ASSB·BSB
Azienda Servizi Sociali di Bolzano
Betrieb für Sozialdienste Bozen

AZIENDA SERVIZI SOCIALI DI BOLZANO

BETRIEB FÜR SOZIALDIENSTE BOZEN

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

approvato con Decreto del Direttore Generale *pro tempore* n. 171 dd. 05/07/2021

BENUTZUNGSVERORDNUNG FÜR DEN KORREKTEN EINSATZ DER INFORMATIONS- UND KOMMUNIKATIONSMITTEL IM BSB

mit Dekret des Generaldirektors *pro tempore* Nr. 171 vom 05/07/2021 genehmigt

ASSB·BSB
Azienda Servizi Sociali di Bolzano
Betrieb für Sozialdienste Bozen

INDICE

Premesse pg. 5

CAPO I – DISPOSIZIONI GENERALI

Art. 1 pg. 5
Definizioni

Art. 2 pg. 12
Finalitá

Art. 3 pg. 12
Oggetto e ambito di applicazione

Art. 4 pg. 13
Principi generali

Art. 5 pg. 16
Tutela della/del Lavoratrice/Lavoratore

Art. 6 pg. 16
Soggetti, competenze e responsabilità

CAPO II – DISPOSIZIONI SULL'UTILIZZO DELLA STRUMENTAZIONE IN DOTAZIONE

Art. 7 pg. 18
Assegnazione, variazione e revoca delle credenziali di autenticazione

Art. 8 pg. 20
Gestione delle credenziali di autenticazione

Art. 9 pg. 21
Procedura di attivazione del servizio di assistenza remota (c.d. teleassistenza)

Art. 10 pg. 22
Utilizzo della rete e delle risorse logiche

Art. 11 pg. 26

INHALTSVERZEICHNIS

Prämissen Seite 5

ABSCHNITT I - ALLGEMEINE ANORDNUNGEN

Art. 1 Seite 5
Definitionen

Art. 2 Seite 12
Ziele

Art. 3 Seite 12
Betreff und Anwendungsbereich

Art. 4 Seite 13
Allgemeine Grundsätze

Art. 5 Seite 16
Schutz der Arbeitnehmer

Art. 6 Seite 16
Subjekte, Zuständigkeiten und Verantwortungsbereiche

ABSCHNITT II – ANORDNUNGEN ZUR BENUTZUNG DER ZUGETEILTEN ARBEITSMITTEL

Art. 7 Seite 18
Zuweisung, Änderung und Widerrufung von Zugangsberechtigungen

Art. 8 Seite 20
Verwaltung von Zugangsdaten

Art. 9 Seite 21
Vorgehensweise zur Aktivierung des Fernwartungsdienstes (sog. Teleassistenz)

Art. 10 Seite 22
Verwendung von Netzwerk

Art. 11 Seite 26
Zuweisung von Hardware und Software an Mitarbeiter und Regeln für

Assegnazione di Hardware e Software al personale e regole per l'utilizzo

Art. 12 pg. 27
Utilizzo degli strumenti: Postazione di Lavoro (PDL) ed altri strumenti con relativi Software

Art. 13 pg. 31
Utilizzo delle periferiche, delle risorse di rete

Art. 14 pg. 32
Amministrazione digitale e domicilio digitale

CAPO III – AMMINISTRAZIONE DIGITALE E DOMICILIO DIGITALE

Art. 15 pg. 34
Utilizzo della posta elettronica

Art. 16 pg. 39
Assenze e cessazione dal servizio

Art. 17 pg. 41
Disclaimer di posta

Art. 18 pg. 41
Proprietà dei sistemi

Art. 19 pg. 42
Modalità e precauzioni per l'utilizzo della posta elettronica da parte del/la dipendente

CAPO IV – UTILIZZO DELLA RETE *INTERNET*

Art. 20 pg. 44
Ambito di applicazione

Art. 21 pg. 45
Responsabilità

Art. 22 pg. 45

die Nutzung

Art. 12 Seite 27
Benutzung der Geräte: Arbeitsplatz und andere Instrumente mit zugehöriger Software

Art. 13 Seite 31
Verwendung von Peripheriegeräten, Netzwerkressourcen

Art. 14 Seite 32
Digitale Verwaltung und digitales Domizil

ABSCHNITT III – ANORDNUNGEN ZUR BENUTZUNG VON E-MAIL

Art. 15 Seite 34
Benutzung der elektronischen Post

Art. 16 Seite 39
Abwesenheiten und Beendigung des Dienstes

Art. 17 Seite 41
E-Mail Verwaltungsausschluss (Disclaimer)

Art. 18 Seite 41
Eigenschaften der Systeme

Art. 19 Seite 42
Modalitäten und Vorsichtsmaßnahmen für die Benutzung der E-Mails von Seiten der Bediensteten

ABSCHNITT IV – *INTERNET*-NUTZUNG

Art. 20 Seite 44
Anwendungsbereich

Art. 21 Seite 45
Verwaltung

Art. 22 Seite 45

Accesso e utilizzo di Internet

Art. 23 pg. 47
Utilizzo dei telefoni, cellulari, fax, fotocopiatrici, scanner e stampanti

Art. 24 pg. 48
Assistenza agli utenti e manutenzioni

CAPO V – CONTROLLI E GARANZIE

Art. 25 pg. 50
Controlli

Art. 26 pg. 51
Modalità

Art. 27 pg. 52
Informazioni generali in merito ai controlli

Art. 28 pg. 53
Controlli sugli strumenti

Art. 29 pg. 55
Conservazione dei dati

Art. 30 pg. 56
Partecipazione a Social Media

CAPO VI – VIOLAZIONI DEL REGOLAMENTO E DISPOSIZIONI FINALI

Art. 31 pg. 57
Responsabilità

Art. 32 pg. 58
Violazioni

Art. 33 pg. 59
Violazione Privacy e Data Breach

Art. 34 pg. 62

Zugang zum Internet und Benutzung

Art. 23 Seite 47
Nutzung von Telefonen, Handys, Faxgeräten, Kopierern, Scannern und Druckern

Art. 24 Seite 48
Technischer Beistand an die Nutzer und Wartung

ABSCHNITT V – KONTROLLEN UND GARANTIEN

Art. 25 Seite 50
Kontrollen

Art. 26 Seite 51
Modalitäten

Art. 27 Seite 52
Allgemeine Informationen hinsichtlich der Kontrollen

Art. 28 Seite 53
Kontrolle über die Arbeitsmittel

Art. 29 Seite 55
Datenspeicherung

Art. 30 Seite 56
Teilnahme an *social media*

ABSCHNITT VI – MISSACHTUNGEN GEGEN DIE VERORDNUNG UND SCHLUSSBESTIMMUNGENMISSACHTUNGEN GEGEN DIE VERORDNUNG UND SCHLUSSBESTIMMUNGEN

Art. 31 Seite 57
Verwaltung

Art. 32 Seite 58
Missachtungen

Art. 33 Seite 59
Verstöße gegen Privacy und *Data Breach*

Art. 34 Seite 62

Sanzioni disciplinari **Art. 35** **pg. 62**
Revisione periodica **ALLEGATI** **pg. 63**

Disziplinarstrafen **Art. 35** **Seite 62**
Periodische Überprüfung **ANHÄNGE** **Seite 63**

REGOLAMENTO

PREMESSE

L'Azienda Servizi Sociali di Bolzano (di seguito: ASSB) adotta il presente regolamento per l'utilizzo degli strumenti informatici e telematici, definito con il coinvolgimento delle rappresentanze sindacali e nel rispetto delle seguenti norme e disposizioni ed eventuali ss.mm. e ii.:

- Legge 20.05.1970, n.300 (Statuto dei lavoratori);
- Regolamento europeo sulla protezione dei dati 2016/679 (GDPR);
- Decreto Legislativo 30.06.2003, n.196 (Codice in materia di protezione dei dati personali);
- D. Lgs. 10 agosto 2018, n.101;
- Decreto Legislativo 07.03.2005 n.82 (Codice dell'amministrazione digitale);
- D. Lgs. 14.09.2015 n. 151;
- Decreto legge 16.07.2020 n. 76 (decreto semplificazioni) convertito in legge 11.9.2020 n. 120;
- Raccomandazioni dell'Autorità garante per la protezione dei dati personali;
- Linee guida del Garante per posta elettronica e internet pubblicate in Gazzetta Ufficiale n. 58 del 10.03.2007;
- *Circolare AGID n. 2 del 18.04.2017 recante Misure minime di sicurezza ICT per le pubbliche amministrazioni.*

VERORDNUNG

PRÄMISSEN

Der Betrieb für Sozialdienste Bozen (im Folgenden: BSB) erlässt die vorliegende Verordnung für den Einsatz von EDV- und Telematikinstrumenten, die unter Einbeziehung der Gewerkschaftsvertreter und unter Beachtung der nachfolgenden Regeln und Bestimmungen sowie eventueller späterer Änderungen und Ergänzungen festgelegt wurde:

- Gesetz 20.05.1970, Nr. 300 (Arbeiterstatut);
- Europäische Datenschutzverordnung 2016/679 (DSGVO);
- Gesetzesverordnung 30.06.2003, Nr.196 (Gesetz zum Schutz personenbezogener Daten);
- Gesetzesverordnung 10. 08.2018, Nr. 101;
- Gesetzesverordnung 07.03.2005, Nr. 82 (Digitaler Verwaltungscodex);
- Gesetzesverordnung 14.09.2015, Nr. 151;
- Gesetzesdekret 16.07.2020, Nr. 76 (Vereinfachungsdekret) umgewandelt in Gesetz 11.09.2020, Nr. 120;
- Empfehlungen der Garantenbehörde zum Schutz personenbezogener Daten;
- Richtlinien des Garanten für elektronische Post und Internet, veröffentlicht im Amtsblatt Nr. 58 vom 10.03.2007;
- *AGID-Rundschreiben Nr. 2 vom 18.04.2017 über IKT-Mindestsicherheitsmaßnahmen für öffentliche Verwaltungen.*

CAPO I DISPOSIZIONI GENERALI

Art. 1
Definizioni

(in ordine alfabetico)
Ai fini del presente regolamento si intende per:

Account: iscrizione registrata su un *server* e che, tramite l'inserimento di *username* e *password*, consente l'accesso alla rete e o ad altri servizi. Si indicano, a titolo esemplificativo, l'*account* che consente di accedere alle risorse della rete locale, ai *file server*, alle stampanti e al sistema di archiviazione documentale (D3).

