an die Informatikgesellschaft der italienischen Handelskammern, InfoCamere K.A.G., übertragen worden.

10.2 Wichtigste Verweise und Verbindungen

Zum Zeitpunkt der Aktualisierung des vorliegenden Dokuments ergeben sich die wichtigsten Verweise im Bereich der IT-Sicherheit auf folgende Dokumente:

- ☐ **Sicherheitsplan des Aufbewahrungssystems**
  Dokument, welches vom Aufbewahrer (entsprechend den AgID-Richtlinien) erstellt und aktualisiert wird und das im Rahmen des allgemeinen Sicherheitsplans die Tätigkeiten zum Schutz des Aufbewahrungssystems der informatischen Dokumente vor möglichen Risiken (Verlust oder unzureichende Vertraulichkeit, Integrität oder Verfügbarkeit) beschreibt und vorsieht bzw. im Laufe der Zeit gewährleistet, dass die Dokumente korrekt aufbewahrt werden und deren Verfügbarkeit, Authentizität, Integrität, Zuverlässigkeit und Lesbarkeit fortbesteht.

- ☐ **Allgemeiner Sicherheitsplan der Kammer**
  Dokument zur Planung der Maßnahmen für die Umsetzung eines Systems zum Schutz aller möglichen Tätigkeiten und Aktionen im Rahmen der gesamten Organisation vor eventuellen Risiken, in Übereinstimmung mit dem AgID-Rundschreiben Nr. 1/2017, das die "Mindestmaßnahmen für die IKT-Sicherheit in öffentlichen Verwaltungen" enthält.

☐ **Sicherheitsplan des informatischen Dokumentenverwaltungssystems**
Von der Kammer erstelltes und aktualisiertes Dokument (in Übereinstimmung mit den AgID-Richtlinien), das als Teil des allgemeinen Sicherheitsplans Aktivitäten beschreibt und plant, die darauf abzielen, verarbeitete und gehostete Daten, Infrastrukturen, Anwendungen und Dienste des informatischen Dokumentenverwaltungssystems vor möglichen Risiken zu schützen, denen sie ausgesetzt sind (Verlust oder Unzulänglichkeit der Vertraulichkeit, Integrität und Verfügbarkeit).

10.3 Sichere Organisation der Aufbewahrung der informatischen Dokumente

Bei der Bereitstellung des Aufbewahrungsdienstes berücksichtigt InfoCamere das OAIS-Modell (Open Archival Information System) oder, wie es die AgID beschreibt, "eine organisierte Struktur von Personen und Systemen, die die Verantwortung für die Aufbewahrung von Informationen und deren Bereitstellung für eine Bezugsgemeinschaft übernimmt".
Nachfolgend eine zusammenfassende Skizze der Rollen und Bereiche, die bei der Bewertung des Sicherheits- und Datenschutzniveaus des digitalen Dienstes berücksichtigt werden.