Amministratore di Sistema: secondo la definizione dell'Autorità garante per la protezione dei dati personali deducibile nel provvedimento del 27 novembre 2008, successivamente modificato con provvedimento del 25 giugno 2009, è la figura professionale dedicata alla gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di *software* complessi. L'amministratore di sistema fornisce indicazioni su come procedere nel pieno rispetto delle disposizioni vigenti in tema di trattamento, ivi compreso il profilo relativo alla sicurezza.

Antivirus: *software* atto a prevenire, rilevare e rimuovere quando possibile, programmi o file dannosi per il pc e gli altri supporti/strumenti informatici.

Attachment / allegato di posta elettronica: file o documento che viene

ABSCHNITT I *ALLGEMEINE ANORDNUNGEN*

Art. 1
Definitionen

Für die Zwecke dieser Verordnung gilt:

Account: Registrierung auf einem *Server*, der durch Eingabe eines Benutzernamens und eines Passworts den Zugriff auf das Netzwerk und oder andere Dienste ermöglicht. Beispiele sind der *Account*, der den Zugriff auf lokale Netzwerkressourcen, *file server*, Drucker und das Dokumentenspeichersystem (D3) ermöglicht.

Systemadministrator: gemäß der Definition der Datenschutzbehörde für den Schutz personenbezogener Daten, ableitbar aus der Maßnahme vom 27. November 2008, nachträglich geändert durch die Maßnahme vom 25. Juni 2009, ist die professionelle Figur, die sich der Verwaltung und Wartung von Verarbeitungssystemen widmet, mit denen personenbezogene Daten verarbeitet werden, einschließlich Datenbankverwaltungssystemen, Administratoren von Netzwerken und Sicherheitseinrichtungen und Administratoren komplexer *Software*. Der Systemadministrator gibt Hinweise, wie man in voller Übereinstimmung mit den geltenden Bestimmungen hinsichtlich der Verarbeitung, einschließlich des Sicherheitsprofils, vorgehen kann.

Antivirus: *Software,* die Programme oder Dateien, die für den PC und andere Medien/Computermedien-geräte schädlich sind, verhindern, erkennen und, wenn möglich, entfernen soll.

Attachment / Anhang zur E-Mail: Dateien oder Unterlagen die zusammen

inviato assieme a un messaggio di posta elettronica.

Autorizzati al trattamento: tutti/e i/le dipendenti/collaboratori/collaboratrici di ASSB, incaricati/e al trattamento di dati personali, ai sensi dell'art. 29 del Regolamento europeo 2016/679.

Backup: copia di sicurezza di tutti i dati contenuti all'interno dei Server di ASSB.

Browser: *software* che consente la visualizzazione e la navigazione nelle pagine di *internet* e/o *intranet*. Spesso tale sistema deve essere affiancato da plug-in per rendere attive determinate funzionalità quali il sonoro e i filmati. I due *browser* più noti sono *Mozilla Firefox* e *Google Chrome.*

Centro Elaborazione Dati (CED): unità organizzativa dell'Ufficio programmazione, controllo e sistemi informativi di ASSB, composta dagli amministratori di sistema; si occupa della manutenzione e dello sviluppo del sistema informatico (*software* e *hardware*) aziendale.

Chat (webchat): sistema che consente il dialogo (tramite digitazione sulla tastiera) di più utenti contemporaneamente tramite internet/intranet. Le *chat* possono essere pubbliche (ognuno legge i messaggi di tutti e invia i propri a tutti i presenti) o private (ospitate in stanze virtuali).

Client: unità periferica/PC di un sistema organizzato a rete tramite un server, al quale richiede l'accesso a uno o più servizi o alle sue risorse.

Client di posta elettronica: *software* locale installato sul pc che, collegandosi ad un server, consente lo scambio di

mit einer E-Mail verschickt werden.

Berechtigte zur Verarbeitung: alle Mitarbeiter/Mitarbeiterinnen von BSB, die mit der Verarbeitung personenbezogener Daten beauftragt sind, gemäß Artikel 29 der Europäischen Verordnung 2016/679.

Backup: Sicherheitskopie aller Daten im Server von BSB.

Browser: Software, die die Visualisierung und Navigation von *Internet- und/oder Intranetseiten* ermöglicht. Oft muss dieses System durch Plug-Ins ergänzt werden, um bestimmte Funktionen wie Ton und Video zu aktivieren. Die beiden bekanntesten Browser sind *Mozilla Firefox* und *Google Chrome*.

EDV-Dienststelle: Organisationseinheit des Amtes für Planung, Steuerung und Informationssysteme von BSB, die sich aus Systemadministratoren zusammensetzt; sie befasst sich mit der Wartung und Entwicklung des Computersystems des Betriebes (Software und Hardware).

Chat (webchat): System das den Dialog (über Tastatur) mehrerer Nutzer im Internet/Intranet gleichzeitig ermöglicht. Es gibt öffentliche Chats (jeder kann die Nachrichten der anderen lesen und seine eigenen senden) und private Chats (die in virtuellen Zimmern stattfinden).

Client: peripherische-/PC-Einheit eines vernetzten Systems, die über einen Server den Zugriff auf einen oder mehrere seiner Dienste oder Ressourcen anfordert.

Client E-Mail: lokale, auf dem Rechner installierte *Software* die über die Verbindung zu einem Server den

messaggi e di file (allegati) attraverso il servizio di posta elettronica. Es. *Lotus Notes*, *Outlook*, *Thunderbird*.

Austausch von Nachrichten und Dateien (Anhänge) durch E-Mails ermöglicht. Beispiel: *Lotus Notes, Outlook, Thunderbird.*

Credenziali di autenticazione: *username* e *password* assegnate o associate individualmente per l'autenticazione dell'incaricato.

Authentifizierungsdaten: Benutzername und Passwort, die für die Authentifizierung der beauftragten Person individuell vergeben oder zugeordnet werden.

Database: archivio di dati strutturato in modo da razionalizzare la gestione e l'aggiornamento delle informazioni e da permettere lo svolgimento di ricerche complesse.

Datenbank: ein Archiv von Daten, das so strukturiert ist, dass die Verwaltung und Aktualisierung von Informationen rationalisiert wird und komplexe Suchvorgänge möglich sind.

Datore di lavoro: soggetto titolare del rapporto di lavoro con il/la lavoratore/lavoratrice o collaboratore/collaboratrice. Nel caso di ASSB, il datore di lavoro è il/la Direttore/ Direttrice Generale che ha la direzione gestionale dell'Azienda stessa.

Arbeitgeber: das Subjekt, das das Arbeitsverhältnis mit dem Bediensteten oder Mitarbeiter hat. Im Fall von BSB ist der Arbeitgeber der/die Generaldirektor/in, der/die die Leitung des Betriebes selbst innehat.

Delegato al trattamento: ogni dirigente di ASSB preposto/a a un determinato ufficio/struttura/servizio, specificamente nominato/a in tal senso da parte del/la titolare, ai sensi dell'art. 2 *quaterdecies*, comma 1, del D. Lgs. n. 196/2003.

Delegierter für die Datenverarbeitung: jede Führungskraft von BSB, die für ein bestimmtes Büro/eine Struktur/einen bestimmten Dienst zuständig ist und vom Rechtsinhaber der Datenverarbeitung gemäß Art. 2, Abs. 1, des Gesetzesdekrets Nr. 196/2003 eigens zu diesem Zweck ernannt wurde.

Dipendente/Collaboratore/ collaboratrice: tutti/e i/le dipendenti – dirigenti compresi/e, nonché i collaboratori/collaboratrici - anche esterni all'ente - che, a qualsiasi titolo, espletano attività lavorativa in favore di ASSB e presso la struttura organizzativa aziendale.

Bedienstete/Mitarbeiter: alle Bediensteten, einschließlich der Führungskräfte, sowie Mitarbeiter, auch von außerhalb des Betriebes, die aus irgendeinem Grund für BSB und innerhalb der Organisationsstruktur des Betriebes arbeiten.

Direttore del Centro Elaborazione Dati: è il/la Direttore/Direttrice dell'Ufficio programmazione, controllo e sistemi informativi.

Direktor/in des Datenverarbeitungszentrums: ist der/die Direktor/in des Amtes für Planung, Steuerung und Informationssysteme.

Download: operazione di trasferimento di un file (di programma o di dati) da un sito internet /intranet.

E-mail: messaggio in formato elettronico trasmesso, in tempo reale, utilizzando una rete locale o internet.

Firewall: *software* o dispositivo *hardware* che protegge la rete ASSB dalle intrusioni esterne. Controlla il traffico in entrata e in uscita in modo che i file non approvati non siano trasferiti.

Freeware: *software* distribuito gratuitamente, che può tuttavia essere soggetto a *copyright* o a limitazioni.

Hardware: insieme dei componenti di base, di un Personal Computer (CPU, HARD DISK, ecc.)

Incaricato rispetto alla fornitura e gestione degli accessi: dipendente e/o collaboratore/collaboratrice a qualsiasi titolo di ASSB, non appartenente al CED dell'ente nominato/a e specificamente incaricato/a per iscritto, da parte del proprio diretto delegato al trattamento, alla richiesta e gestione degli accessi propri e di altri collaboratori/collaboratrici/ dipendenti dell'ente rispetto a banche dati e/o software autonomamente acquistati e gestiti da parte del/la Dirigente.

Intranet: è un sito ad uso esclusivo dell'azienda accessibile solo ai dipendenti. Permette di visualizzare informazioni e file del proprio e degli altri uffici, leggere news aziendali e accedere alla modulistica interna.

Lan (Local Area Network): rete che collega i computer in una zona

Download: Vorgang des Übertragens einer Datei (Programm oder Daten) von einer Internet-/Intranetseite.

E-mail: Eine Nachricht in elektronischem Format, die in Echtzeit über ein lokales Netzwerk oder das Internet übertragen wird.

Firewall: Software- oder Hardware-Gerät, das das BSB-Netzwerk vor Eingriffen von außen schützt. Es kontrolliert den ein- und ausgehenden Datenverkehr, so dass nicht zugelassene Dateien nicht übertragen werden.

Freeware: kostenlos verteilte Software, die jedoch dem Urheberrecht oder Einschränkungen unterliegen kann.

Hardware: Gesamtheit der Grundkomponenten eines Personal Computers (CPU, HARD DISK, etc.).

Beauftragter für die Bereitstellung und Verwaltung der Zugriffe: Bediensteter und/oder Mitarbeiter in irgendeiner Funktion bei BSB, der nicht zu EDV-Dienststelle des Betriebes gehört, der von seinem direkten Delegierten für die Bearbeitung ernannt und ausdrücklich schriftlich damit beauftragt wurde, seinen eigenen Zugriff und den anderer Angestellter/Mitarbeiter des Betriebes in Bezug auf Datenbanken und/oder Software zu beantragen und zu verwalten, die von der Führungskraft autonom erworben und verwaltet werden.

Intranet: ist eine Webseite zur ausschließlichen Nutzung durch den Betrieb, die nur für Mitarbeiter zugänglich ist. Damit kann man Informationen und Dateien aus dem eigenen und anderen Büros einsehen, Firmennachrichten lesen und auf interne Formulare zugreifen.

Lan (Local Area Network): Netzwerk, das Computer in einem begrenzten

circoscritta, come una casa o un ufficio. Si tratta di un sistema chiuso a cui le reti esterne non hanno accesso a meno che non gli sia permesso.

Bereich miteinander verbindet, z. B. zu Hause oder im Büro. Es handelt sich um ein geschlossenes System, auf das externe Netzwerke nur dann Zugriff haben, wenn sie dazu berechtigt sind.

Mailing list: lista di distribuzione automatica di messaggi di posta elettronica a più persone.

Mailing list: Liste der automatischen Verteilung von E-Mail-Nachrichten an mehrere Personen.

Password: parola chiave per l'accesso di un utente a una rete, a un servizio telematico o a un sito *internet che deve rispettare i requisiti minimi di legge.*

Password: Schlüsselwort für den Zugang eines Nutzers zu einem Netzwerk, einem Telematikdienst oder einer Internetseite, die den gesetzlichen Mindestanforderungen entsprechen müssen.

Postazione di lavoro al videoterminale: insieme delle attrezzature comprendenti: il videoterminale, eventualmente con tastiera o altro sistema d'immissione dati, il *software* per l'interfaccia con la macchina, gli accessori opzionali, le apparecchiature connesse, comprendenti l'unità a dischi, il telefono, la stampante, il supporto per i documenti, la sedia, il piano di lavoro, nonché l'ambiente di lavoro immediatamente circostante.

Arbeitsplatz am Bildschirm: ein Gerätesatz, bestehend aus: dem Bildschirm, eventuell mit einer Tastatur oder einem anderen Eingabesystem, der Software zur Kopplung mit dem Gerät, optionalem Zubehör, zugehöriger Ausrüstung einschließlich des Plattenlaufwerks, des Telefons, des Druckers, des Dokumententrägers, des Stuhls, der Arbeitsfläche und der unmittelbaren Arbeitsumgebung.

Responsabile del Centro Elaborazione Dati: il/la dipendente aziendale, appartenente al Centro Elaborazione Dati, al/alla quale spettano le funzioni di coordinamento dell'attività e del personale di quest'ultimo.

Verantwortlicher der EDV-Dienststelle: der zur EDV-Dienststelle gehörende Mitarbeiter des Betriebes, der für die Koordination der Aktivitäten und des Personals derselben verantwortlich ist.

Responsabile del protocollo informatico: il/la dipendente di ASSB, al/alla quale spettano funzioni di coordinamento del settore dell'archivistica dell'ente e del protocollo informatico.

Verantwortlicher des Netzwerk-Protokolls: der Mitarbeiter von BSB, der für die Koordinierung des Archivierungsbereichs der Einrichtung und des Netzwerk-Protokolls zuständig ist.

Responsabile della transizione al digitale: la figura dirigenziale all'interno della PA che ha, tra le sue principali funzioni, quella di garantire operativamente la trasformazione digitale

Verantwortlicher für den Übergang zur Digitalisierung: die Führungsperson innerhalb der öffentlichen Verwaltung, die unter anderem vor allem die Aufgabe hat, die digitale Transformation der

dell'amministrazione, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di nuovi modelli di relazione trasparenti e aperti con i cittadini.

Verwaltung operativ zu gewährleisten, sie bei der Entwicklung digitaler öffentlicher Dienstleistungen zu koordinieren und neue Modelle für transparente und offene Beziehungen zu den Bürgern einzuführen.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento, ai sensi dell'art. 4 del Regolamento europeo 2016/679.

Verantwortlicher der Datenverarbeitung: die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des Rechtsinhabers der Datenverarbeitung verarbeitet, im Sinne von Artikel 4 der Europäischen Verordnung 2016/679.

Router: dispositivo *hardware* appositamente progettato per collegare tra loro due o più reti telematiche.

Router: ein Hardware-Gerät, eigens konstruiert, um zwei oder mehr Telematiknetze zu verbinden.

Server: computer dedicato allo svolgimento di un servizio preciso, come la gestione di una rete locale, alla gestione delle periferiche di stampa (*print server*), allo scambio e condivisione di dati fra i computer (*file server, database server*), all'invio o inoltro di posta elettronica (*mail server*) o a contenere i file di un sito web (*web server*).

Server: Computer, der einen bestimmten Dienst ausführt, z. B. die Verwaltung eines lokalen Netzwerks, die Verwaltung von Druckperipheriegeräten (*printserver*), den Austausch und die gemeinsame Nutzung von Daten zwischen Computern (*file server, database server*), das Senden oder Weiterleiten von elektronischer Post (*mail server*) oder der Dateien einer Website (*web server*).

Software: l'insieme dei programmi che gestiscono e specializzano il funzionamento di un computer.

Software: die Menge der Programme, die die Funktion eines Computers verwalten und spezialisieren.

Titolare del trattamento: ai sensi dell'art. 4 del Regolamento europeo 2016/679, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali: è l'Azienda Servizi Sociali di Bolzano, rappresentata legalmente dal Direttore Generale *pro tempore*.

Rechtsinhaber der Datenverarbeitung: ist gemäß Art. 4 der Europäischen Verordnung 2016/679 die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet: es handelt sich um den Betrieb für Sozialdienste Bozen, gesetzlich vertreten durch den/die Generaldirektor/in *pro tempore.*

Utente: ogni dipendente e collaboratore/collaboratrice ASSB in possesso di specifiche credenziali/dispositivi di autenticazione. Tale figura viene, inoltre, indicata, ai sensi del Regolamento europeo 2016/679, come *autorizzato/a del trattamento*.

Nutzer: jeder Bedienstete oder Mitarbeiter von BSB im Besitz bestimmter Zugangsdaten/Authentifizierungsgeräte. Diese Person ist zudem gemäß der Europäischen Verordnung 2016/679 *als Berechtigter für die Verarbeitung* angegeben.

Videoterminalista: lavoratore che utilizza un'attrezzatura munita di videoterminale, in modo sistematico o abituale, per venti ore settimanali, dedotte le interruzioni previste dall'art. 175 del D.Lgs. 9 aprile 2008, n. 81.

Videoterminalist/in: ein/e Arbeitnehmer/in, der systematisch oder gewohnheitsmäßig zwanzig Stunden pro Woche, nach Abzug der Unterbrechungen gemäß Artikel 175 des Gesetzesdekrets Nr. 81 vom 9. April 2008, eine mit einem Videoterminal ausgestattete Anlage benutzt.

Virus: file in grado di danneggiare, anche irreversibilmente, i dati e le applicazioni di un qualsiasi strumento informatico. Può avere origine da un messaggio di posta elettronica, da una chiavetta USB o scaricando da *internet* dei file non sicuri.

Virus: Datei, die in der Lage ist, die Daten und Anwendungen eines beliebigen Computerprogramms zu beschädigen, sogar unwiderruflich. Sie kann von einer E-Mail-Nachricht, einem USB-Stick oder durch das Herunterladen von unsicheren Dateien aus dem Internet stammen.

Art. 2
Finalitá

1. Il presente regolamento ha la finalità di codificare le regole di comportamento che dipendenti e collaboratori di ASSB sono tenuti a rispettare, al fine di un corretto utilizzo degli strumenti informatici e telematici loro assegnati o da essi comunque utilizzati, ed assicurare così gli adeguati livelli di sicurezza ed integrità del patrimonio informativo di ASSB, con particolare riguardo alla protezione dei dati personali.

Art. 2
Ziele

1. Zweck dieser Verordnung ist es, die Verhaltensregeln zu kodifizieren, die die Bediensteten und Mitarbeiter von BSB einzuhalten haben, um die ihnen zugewiesenen oder von ihnen benutzten Computer- und Telematikinstrumente in jedem Fall korrekt zu verwenden und so ein angemessenes Sicherheits- und Integritätsniveau der Informationsbestände von BSB zu gewährleisten, insbesondere im Hinblick auf den Schutz personenbezogener Daten.

Art. 3
Oggetto e ambito di applicazione

1. Il presente regolamento disciplina:
a) le modalità di utilizzo degli strumenti informatici e telematici nell'ambito dell'espletamento della prestazione

Art. 3
Betreff und Anwendungsbereich

1. Diese Verordnung regelt:
a) die Verfahren für den Einsatz von Computern und telematischen Hilfsmitteln bei der Ausführung der Arbeit;

lavorativa;
b) le modalità di utilizzo della posta elettronica, di *internet*, della rete aziendale e delle *password* assegnate;
c) le misure tecniche, informatiche, organizzative e logistiche necessarie per:

- garantire un'adeguata protezione riguardo ai dati personali dei/delle lavoratori/lavoratrici e di terzi, oggetto di trattamento;
- assicurare gli adeguati livelli di sicurezza ed integrità del patrimonio informativo di ASSB;

d) le modalità di effettuazione dei controlli e le conseguenze della violazione delle disposizioni di cui al presente regolamento.

b) die Methoden der Nutzung von E-Mail, Internet, Betriebsnetzwerk und zugewiesenen Passwörtern;
c) die erforderlichen technischen, informationstechnischen, organisatorischen und logistischen Maßnahmen, um

- einen angemessenen Schutz in Bezug auf die personenbezogenen Daten der Mitarbeiter und Dritter zu gewährleisten, den Betreff der Verarbeitung sind;
- ein angemessenes Maß an Sicherheit und Integrität der Informationsbestände von BSB zu gewährleisten;

d) wie die Kontrollen durchzuführen sind und welche Folgen ein Verstoß gegen die Bestimmungen dieser Verordnung hat.

2. Il presente regolamento si applica a tutti/e i/le dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti/e i/le collaboratori/collaboratrici di ASSB, a prescindere dal rapporto contrattuale intrattenuto.

2. Diese Verordnung gilt für alle Bediensteten, unabhängig von ihrer Position und/oder Ebene, sowie für alle Mitarbeiter des BSB, unabhängig von ihrem Vertragsverhältnis.

3. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per *utente* deve intendersi ogni dipendente e collaboratore/collaboratrice in possesso di specifiche credenziali di autenticazione.

3. Im Sinne der für die Nutzung von Computer- und Telematik-Ressourcen vorgeschriebenen Bestimmungen ist unter einem *Nutzer* jeder Bedienstete oder Mitarbeiter zu verstehen, der im Besitz bestimmter Zugangsdaten ist.

Art. 4
Principi generali

1. L'utilizzo degli strumenti informatici e telematici in ASSB deve sempre ispirarsi ai principi di massima diligenza, buona fede e correttezza, nonché ai principi dettati dalla normativa vigente in materia di protezione dei dati personali.

2. La rete informatica di ASSB è costituita dall'insieme delle risorse informatiche,

Art. 4
Allgemeine Grundsätze

1. Der Einsatz von EDV- und Telematik-Instrumenten in BSB muss stets von den Grundsätzen der äußersten Sorgfalt, des guten Glaubens und der Korrektheit sowie von den Grundsätzen der geltenden Vorschriften zum Schutz personenbezogener Daten geleitet sein.

2. Das Informationsnetzwerk von BSB besteht aus der Menge der

hardware, software, infrastrutture, banche dati e documenti digitali.

Informationsressourcen, Hardware, Software, Infrastruktur, Datenbanken und digitalen Dokumenten.

3. ASSB utilizza in maniera prevalente gestionali centralizzati e privilegia l'utilizzo di risorse informatiche condivise. La strumentazione messa a disposizione del/la dipendente è configurata per garantire l'accesso alle risorse assegnate al suo profilo.

3. BSB verwendet hauptsächlich zentralisierte Führungssysteme und bevorzugt die Verwendung von gemeinsam genutzten Informationsressourcen. Die dem Mitarbeiter zur Verfügung gestellten Arbeitsmittel sind so konfiguriert, dass der Zugriff auf die seinem Profil zugeordneten Ressourcen gewährleistet ist.

4. ASSB mette a disposizione del personale le apparecchiature informatiche, i programmi e, in generale, la strumentazione per usufruire dei servizi di rete, dei servizi *internet* e per la posta elettronica: il relativo utilizzo deve avvenire unicamente per lo svolgimento dell'attività lavorativa e nel pieno rispetto delle norme del presente regolamento.

4. BSB stellt den Bediensteten die Computerausrüstung, die Programme und im Allgemeinen die Instrumente zur Nutzung der Netzwerkdienste, der Internetdienste und der elektronischen Post zur Verfügung: die entsprechende Nutzung darf ausschließlich zur Ausübung der Arbeitstätigkeit und in voller Übereinstimmung mit den Regeln dieser Verordnung erfolgen.

5. ASSB è titolare di tutte le risorse informatiche fornite al proprio personale e ai propri collaboratori/collaboratrici, fatti salvi i PC e i dispositivi personali, compresi i telefoni cellulari, messi a disposizione dai dipendenti per l'espletamento dell'attività in smart working. Il collegamento avviene in questo caso tramite VPN (Sophos o rete VPN nel caso del Consorzio dei Comuni) del PC privato alla rete aziendale. L'acquisizione e il conseguente utilizzo di dispositivi informatici e *software sono* consentiti solo previa espressa autorizzazione del responsabile del CED.

5. BSB ist Eigentümer aller Informatikressourcen, die seinen Bediensteten und Mitarbeitern zur Verfügung gestellt werden, mit Ausnahme von PCs und persönlichen Geräten, einschließlich Mobiltelefonen, die von den Mitarbeitern zur Durchführung von Smart-Working-Aktivitäten zur Verfügung gestellt werden. In diesem Fall erfolgt die Verbindung über VPN (Sophos bzw. VPN-Netz im Falle des Südtiroler Gemeindeverbandes) des privaten PCs zum Firmennetzwerk. Der Erwerb und die anschließende Nutzung von Informatikgeräten und Software ist nur mit ausdrücklicher Genehmigung des Verantwortlichen der EDV-Dienststelle gestattet.

6. Le/I Dirigenti dei servizi, con la collaborazione del responsabile del CED, valutano la dotazione informatica -

6. Die Führungskräfte der Dienste bewerten in Zusammenarbeit mit dem Verantwortlichen der EDV-Dienststelle die

hardware e *software* - del personale, e ne verificano periodicamente la necessità di utilizzo in relazione alle funzioni svolte. Sulla base del fabbisogno rilevato, il CED comunica annualmente la stima economica degli investimenti necessari e pianifica gli interventi di manutenzione ordinaria e straordinaria per garantire:

- un adeguato livello tecnologico e il rispetto dei requisiti di compatibilità alla rete informatica
- l'adozione di misure minime e preventive in conformità alla normativa in materia di *privacy*.

Computerausstattung - *Hardware und Software* - der Mitarbeiter und überprüfen regelmäßig die Notwendigkeit ihrer Nutzung in Bezug auf die ausgeführten Funktionen. Auf der Grundlage des ermittelten Bedarfs übermittelt die EDV-Dienststelle jährlich die wirtschaftliche Schätzung der erforderlichen Investitionen und plant die ordentlichen und außerordentlichen Instandhaltungsmaßnahmen, um Folgendes zu gewährleisten:

- ein angemessenes technologisches Niveau und die Einhaltung der Anforderungen an die Kompatibilität von Computernetzwerken;
- die Verabschiedung von Mindest- und Präventivmaßnahmen in Übereinstimmung mit den Datenschutzbestimmungen.

7. ASSB si conforma alle direttive impartite dalle *Linee guida del Garante per posta elettronica e internet* in Gazzetta Ufficiale n. 58 del 10 marzo 2007 per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete *internet*.

7. BSB hält sich an die Vorgaben der *"Richtlinien des Garanten für elektronische Post und Internet"* im Amtsblatt Nr. 58 vom 10. März 2007, um die korrekte Nutzung der elektronischen Post und des Internets im Arbeitsverhältnis zu überprüfen.

8. Ogni infrazione alle regole previste da tale regolamento per un uso corretto del sistema informatico costituirà una violazione della circolare AGID 2/2017 sopra citata ed espone l'utente alle conseguenze previste dal presente regolamento.

8. Jeder Verstoß gegen die in dieser Verordnung festgelegten Regeln zur ordnungsgemäßen Nutzung des Computersystems stellt einen Verstoß gegen das oben genannte AGID-Rundschreiben Nr. 2/2017 dar und setzt den Nutzer den in dieser Verordnung vorgesehenen Konsequenzen aus.

9. Tutti i soggetti interessati dalle disposizioni del presente regolamento sono tenuti a contattare il/la Dirigente dell'Ufficio/Servizio di cui fanno parte prima di intraprendere qualsiasi attività non esplicitamente compresa nelle disposizioni che seguono, al fine di garantire che le stesse non siano in contrasto con gli standard di sicurezza informatica stabiliti da ASSB. Il/la

9. Alle Personen, die von den Bestimmungen dieser Verordnung betroffen sind, sind verpflichtet, sich mit der Führungskraft des Amtes/der Dienststelle, dem/der sie angehören, in Verbindung zu setzen, bevor sie eine Tätigkeit ausüben, die nicht ausdrücklich in den folgenden Bestimmungen enthalten ist, um sicherzustellen, dass diese nicht im Widerspruch zu den von

Dirigente competente riporterà poi tali richieste direttamente al/la Dirigente del CED di ASSB, in modo che venga valutata la corrispondenza a tali standard.

BSB festgelegten Informationssicherheitsstandards steht. Die zuständige Führungskraft meldet solche Anfragen dann direkt an den Verantwortlichen der EDV-Dienststelle von BSB, damit die Übereinstimmung dieser Standards beurteilt werden kann.

Art. 5
Tutela della/del Lavoratrice/Lavoratore

1. In base all'art. 4, comma 1, della Legge n. 300/1970, la disciplina della materia indicata nel presente regolamento, è finalizzata all'utilizzo, da parte di ASSB, dei sistemi informativi per fare fronte a esigenze produttive, organizzative e di sicurezza nel trattamento dei dati personali, e non all'esercizio di un controllo a distanza dei lavoratori da parte di ASSB.

2. È garantito al/la singolo/a lavoratore/lavoratrice il controllo sui propri dati personali secondo quanto previsto dagli articoli 15, 16, 17, 18, 20, 21 e 77 del Regolamento europeo 2016/679.

Art. 6
Soggetti, competenze e responsabilità

1. Tutti i/le dirigenti aziendali, nella propria qualità di delegati/e al trattamento, nominati/e ai sensi dell'art. 2 *quaterdecies* del D.Lgs. n.196/2003 ss.mm.ii, sono tenuti/e a:

a) informare il personale in merito all'uso consentito delle risorse del sistema informativo dell'ente, specificando dove il presente regolamento possa essere rinvenuto sul sito *internet* aziendale ovvero sulla rete *intranet;*

b) assicurarsi che il personale assegnato si uniformi alle regole e

Art. 5
Schutz der Arbeitnehmer

1. Auf der Grundlage von Art. 4, Abs. 1, des Gesetzes Nr. 300/1970 zielt die in dieser Verordnung angegebene Disziplin auf die Nutzung von Informationssystemen durch BSB zur Erfüllung von Produktions-, Organisations- und Sicherheitsanforderungen bei der Verarbeitung personenbezogener Daten ab und nicht auf die Ausübung einer Fernkontrollen von Arbeitnehmern durch BSB.

2. Die Kontrolle über ihre personenbezogenen Daten wird den einzelnen Mitarbeitern gemäß den Artikeln 15, 16, 17, 18, 20, 21 und 77 der Europäischen Verordnung 2016/679 garantiert.

Art. 6
Subjekte, Zuständigkeiten und Verwaltungsbereiche

1. Alle Führungskräfte des Betriebes, in ihrer Eigenschaft als Delegierte für die Datenverarbeitung, die gemäß Art. 2-*quaterdecies* der Gesetzesverordnung Nr. 196/2003 i.g. F. Änderungen und Ergänzungen) ernannt wurden, sind verpflichtet:

a) das Personal über die zulässige Nutzung der Ressourcen des Informationssystems zu informieren, wobei anzugeben ist, wo diese Regelungen auf der Website oder im Intranet des Unternehmens zu finden sind;

b) dafür zu sorgen, dass das ihm

alle procedure descritte nel presente regolamento, e riportare in sede di relazione annuale alla Direzione Generale, le infrazioni eventualmente commesse dalla propria Unità Organizzativa di responsabilità nonché i provvedimenti conseguentemente assunti;

c) valutare la necessità di dotare o meno il personale di strumenti informatici, determinarne il profilo per l'accesso al sistema informativo e comunicare le eventuali successive variazioni al responsabile del CED;

d) raccogliere e valutare le richieste di accesso ai sistemi e alle banche dati;

e) vigilare sul personale incaricato ai fini dell'assegnazione e gestione degli accessi, propri e di altri collaboratori/collaboratrici/dipendenti di ASSB, a banche dati e/o a software autonomamente, e in via del tutto eccezionale, acquistati e gestiti da parte del/la Dirigente stesso/a.