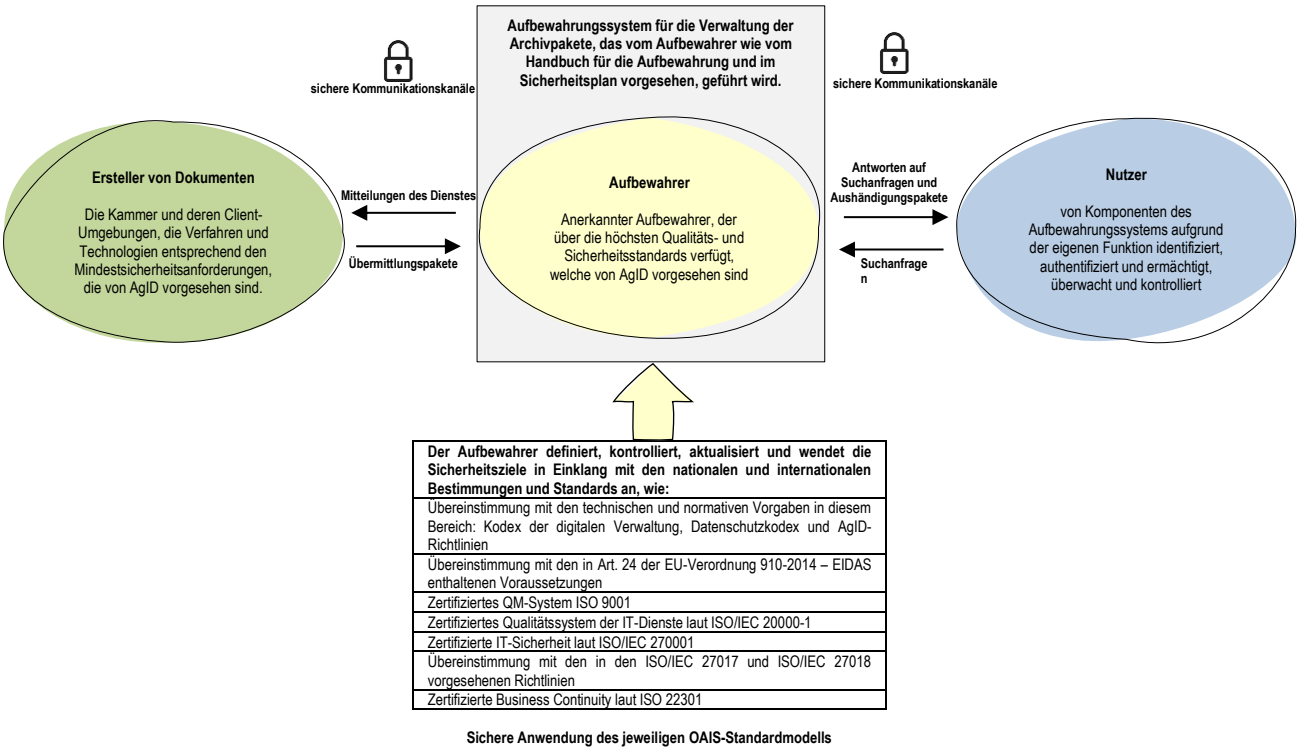

Abbildung 3 - Rollen und Bereiche betreffend das Sicherheitsniveau und den Datenschutz

10.4 Ziele der Sicherheitsmaßnahmen

Die folgenden Angaben dienen als Referenz für die Angemessenheit der getroffenen Sicherheitsmaßnahmen sowie für alle anderen Informationen, die für die Verwaltung und Überprüfung des sicheren Betriebs des vom Aufbewahrer verwalteten Aufbewahrungssystems im Laufe der Zeit nützlich sind:

- Kontext und Zweck des digitalen Aufbewahrungsverfahrens, welches gewährleistet, dass die informatischen Dokumente im Sinne der gesetzlichen Vorgaben aufbewahrt werden und deren Authentizität, Integrität, Zuverlässigkeit, Lesbarkeit und Wiederauffindbarkeit gewährleistet ist;

- Angemessenheit der Kompetenzen des Aufbewahrers in Bezug auf seine erworbenen Zertifizierungen, der Einhaltung des gesetzlichen Bezugsrahmens und der Übersichten und Richtlinien von AgID, welche für ein System vorgeschrieben und notwendig sind, damit es hinsichtlich IT-Sicherheit und Datenschutz als verlässlich und garantiert eingestuft werden kann;
- Angemessenes Sicherheitsniveau der Informationen und des Schutzes personenbezogener Daten, welches mit angemessenen technischen und organisatorischen Maßnahmen gewährleistet werden muss, um folgende Risiken für die übermittelten Daten und Informationen, die von Systemen oder Infrastrukturen aufbewahrt oder bearbeitet werden, zu verringern: Zerstörung, Verlust, Änderung, unrechtmäßige Verbreitung oder Zugriff bzw. Nichtverfügbarkeit, sei es ungewollt oder aus vorsätzlichen Gründen;
- ein geeignetes und formalisiertes Verfahren zur Benachrichtigung der Aufsichtsbehörde und zur Benachrichtigung der betroffenen Person über eine Verletzung des Schutzes personenbezogener Daten;
- Schulung und Sensibilisierung des befugten Personals im Rahmen der IT-Sicherheit und in Bezug auf den Schutz der verarbeiteten personenbezogenen Daten;
- laufende Überwachung der Wirksamkeit und Effizienz der angewandten technischen und organisatorischen Sicherheitsmaßnahmen.

10.5 Kontrolle der Zugriffe auf das Aufbewahrungssystem

Es werden Regeln zum Schutz vor unbefugtem Zugriff aufgestellt, um die Vertraulichkeit zu wahren und eine unbefugte Verarbeitung durch Nutzer, die nicht über die erforderlichen Rechte verfügen, zu verhindern.