2. Il personale appartenente al CED, nel suo ruolo di amministratore di sistema, nell'ambito delle risorse informatiche amministrate e nei limiti dei poteri conferiti dal/la titolare ASSB in sede di nomina, ha il compito di:

a) monitorare i sistemi per individuare un eventuale uso scorretto degli stessi dati, nel rispetto della normativa *privacy* e dello Statuto dei Lavoratori, secondo le previsioni del presente regolamento;

b) segnalare prontamente alla Direzione dell'Ufficio programmazione, controllo e sistemi informativi di ASSB e al direttore del servizio competente ogni eventuale attività non

zugewiesene Personal die in dieser Verordnung beschriebenen Regeln und Verfahren einhält, und der Generaldirektion im Jahresbericht über Verstöße seiner zuständigen Organisationseinheit sowie über die daraufhin ergriffenen Maßnahmen zu berichten;

c) die Notwendigkeit, das Personal mit Informatiksystemen auszustatten oder nicht, zu beurteilen, das Profil für den Zugang zum Informationssystem festzulegen und alle nachfolgenden Änderungen an den Verantwortlichen der EDV-Dienststelle mitzuteilen;

d) Anfragen für den Zugriff auf Systeme und Datenbanken zu sammeln und zu beurteilen;

e) das beauftragte Personal, das für die Zuweisung und Verwaltung der eigenen und anderer BSB-Mitarbeiter/Zugänge zu Datenbanken und/oder unabhängiger Software zuständig ist, zu beobachten, die in Ausnahmefällen auch von der Führungskraft selbst erworben und und verwaltet wurde.

2. Das zur EDV-Dienststelle gehörende Personal hat in seiner Rolle als Systemadministrator im Rahmen der verwalteten Informatikressourcen und im Rahmen der vom BSB-Inhaber zum Zeitpunkt der Ernennung übertragenen Befugnisse die Aufgabe:

a) die Systeme zu überwachen, um jeden Missbrauch derselben Daten unter Einhaltung der Datenschutzbestimmungen und des Arbeitnehmerstatuts festzustellen;

b) der Direktion des Amtes für Planung, Steuerung und Informationssysteme von BSB und dem Direktor der zuständigen Dienststelle jede unbefugte Tätigkeit an den Systemen unverzüglich zu melden.

autorizzata sui sistemi.

3. Il personale incaricato ai fini dell'assegnazione e gestione degli accessi alle banche dati ha il compito di:

a) attivare gli accessi su richiesta del Direttore dell'Ufficio nell'ambito del quale verrà inserito il/la nuovo/a utente;
b) segnalare prontamente al Direttore dell'Ufficio nell'ambito del quale verrà inserito il/la nuovo/a utente e al/la proprio/a Dirigente eventuali richieste non corrette;
c) provvedere che il Direttore dell'Ufficio verifichi almeno annualmente, la correttezza delle attivazioni;
d) monitorare gli accessi attivi e il loro utilizzo e segnalare l'eventuale non utilizzo di un accesso per più di sei mesi al Direttore dell'Ufficio di competenza dell'utente e al/la proprio/a Dirigente.

4. Ciascun dipendente aziendale e collaboratore/collaboratrice a qualsiasi titolo è personalmente e direttamente responsabile per ciò che concerne:
a) il rispetto delle regole di cui al presente regolamento;
b) ogni uso delle attrezzature informatiche e delle credenziali (*account, password*, *user Id*) assegnate, fatto salvo l'eventuale uso improprio delle stesse derivante da fatto a lui/lei non imputabile.

CAPO II – DISPOSIZIONI SULL'UTILIZZO DELLA STRUMENTAZIONE IN DOTAZIONE

Art. 7
Assegnazione, variazione e revoca delle credenziali di autenticazione

3. Das Personal, das für die Zuweisung und Verwaltung des Zugriffs auf die Datenbanken beauftragt ist, hat die Aufgabe:

a) die Zugänge auf Anfrage des Direktor des Amtes, in das der neue Nutzer eingefügt wird, zu aktivieren;
b) den Direktor des Amtes, in das der neue Nutzer eingesetzt wird, und seinen eigenen Direktor unverzüglich über fehlerhafte Anträge zu informieren;
c) sicherzustellen, dass der Direktor des Amtes mindestens einmal jährlich die Richtigkeit der Aktivierungen überprüft;
d) die aktiven Zugänge und deren Nutzung zu überwachen und jede Nichtnutzung eines Zugangs für mehr als sechs Monate dem Direktor des Amtes, für das der Nutzer verantwortlich ist, und seinem Vorgesetzten zu melden.

4. Jeder/Jede Mitarbeiter/in des Betriebes und jeder/jede Mitarbeiter/in in welcher Funktion auch immer ist persönlich und direkt verantwortlich für:
a) die Einhaltung der in dieser Verordnung festgelegten Regeln;
b) jede Nutzung der Computerausrüstung und der zugewiesenen Zugangsdaten (*account, password*, *user Id*), unbeschadet einer missbräuchlichen Nutzung derselben, die auf ein ihm nicht zurechenbares Ereignis zurückzuführen ist.

ABSCHNITT II – ANORDNUNGEN ZUR BENUTZUNG DER ZUGETEILTEN ARBEITSMITTEL

Art. 7
Zuweisung, Änderung und

Widerrufung von Zugangsberechtigungen

1. L'accesso alla rete informatica aziendale, alle unità di rete e alle banche dati informatizzate, è consentito ai/alle dipendenti, ed eventuali collaboratori/collaboratrici esterni/e, autorizzati/e al trattamento, previa assegnazione di un profilo di accesso e sua attivazione.

1. Der Zugang zum Betriebscomputernetz, zu den Netzeinheiten und zu den computergestützten Datenbanken ist den Mitarbeitern und eventuellen externen Mitarbeitern, die zur Behandlung berechtigt sind, nach der Zuweisung eines Zugangsprofils und dessen Aktivierung gestattet.

2. Nel rispetto della procedura in materia di accessi informatici, è responsabilità del/la Direttore/trice dell'Ufficio nell'ambito del quale verrà inserito il/la nuovo/a utente, provvedere tempestivamente alla presentazione di richiesta scritta al CED, nei seguenti casi:

a) assunzione di un/a dipendente che necessita di un accesso alla rete dati aziendale, a specifiche banche dati e a unità di rete;
b) variazione del profilo d'accesso alla rete dati a causa di cambio di mansioni all'interno dello stesso ufficio/servizio;
c) disattivazione del profilo del/la dipendente a seguito di trasferimento ad altro servizio aziendale;
d) attivazione del profilo del/la dipendente presso il proprio ufficio/ servizio a seguito di trasferimento da altro servizio aziendale;
e) cessazione temporanea o definitiva del rapporto lavorativo in essere di un/a dipendente in possesso di un accesso alla rete dati aziendale;
f) disattivazione delle credenziali del/ la dipendente a seguito della perdita del requisito di necessità di utilizzo della rete informatica aziendale.

2. In Übereinstimmung mit dem Verfahren für den Computerzugang ist es die Aufgabe des Direktor des Amtes, in dem der neue Nutzer eingestellt wird, in den folgenden Fällen unverzüglich für die Einreichung eines schriftlichen Antrags an die EDV-Dienststelle zu sorgen:

a) Einstellung eines Mitarbeiters, der Zugriff auf das betriebliche Netzwerk, bestimmte Datenbanken und Netzwerkeinheiten benötigt;
b) Änderung des Zugangsprofils aufgrund eines Aufgabenwechsels innerhalb desselben Büros/Dienstes;
c) Deaktivierung des Profils des Mitarbeiters nach einem Versetzung in eine andere Betriebsabteilung;
d) Aktivierung des Profils des Mitarbeiters in seinem eigenen Büro/Dienst nach einer Versetzung aus einer anderen Betriebsabteilung;
e) vorübergehende oder dauerhafte Beendigung des bestehenden Arbeitsverhältnisses eines Mitarbeiters, der Zugang zum Datennetz des Betriebes hat;
f) Deaktivierung der Zugangsdaten des Mitarbeiters, wenn die Notwendigkeit der Nutzung von betrieblichen Netzwerken nicht mehr gegeben ist.

3. La richiesta di attivazione/disattivazione delle

3. Der Antrag auf Aktivierung/Deaktivierung von

credenziali dovrà essere completa delle generalità dell'utente, dell'elenco delle risorse informatiche per le quali deve essere abilitato/disabilitato l'accesso, e della data effettiva a partire dalla quale le credenziali dovranno essere abilitate/disabilitate.

Zugangsdaten muss vollständig sein und die Benutzerdetails, die Liste der Informatikressourcen, für die der Zugriff aktiviert/deaktiviert werden muss, und das Datum, ab dem die Berechtigungsnachweise aktiviert/deaktiviert werden müssen, enthalten.

4. La richiesta di assegnazione di credenziali di autenticazione a collaboratori/collaboratrici esterni/e, deve essere inoltrata al CED direttamente dalla Direzione Generale di ASSB o dal/la Direttore/trice dell'Ufficio presso il quale il collaboratore/la collaboratrice è collocato/a nell'espletamento del proprio incarico.

4. Der Antrag auf Zuteilung von Zugangsdaten für externe Mitarbeiter muss direkt von der Generaldirektion von BSB oder vom Direktor des Büros, in dem der Mitarbeiter tätig ist, an die EDV-Dienststelle weitergeleitet werden.

5. Le credenziali di autenticazione per l'accesso alle risorse informatiche, nonché le istruzioni iniziali per la corretta autenticazione e le istruzioni per la modifica immediata delle *password* assegnate al primo *login*, vengono comunicate al personale da parte del CED.

5. Zugangsdatendaten für den Zugriff auf Informatikressourcen sowie erste Anweisungen für einen ordnungsgemäßen Zugang und Anweisungen zum sofortigen Ändern von Passwörtern, die bei der ersten Anmeldung vergeben werden, werden den Mitarbeitern von der EDV-Dienststelle mitgeteilt.

6. Eccezionalmente, il compito di gestire e controllare l'assegnazione e la modifica degli accessi può essere attribuito per iscritto anche ad altri/e dipendenti, in considerazione della loro professionalità, diligenza e capacità, ad opera del/la Dirigente responsabile.

6. Ausnahmsweise kann die Aufgabe der Verwaltung und Kontrolle der Zugangsvergabe und -änderung auch anderen Mitarbeitern unter Berücksichtigung ihrer Fachlichkeit, Sorgfalt und Fähigkeit von der verantwortlichen Führungskraft schriftlich übertragen werden.

7. I/le dipendenti incaricati/e di attivare profili di accesso sono responsabili delle modalità tecniche di esecuzione e dell'archiviazione della relativa documentazione.

7. Die mit der Aktivierung von Zugangsprofilen beauftragten Mitarbeiter sind für die technischen Modalitäten und Archivierung der entsprechenden Dokumentation verantwortlich.

Art. 8
Gestione delle credenziali di autenticazione

1. Le credenziali di autenticazione sono costituite da un codice nominativo per

Art. 8
Verwaltung von Zugangsdaten

1. Die Zugangsdaten bestehen aus einem Nominativcode zur Identifikation

l'identificazione dell'utente, altresì nominato *username*, nome utente o *user id*, generalmente coerente con il modello *nome.cognome,* e una password di attivazione, personalizzata dall'utente al suo primo accesso.

2. La *password* deve essere:
- di adeguata robustezza;
- composta da almeno 8 caratteri;
- formata da lettere maiuscole e minuscole e/o numeri;
- non può essere ripetibile nel tempo.

3. La *password* non deve contenere riferimenti agevolmente riconducibili all'utente, quali username, nomi o date relative alla persona o a un familiare.

4. La *password* è personale e riservata, deve essere conservata e custodita dall'utente con la massima diligenza e non divulgata a terzi.

5. L'utente deve procedere alla modifica della *password* almeno ogni tre mesi. Un avviso automatico inviato all'indirizzo di posta elettronica dell'utente ricorda la scadenza.

Art. 9
Procedura di attivazione del servizio di assistenza remota (c.d. teleassistenza)

1. L'attivazione dal proprio pc di un servizio di assistenza remota (teleassistenza) a soggetti esterni all'Azienda può avvenire, attivando esclusivamente il *software* standard aziendale, previa richiesta di autorizzazione al/la Responsabile CED, e solo se il soggetto è stato

der Nutzer, auch *username*, User-Name oder u*ser id* genannt, der im Allgemeinen mit dem Modell Vorname.Nachname übereinstimmt, und einem Aktivierungspasswort, das vom Nutzer bei seinem ersten Zugriff personalisiert wird.

2. Das Passwort muss:
- von ausreichender Festigkeit sein;
- aus mindestens 8 Zeichen bestehen;
- aus Groß- und Kleinbuchstaben und/oder Zahlen bestehen;
- kann im Laufe der Zeit nicht wiederholt werden.

3. Das Passwort darf keine Hinweise enthalten, die leicht auf den Nutzer zurückgeführt werden können, wie z. B. Nutzername, Namen oder Daten, die sich auf die Person oder ein Familienmitglied beziehen.

4. Das Passwort ist persönlich und vertraulich, es ist vom Nutzer mit größter Sorgfalt aufzubewahren und zu hüten und nicht an Dritte weiterzugeben.

5. Der Nutzer muss sein Passwort mindestens alle drei Monate ändern. Eine automatische Benachrichtigung, die an die E-Mail-Adresse des Nutzers gesendet wird, erinnert den Nutzer an das Verfallsdatum.

Art. 9
Vorgehensweise zur Aktivierung des Fernwartungsdienstes (sog. Teleassistenz)

1. Die Aktivierung eines Fernwartungsdienstes (Tele-Assistenz) vom eigenen PC aus für Personen außerhalb des Betriebes kann erfolgen, indem nur die Standardsoftware des Betriebes aktiviert wird, und zwar auf Anfrage der Autorisierung an den Verantwortlichen der EDV-Dienststelle

preventivamente nominato Responsabile esterno.

2. Prima dell'attivazione del collegamento del soggetto esterno, il/la dipendente è tenuto/a a chiudere tutti i programmi attivi e file non attinenti all'applicazione per la quale è stata richiesta l'assistenza. Durante il collegamento, il/la dipendente non può abbandonare il posto di lavoro e deve verificare attentamente le operazioni che il soggetto esterno sta compiendo. Nel caso rilevi comportamenti scorretti o abusi, il/la dipendente è tenuto/a a chiudere immediatamente la connessione.

Art. 10
Utilizzo della rete e delle risorse logiche

1. Per l'accesso alle risorse informatiche di ASSB attraverso la rete locale o *internet* (es. per applicativi gestionali *software*), ciascun utente deve essere in possesso di credenziali di autenticazione (vedi art. 8). È tassativamente proibito accedere alla rete e ai sistemi informativi, utilizzando credenziali di altri utenti.

2. L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i documenti informatici (file) di lavoro, o per vari criteri oppure per obiettivi specifici di lavoro.

3. Tutte le cartelle di rete - condivise o personali - possono ospitare esclusivamente contenuti professionali. É vietato il salvataggio nelle condivisioni di rete di ASSB, ovvero negli strumenti in generale, di documenti non inerenti all'attività lavorativa, quali, a titolo

und nur dann, wenn die Person zuvor als externer Verantwortlicher ernannt worden ist.

2. Vor dem Aktivieren der Verbindung der externen Person muss der/die Mitarbeiter/in alle aktiven Programme und Dateien schließen, die nicht mit der Anwendung zusammenhängen, für die Hilfe angefordert wurde. Während der Verbindung darf der/die Mitarbeiter/in den Arbeitsplatz nicht verlassen und muss die Arbeiten, die die externe Person durchführt, sorgfältig kontrollieren. Bei unkorrektem Verhalten oder Missbrauch muss der/die Mitarbeiter/in die Verbindung sofort beenden.

Art. 10

Verwendung von Netzwerk

1. Für den Zugriff auf die Informatikressourcen von BSB über das lokale Netzwerk oder das Internet (z. B. für Anwendungen der Verwaltungssoftware) muss jeder Nutzer im Besitz von Zugangsdaten sein (siehe Art. 8). Es ist strengstens untersagt, mit den Zugangsdaten anderer Nutzer auf das Netzwerk und die Informationssysteme zuzugreifen.

2. Der Zugriff auf das Netzwerk garantiert dem Nutzer die gemeinsame Nutzung des Netzwerkes (Ordnern auf Servern), in die arbeitsbezogene Informatikdokumente (Dateien) entweder nach verschiedenen Kriterien oder nach bestimmten Arbeitszielen eingefügt und gespeichert werden sollen.

3. Alle Netzwerkordner - freigegeben oder persönlich - können nur arbeitstechnische Inhalte enthalten. Es ist verboten, in den BSB-Netzwerkfreigaben oder in den Arbeitsgeräten im Allgemeinen, Dokumente zu speichern, die nicht zu den Arbeitsaktivitäten gehören, wie z. B.:

esemplificativo: documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro.

Dokumente, Fotos, Videos, Musik, persönliche Dateien, Textnachrichten, persönliche E-Mails, Filme und alles andere.

4. Ogni materiale personale rilevato dal personale del CED, a seguito di interventi di analisi della sicurezza informatica ovvero di manutenzione/aggiornamento, verrà rimosso secondo quanto stabilito all'art. 29 *Controlli sugli strumenti* del presente regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

4. Jegliches personenbezogene Material, das von Mitarbeitern der EDV-Dienststelle nach einer Computersicherheitsanalyse oder nach Wartungs- bzw. Aktualisierungseingriffen entdeckt wird, wird gemäß den Bestimmungen des Art. 28 *"Kontrolle über die Arbeitsmittel"* der vorliegenden Verordnung entfernt, unbeschadet jeglicher weiteren zivil-, straf- und disziplinarrechtlichen Verantwortung.

5. Tutte le risorse di memorizzazione locali del Personal Computer in dotazione, non sono sottoposte ad attività di controllo regolare e non sono oggetto di *backup* periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali delle postazioni di lavoro (di seguito: pdl), la cartella *Documenti* o *Desktop* dell'utente. Gli eventuali dispositivi di memorizzazione locali di disponibilità personale come *hard disk* portatili o chiavette USB **NON** devono essere utilizzati nei PC aziendali.

5. Alle lokalen Speicherressourcen des zur Verfügung gestellten PCs unterliegen keiner regelmäßigen Überprüfung und werden nicht regelmäßig gesichert. Beispiele sind unter anderem: die Festplatte C oder andere lokale Festplatten der Arbeitsplätze, der Ordner *"Dokumente"* oder *"Desktop"* des Nutzers. Lokale Speichermedien, die für den persönlichen Gebrauch zur Verfügung stehen, wie z. B. tragbare Festplatten oder USB-Sticks, dürfen **NICHT** auf Betriebs-PCs verwendet werden.

6. Tutte le aree di memorizzazione, sopra menzionate nel comma precedente, non devono ospitare dati di interesse di ASSB; poiché non sono garantite la sicurezza e la protezione contro l'eventuale perdita o sottrazione di dati. Pertanto la responsabilità dei salvataggi dei dati in questi dispositivi è a carico del singolo utente.

6. Alle im vorigen Absatz genannten Speicherbereiche dürfen keine Daten enthalten, die für BSB von Interesse sind, da die Sicherheit und der Schutz vor möglichem Verlust oder Diebstahl von Daten nicht gewährleistet ist. Daher liegt die Verantwortung für das Speichern von Daten in diesen Geräten beim einzelnen Nutzer.

7. Senza il consenso del/la titolare **NON** è permessa la connessione di dispositivi personali alla rete dell'ente, sia essa cablata o *wireless.*

7. Ohne die Zustimmung des Inhabers ist es **NICHT** gestattet, sich mit dem Netzwerk des Betriebes mit persönlichen Geräten zu verbinden, weder kabelgebunden noch *wireless*.

8. Con regolare periodicità (almeno una volta al mese) è opportuno che ciascun utente provveda alla pulizia degli archivi informatici in sua gestione, mediante cancellazione dei file obsoleti o inutili.