InfoCamere achtet auf die Verwaltung von Benutzern und Zugangsprofilen, indem es Referenzrichtlinien und -verfahren definiert; es gewährleistet, dass das System sicher und zuverlässig ist und dass Daten und gehostete Anwendungen geschützt und nur für autorisierte Benutzer zugänglich sind.
Die Kammer hat Kontrollen eingerichtet, um den Zugang zum System wirksam auf Mitarbeiter zu beschränken, die einen legitimen Bedarf haben, gemäß dem Grundsatz, dass der Zugang zu Daten und Systemen mit Hilfe von Computeranwendungen auf das für die Ausführung der erforderlichen Tätigkeiten unbedingt erforderliche Maß beschränkt werden muss.
Identitäten und Zugangsberechtigungen für autorisierte Benutzer werden verwaltet, regelmäßig überprüft und widerrufen. Zugriffsrechte und Berechtigungen werden nach dem Prinzip der minimalen Privilegien und der Trennung von Funktionen verwaltet.

10.6 Wichtigste Sicherheitsmaßnahmen für die Arbeitsplätze und Verhaltensregeln für die Nutzer

Die Verwendung von Arbeitsplätzen, die gemäß den besten Sicherheitspraktiken (z. B. Anti-Malware, Deaktivierung unnötiger Dienste usw.) der installierten und zertifizierten Software konfiguriert sind, ermöglicht zusammen mit der Verwaltung von Berechtigungen für einzelne Benutzer eine wirksame Kontrolle über die unsachgemäße Verwendung von Arbeitsmitteln und das Verbot der Installation gefährlicher Software, die von der Kammer als nicht zuverlässig eingestuft wird.
Die Kammer fordert das befugte Personal auf, die Verantwortung für die korrekte Nutzung der zugewiesenen IT-Ausrüstung zu übernehmen, und weist darauf hin, dass eine unsachgemäße Nutzung im Hinblick auf die zugewiesenen Aufgaben und Arbeitstätigkeiten zu Ineffizienzen und Fehlfunktionen sowie zu einer Gefährdung der Sicherheit und des Schutzes der verarbeiteten Daten beitragen kann.
Unter Bezugnahme auf die in Abschnitt "10.2 Verweise und Verbindungen" aufgeführten Verweise werden im Folgenden einige grundlegende Regeln und Vorsichtsmaßnahmen genannt:

- Bewusstsein für die eigene Rolle und Verantwortung und Beitrag zur korrekten und sicheren Nutzung der zugewiesenen Ressourcen, Meldung aller unbekannten Ereignisse, die Systeme, Anwendungen und verarbeitete Daten gefährden könnten;
- Verpflichtung zu einem Verhalten, das das Risiko eines Angriffs auf das System durch bösartige Software verringert (typische Beispiele für bewusstes Verhalten sind: keine verdächtigen E-Mails oder Anhänge öffnen, nicht auf nicht als vertrauenswürdig anerkannten Websites surfen, keine Zugangsdaten weitergeben usw.);
- Laufende Aktualisierung der Anwendungen und des angewandten Anti-Malware-Systems;
- Begrenzung der Verbindung zu unbekannten/nicht identifizierten Geräten;
- Sichere Konfiguration der Arbeitsplätze (sei es physisch als auch virtuell);
- Auditing-Dienste, die je nach Bedarf auf den Arbeitsstationen aktiviert werden können;
- Keine Authentifizierungscodes weitergeben und die Referenzrichtlinien beachten;
- Keine unkontrollierten persönlichen Daten und Informationen weitergeben, welche die Sicherheit und Vertraulichkeit von Einzelpersonen oder der Kammer gefährden könnten.

10.7 Informationen zum Datenschutz und Einhaltung des GDPR

Die Aufbewahrung von informatischen Dokumenten umfasst die Verarbeitung von Daten unterschiedlicher Art und Sensibilität, einschließlich personenbezogener Daten, d. h. Informationen, die eine natürliche Person direkt oder indirekt identifizieren oder identifizierbar machen und Aufschluss über ihre Eigenschaften, Gewohnheiten, Lebensweise, persönlichen Beziehungen, Gesundheit, wirtschaftliche Lage usw. geben können. Diese Vorgänge erfordern die Einhaltung des rechtlichen Rahmens für den Schutz personenbezogener Daten und die Bewertung potenzieller Bedrohungen (Verletzung der Daten und Kontrollverlust). Dabei ist zu berücksichtigen, dass diese Daten in verschiedene Arten eingeteilt werden können, die je nach ihrer Sensibilität mit unterschiedlichen Vorsichtsmaßnahmen und Regeln verarbeitet werden müssen, wobei die vorherige Bewertung der Auswirkungen der Datenverarbeitung auf die Freiheiten und Rechte der betroffenen Personen durch den für die Verarbeitung Verantwortlichen zu berücksichtigen ist.