8. Jeder Nutzer sollte regelmäßig (mindestens einmal im Monat) die von ihm verwalteten Computerarchive aufräumen, indem er veraltete oder unbrauchbare Dateien löscht.

9. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo necessario evitare un'archiviazione ridondante.

9. Besonderes Augenmerk muss auf die Duplizierung von Daten gelegt werden, um eine übermäßige Archivierung zu vermeiden.

10. ASSB mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno delle proprie strutture, mediante rete VPN (*Virtual Private Network*), un canale privato e criptato verso la rete interna con l'ausilio di Firewall SOPHOS, adeguatamente configurato e protetto da eventuali intrusioni e validato dal DPO di ASSB.

10. BSB bietet seinen Nutzern die Möglichkeit, auch von außerhalb seiner Einrichtungen auf seine Informatikressourcen zuzugreifen, und zwar über ein VPN (*Virtual Private Network*), einen privaten und verschlüsselten Kanal zum internen Netzwerk mit Hilfe einer SOPHOS-Firewall, die angemessen konfiguriert und vor möglichen Eingriffen geschützt und vom Datenschutzbeauftragten von BSB validiert ist.

11. L'accesso mediante VPN viene concesso a dipendenti e funzionari dell'ente che abbiano bisogno di svolgere compiti specifici, pur non essendo presenti nella propria sede abituale di lavoro (smart working).

11. Der Zugriff über VPN wird Mitarbeitern und Führungskräften des Betriebes gewährt, die bestimmte Aufgaben erledigen müssen, obwohl sie nicht an ihrem üblichen Arbeitsplatz anwesend sind (*Smart Working*).

12. All'interno di ASSB verranno rese disponibili reti senza fili (*wireless*), c.d. *wi-fi*. Tali reti consentiranno l'accesso a *internet* per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso a queste reti verrà concesso ad amministratori, dipendenti, consulenti, professionisti, tecnici, fornitori e cittadini che ne abbiano necessità.

12. Innerhalb von BSB werden drahtlose Netzwerke (wi-fi) zur Verfügung gestellt. Diese Netzwerke ermöglichen den Internetzugang für Geräte, die nicht per Kabel mit dem LAN verbunden sind. Der Zugang zu diesen Netzwerken wird Administratoren, Mitarbeitern, Beratern, Fachleuten, Technikern, Lieferanten und Bürgern gewährt, die ihn benötigen.

13. La richiesta per l'accesso alla rete tramite VPN verrà fatta con le stesse modalità sopra descritte al capo II.

13. Die Beantragung des Netzwerkzugangs über VPN erfolgt auf die gleiche Weise wie oben in Abschnitt II beschrieben.

14. Ogni utente avente la possibilità di accesso alla rete dell'ente attraverso

14. Jeder/Jede Nutzer/in, der/die die Möglichkeit hat, über persönliche Geräte

dispositivi personali deve garantire l'aggiornamento e la protezione degli stessi in termini di sicurezza. Il CED si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'ente. Nella modalità smart working il collegamento come precedentemente menzionato all'art. 4 comma 5 e nel comma precedente, avviene tramite VPN (Sophos o rete VPN nel caso del Consorzio dei Comuni) del PC privato alla rete aziendale nel rispetto del seguente Regolamento.

auf das Netzwerk des Betriebes zuzugreifen, muss gewährleisten, dass diese in Bezug auf die Sicherheit aktualisiert und geschützt sind. Die EDV-Dienststelle behält sich das Recht vor, den Zugang zum Netzwerk durch Geräte zu verweigern oder zu unterbrechen, die nicht ausreichend geschützt und/oder aktualisiert sind und eine reale Bedrohung für die Informatiksicherheit des Betriebes darstellen können. Im Smart-Working-Modus erfolgt die Verbindung, wie bereits in Art. 4, Abs. 5, und im vorigen Absatz erwähnt, über VPN (Sophos oder VPN-Netz im Falle des Südtiroler Gemeindeverbandes) des privaten PCs mit dem Betriebsnetz unter Einhaltung der Verordnung.

15. I locali o armadi tecnici adibiti alla gestione di apparati di rete e sistemi informatici sono accessibili soltanto al personale tecnico e vengono mantenuti chiusi a chiave.

15. Technische Räume oder Schränke, die für die Verwaltung von Netzwerkgeräten und Computersystemen verwendet werden, dürfen nur dem technischen Personal zugänglich sein und müssen verschlossen gehalten werden.

16. I *log* relativi all'accesso alla rete e agli archivi elettronici condivisi, possono essere registrati, attraverso sistemi automatici di monitoraggio, e possono essere oggetto di controllo da parte del titolare del trattamento, attraverso il CED, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'ente.

16. *Log* über den Zugang zum Netz und zu gemeinsam genutzten elektronischen Archiven können durch automatische Überwachungssysteme aufgezeichnet werden und können aus organisatorischen und produktionstechnischen Gründen, aus Gründen der Arbeitssicherheit und zum Schutz des Eigentums des Betriebes der Kontrolle des Rechtsinhabers der Datenverarbeitung durch die EDV-Dienststelle, unterliegen.

17. I controlli possono avvenire secondo le disposizioni previste nel presente regolamento. Le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di

17. Kontrollen können nach den Bestimmungen dieses Verordnung durchgeführt werden. Die gesammelten Informationen können für alle Zwecke im Zusammenhang mit dem Arbeitsverhältnis verwendet werden, einschließlich der Überprüfung der Einhaltung dieser Verordnung, die eine

effettuazione dei controlli ai sensi del Regolamento europeo 2016/679.

angemessene Information über die Verwendung der Geräte und die Durchführung der Kontrollen gemäß der Europäischen Verordnung 2016/679 darstellt.

18. In caso di cessazione del rapporto lavorativo, la cartella personale presente nelle condivisioni di rete verrà conservata per un periodo di 6 mesi e successivamente eliminata.

18. Im Falle der Beendigung des Arbeitsverhältnisses wird der in den gemeinsam genutzten Netzwerken vorhandene persönliche Ordner für einen Zeitraum von 6 Monaten aufbewahrt und anschließend gelöscht.

Art. 11
Assegnazione di Hardware e Software al personale e regole per l'utilizzo

1. Per prevenire l'introduzione di virus e/o altri programmi dannosi e per proteggere l'integrità del sistema informativo aziendale, il/la dipendente utilizza esclusivamente l'*hardware* (compresi modem, masterizzatori, *webcam*, microfoni e in generale qualsiasi tipo di supporto informatico), e i *software* in dotazione agli uffici/servizi, registrati a nome di ASSB, e precauzionalmente autorizzati dal/la Dirigente competente e dal/la Responsabile del CED.

Art. 11
Zuweisung von Hardware und Software an Mitarbeiter und Regeln für die Nutzung

1. Um die Einschleppung von Viren und/oder anderen schädlichen Programmen zu verhindern und die Integrität des Informationssystems des Betriebes zu schützen, darf der/die Mitarbeiter/in ausschließlich die Hardware (einschließlich Modems, Brenner, Webcams, Mikrofone und allgemein jede Art von Computertechnik) und Software verwenden, die den Büros/Dienststellen zur Verfügung gestellt werden, auf den Namen von BSB registriert sind und von der zuständigen Führungskraft und dem Verantwortlichen der EDV-Dienststelle vorsorglich genehmigt wurden.

2. Per garantire la compatibilità funzionale, tecnica e il mantenimento dell'efficienza dei sistemi e della rete, di norma, non possono essere utilizzati *software* di proprietà personale quali:

- i programmi regolarmente acquistati e registrati;
- i programmi *shareware* e/o *freeware*;
- i software scaricati da *internet* o provenienti da supporti informatici;
- allegati a riviste e/o giornali o altri *software* posseduti a qualsiasi titolo.

2. Um die funktionelle und technische Kompatibilität zu gewährleisten und die Leistungsfähigkeit der Systeme und des Netzwerks zu erhalten, darf grundsätzlich keine Software aus dem persönlichem Eigentum des Mitarbeiters verwendet werden, wie z. B.:

- die regelmäßig gekauften und registrierten Programme;
- Shareware- und/oder Freeware-Programme;
- Software, die aus dem Internet oder von Computermedien heruntergeladen wurde;
- Anhänge an Zeitschriften und/oder

In via eccezionale tali *software* di proprietà personale, nel caso vengano considerati utili ai fini lavorativi, possono essere usufruiti, **previa autorizzazione scritta da parte del/la proprio/a Dirigente che ne verifica l'idoneità, nonché del/la Responsabile del CED che ne verifica i requisiti tecnici, di compatibilità e idoneità della licenza.**

3. Il personale è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (*copyright*), e non può installare, duplicare o utilizzare i *software* al di fuori di quanto consentito dagli accordi di licenza. Ogni utente è comunque responsabile dell'utilizzo improprio di tali mezzi.

4. Qualora il personale del CED rilevasse la presenza di quanto descritto ai precedenti commi del presente articolo, sarà inoltrata al/la dirigente competente e al/la Direttore/trice dell'Ufficio CED segnalazione scritta e proposta di organizzazione degli interventi necessari per l'immediata rimozione.

Art. 12

Utilizzo degli strumenti: Postazione di Lavoro (PDL) ed altri strumenti con relativi Software

1. Il/la dipendente/collaboratore/ collaboratrice è consapevole che gli strumenti forniti sono di proprietà di ASSB e utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è

Zeitungen oder andere Software, die sich aus irgendeinem Grund in Besitz des Bediensteten befinden.

In Ausnahmefällen, wenn eine solche im persönlichen Besitz befindliche Software für Arbeitszwecke als nützlich erachtet wird, darf sie verwendet werden, **vorbehaltlich einer schriftlichen Genehmigung durch den eigenen Vorgesetzten, der ihre Eignung überprüft, sowie durch den Verantwortlichen der EDV-Dienststelle, der die technischen Anforderungen, die Kompatibilität und die Eignung der Lizenz überprüft.**

3. Das Personal ist verpflichtet, die Gesetze zum Schutz des geistigen Eigentums (Urheberrecht) zu beachten und darf die Software nicht installieren, vervielfältigen oder außerhalb des durch die Lizenzvereinbarungen erlaubten Rahmens nutzen. Für den unsachgemäßen Gebrauch solcher Mittel ist auf jeden Fall jeder/jede Nutzer/in selbst verantwortlich.

4. Falls das Personal der EDV-Dienststelle das Vorhandensein eines der in den vorhergehenden Absätzen dieses Artikels beschriebenen Mittel feststellt, wird ein schriftlicher Bericht an die zuständige Führungskraft und an den Direktor des Büros der EDV-Dienststelle geschickt, zusammen mit einem Vorschlag notwendiger Maßnahmen für ihre sofortige Beseitigung zu organisieren.