InfoCamere hat als Aufbewahrer ein Organisationsmodell für den Schutz personenbezogener Daten erstellt und führt die Verarbeitung der Daten der betroffenen Personen nur auf der Grundlage einer förmlichen Ernennung zum Datenverarbeiter gemäß Art. 28 der Verordnung (EU) 2016/679 durch, indem geeignete technische und organisatorische Maßnahmen ergriffen werden, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten für die gesamte Vertragsdauer zu gewährleisten, und zwar unter Beachtung der rechtlichen Aspekte, des nationalen und europäischen Bezugsrahmens und im Einklang mit den Bestimmungen der Datenschutzbehörde. Die wichtigsten Strategien und Maßnahmen werden im Folgenden beschrieben:

- Der Aufbau des Archivierungssystems besteht aus IT-Ressourcen, die in Datenzentren in Italien untergebracht sind. Es werden physische Sicherheitsmaßnahmen ergriffen, um die Räumlichkeiten, Datenzentren und sensiblen Bereiche vor unbefugtem Zugang und Umweltrisiken zu schützen.
- Definierte Rollen und Zuständigkeiten (intern und extern), einschließlich der Verwaltung der Zuständigkeiten und der Kontrolle aller externen Lieferanten, auf die sich der Aufbewahrer das Recht vorbehält, für die Durchführung von Vorgängen, einzelnen Aktivitäten, Dienstleistungen im Zusammenhang mit Funktionen oder Phasen des Aufbewahrungsprozesses zurückzugreifen und die aufgrund von Wissen, Erfahrung, Kapazität und Zuverlässigkeit geeignete zertifizierte Garantien bieten.
- Ernennung des DPO, welcher der Direktion berichtet und die Aufgaben laut EU-Verordnung 679/2016 ausübt.
- Festlegung eines kontinuierlichen, spezifischen Weiterbildungsplans über Sicherheitsaspekte bei der Verarbeitung personenbezogener Daten.

- Festlegung eines Verfahrens zur Beschreibung der Verarbeitungen, zur Bewertung ihrer Angemessenheit und als Beitrag zum Management der Risiken für die Rechte und Freiheiten natürlicher Personen, die sich aus den Verarbeitungen ergeben.
- Ermittlung und Anwendung geeigneter technischer und organisatorischer Maßnahmen, die in einem angemessenen Verhältnis zur Verarbeitung personenbezogener Daten stehen, und zwar auf systematische Weise und unter Anwendung eines risikobasierten Ansatzes.
- Klare und angemessene Datenschutz- und Cookie-Richtlinien, Einholung und Verwaltung von Einwilligungen, sofern erforderlich, Methoden der Datenweitergabe und -übermittlung, Rechte an geistigem Eigentum.
- Verfahren zur Überwachung und Kontrolle der Einhaltung der in der Unternehmenspolitik festgelegten Sicherheitsmaßnahmen, wobei insbesondere den Aspekten der Zugangsverwaltung und der Datenübertragung unter Verwendung von Mechanismen (Anwendung komplexer Passwortkriterien) und zuverlässigen und sicheren Protokollen für die verwendeten IKT-Ressourcen (Infrastrukturen, Daten, Anwendungen und Dienste) große Aufmerksamkeit gewidmet wird, um sicherzustellen, dass sie geschützt und nur für autorisierte und zertifizierte Benutzer mit Kriterien auf der Grundlage von Rollen und Zugangsbedürfnissen zugänglich sind. Diese werden überwacht und kontrolliert, um Anzeichen von Verstößen zu erkennen und ein rechtzeitiges Eingreifen im Falle anormaler Ereignisse zu ermöglichen.
- Festlegung des Verfahrens und der Politik für die Meldung und Verwaltung von Sicherheitsvorfällen und die Ermittlung von Schwachstellen in Systemen, die personenbezogene Daten verarbeiten.
- Formalisierung des Verfahrens, mit dem Sicherheitsverletzungen gehandhabt und mitgeteilt werden, die die Rechte und Freiheiten von Personen gefährden, wobei die zuständigen Behörden und die für die Datenverarbeitung Verantwortlichen gemäß den in den Referenzvorschriften angegebenen Fristen und Methoden informiert werden.
- Business-Continuity-Plan sowie Festlegung, Bewertung und regelmäßiger Test von Sicherungs- und Wiederherstellungsverfahren.

Weitere Einzelheiten und Bestimmungen stehen in den Unternehmensrichtlinien und -verfahren, den Vorschriften und Normen, an die sich InfoCamere als Aufbewahrer hält, sowie in den von der Kammer angegebenen Verweisen.

Zurück zum Inhaltsverzeichnis