Art. 12

Benutzung der Geräte: Arbeitsplatz und andere Instrumente mit zugehöriger Software

1. Dem/Der Bediensteten/Mitarbeiter/in ist bekannt, dass die zur Verfügung gestellten Mittel Eigentum von BSB sind und ausschließlich zur Durchführung der Arbeitstätigkeit verwendet werden.

responsabile dell'utilizzo delle dotazioni informatiche, ricevute in assegnazione o che comunque utilizza.

2. Per postazione di lavoro si intende il complesso unitario di pc, accessori, periferiche ed ogni altro *device* concesso, da ASSB, in utilizzo all'utente e/o video-terminalista.

3. Il pc, assegnato all'utente e/o video-terminalista da ASSB, deve essere utilizzato secondo i principi di diligenza, correttezza e con le modalità indicate nell'elencazione che segue:

a) evitare ogni possibile forma di danneggiamento;
b) non è consentito l'utilizzo del pc di ASSB per motivi personali;
c) il/la dipendente non può spostare il pc di proprietà dell'ente in altro ufficio o fuori dai locali di ASSB, salvo autorizzazione del/la Dirigente preposto/a e sentito il servizio CED. È tenuto, inoltre, a custodire il pc con la massima diligenza, curando di spegnerlo al termine della giornata lavorativa, salva la possibilità di attivare unicamente la disconnessione, nell'ambito di *smart working* / telelavoro autorizzati;
d) nel caso di assenze prolungate dall'ufficio, al fine di evitare accessi da parte di terzi non autorizzati, di incorrere in potenziali rischi elettrici e di sprecare risorse energetiche, il/la dipendente spegne il pc, salva la possibilità di attivare unicamente la disconnessione, nell'ambito di *smart working* / telelavoro autorizzati;
e) per assenze brevi dall'ufficio è necessario attivare il salvaschermo dotato di password (ctrl+alt+canc + blocca);

Jeder/Jede Mitarbeiter/in ist für die Nutzung der Informatikgeräte verantwortlich, die ihm zugewiesen wurden oder die er benutzt.

2. Der Begriff *"Arbeitsplatz"* bezieht sich auf den einheitlichen Satz von PCs, Zubehör, Peripheriegeräten und allen anderen Geräten, die BSB dem Nutzer und/oder dem Video-Terminalisten zur Verfügung stellt.

3. Der PC, der dem/der Nutzer/in und/oder dem Video-Terminalisten von BSB zugewiesen wurde, muss nach den Grundsätzen der Sorgfalt, der Korrektheit und in der Art und Weise verwendet werden, die in der folgenden Liste angegeben ist:

a) Beschädigungen jedweder Art müssen vermieden werden;
b) die Nutzung des PCs des Betriebes zu persönlichen Zwecken ist nicht gestattet;
c) der/die Mitarbeiter/in darf den zur Einrichtung gehörenden PC nicht in ein anderes Büro oder außerhalb des BSB-Geländes verlegen, es sei denn, die zuständige Führungskraft hat dies nach Rücksprache mit der EDV-Dienststelle genehmigt. Darüber hinaus ist der/die Mitarbeiter/in verpflichtet, den PC mit der größtmöglichen Sorgfalt zu behandeln und ihn am Ende des Arbeitstages abzuschalten, unbeschadet der Möglichkeit, die Abschaltung nur im Rahmen von genehmigtem Smart Working / Telearbeit zu aktivieren;
d) bei verlängerten Abwesenheiten muss der PC abgeschaltet werden, damit kein unbefugter Zugang von Seiten Dritter erfolgen kann, damit mögliche elektrische Schäden verhindert und eine Energieeinsparung erzielt werden kann;unbeschadet der Möglichkeit, nur die Abschaltung im Rahmen von Smart Working / Telearbeit zu aktivieren, die genehmigt wurde;
e) bei kurzen Abwesenheiten vom

f) il/la dipendente non può modificare la configurazione impostata del pc assegnato, e installare dispositivi esterni senza l'autorizzazione di cui al precedente articolo 11, comma 2;

g) è possibile utilizzare il pc di un/a collega assente, accedendovi con le proprie credenziali di autenticazione, solo ed esclusivamente per improrogabili necessità di lavoro (quali, ad esempio, la temporanea impossibilità di utilizzo del pc per cause tecniche), previa autorizzazione del/la Dirigente/Responsabile preposto/a.

Büro ist es notwendig, den Bildschirmschoner mit Passwort zu aktivieren (Strg+Alt+Löschen+Sperren);

f) der/die Mitarbeiter/in darf die Konfiguration des zugewiesenen PCs nicht ändern und keine externen Geräte ohne die in Artikel 11, Absatz 2, oben genannte Genehmigung installieren;

g) es ist möglich, den PC eines abwesenden Kollegen zu nutzen, indem man mit seinen eigenen Zugangsdaten darauf zugreift, nur und ausschließlich für dringende Arbeitsbedürfnisse (wie z. B. bei vorübergehende Unmöglichkeit, den eigenen PC aus technischen Gründen zu nutzen), mit vorheriger Genehmigung der zuständigen Führungskraft.

4. É assolutamente vietato cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi non autorizzati.

4. Es ist absolut verboten, die Nutzung der Informatikeinrichtungen und -Anlagen des Betriebes, auch nur vorübergehend, an unbefugte Dritte zu übertragen.

5. Il servizio CED provvede alla gestione della manutenzione del materiale informatico e alla configurazione del posto di lavoro, in modo tale da garantirne un uso adeguato in termini di sicurezza informatica del sistema, nonché di profilo, del/la dipendente assegnatario/a.

5. Die EDV-Dienststelle sorgt für die Verwaltung der Wartung des Materials und der Konfiguration des Arbeitsplatzes, um eine angemessene Nutzung in Bezug auf die technische Sicherheit des Systems sowie das Profil des zugewiesenen Mitarbeiters zu gewährleisten.

6. I tecnici del servizio CED accedono alle risorse del sistema informatico, compresi i pc, con strumenti di assistenza remota e di diagnostica per poter svolgere le attività di manutenzione ordinaria e straordinaria.

6. Die Techniker der EDV-Dienststelle greifen mit Fernwartungs- und Diagnoseprogramme auf die Ressourcen des Computersystems, einschließlich der PCs, zu, um ordentliche und außerordentliche Wartungsarbeiten durchzuführen.

7. Per garantire la sicurezza informatica e il corretto funzionamento della rete, il CED può diramare in qualsiasi momento avvisi rivolti alla generalità dei/lle dipendenti o a gruppi più ristretti, a seconda dei casi, per segnalare la presenza di *file* non consentiti, pericolosi o meno per l'integrità del sistema, con l'invito a rimuoverli autonomamente entro un breve termine perentorio. Decorso inutilmente il termine, i *file* verranno rimossi dal CED, con conseguente segnalazione al/la Dirigente nella cui area o servizio è avvenuta la violazione per i necessari provvedimenti.

7. Um die Computersicherheit und das korrekte Funktionieren des Netzwerks zu gewährleisten, kann die EDV-Dienststelle jederzeit Mitteilungen an alle Mitarbeiter oder ggf. an kleinere Gruppen ausgeben, um das Vorhandensein von nicht erlaubten, für die Integrität des Systems gefährlichen oder nicht gefährlichen Dateien zu signalisieren, mit der Aufforderung, diese innerhalb einer kurzen Frist selbständig zu entfernen. Nach erfolglosem Ablauf der Frist werden die Dateien von der EDV-Dienststelle entfernt, mit anschließender Meldung an den Vorgesetzten, in dessen Bereich oder Dienst der Verstoß aufgetreten ist, für die notwendigen Maßnahmen.

8. Le informazioni archiviate sulla pdl locale devono essere esclusivamente quelle necessarie all'attività lavorativa e non sono soggette ad attività di *backup* periodico.

8. Die am betrieblichen Arbeitsplatz gespeicherten Informationen müssen ausschließlich solche sein, die für die Arbeitstätigkeit notwendig sind und unterliegen keinem periodischen *backup*.

9. La gestione dei dati sulle pdl è demandata all'utente utilizzatore/utilizzatrice, che dovrà provvedere a memorizzare sulle condivisioni dell'ente dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.

9. Die Verwaltung der Daten auf den betrieblichen Arbeitsplätzen wird an den Nutzer delegiert, der dafür sorgen muss, dass die Daten auf den gemeinsam genutzten Trägern des Betriebes gespeichert werden, die auch von anderen Nutzern verwendet werden können, um die Exklusivität diese Daten zu vermeiden.

10. Non è consentita l'installazione autonoma di programmi nelle pdl e in ogni caso di programmi diversi da quelli autorizzati dall'ente e sprovvisti di adeguata licenza di utilizzo.
Tutte le richieste di risorse *hardware* e *software* dovranno essere inoltrate al CED per le opportune valutazioni.

10. Es ist nicht erlaubt, eigenständige Programme auf den betrieblichen Arbeitsplätzen zu installieren und auf keinen Fall Programme, die nicht vom Betrieb autorisiert sind und keine entsprechende Lizenz besitzen. Alle Anfragen für Hardware- und Software-Ressourcen müssen an die EDV-Dienststelle zur entsprechenden Bewertung weitergeleitet werden.

11. Gli operatori del CED potranno in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza delle pdl, della rete locale e dei *server* dell'ente, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'ente.

11. Die Mitarbeiter der EDV-Dienststelle können jederzeit alle Dateien oder Anwendungen entfernen, die sie als gefährlich für die Sicherheit der betrieblichen Arbeitsplätze, des lokalen Netzwerks und der Server des Betriebes erachten, sowie alle Einstellungen, die so konfiguriert sein können, dass sie das korrekte Funktionieren der Informatikdienste des Betriebes beeinträchtigen können.

12. È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere la pdl sempre protetta.

12. Es ist zwingend erforderlich, die Installation von System-Aktualisierungen, die automatisch vorgeschlagen werden, zum ersten verfügbaren Zeitpunkt zuzulassen, so dass die betrieblichen Arbeitsplätze immer geschützt sind.

13. Nel caso in cui si dovessero notare anomalie nella pdl, l'utente stesso è tenuto a comunicarlo tempestivamente al CED.

13. Im Falle von Anomalien am Arbeitsplatz muss der Nutzer die EDV-Dienststelle umgehend informieren.

14. I controlli possono avvenire secondo le disposizioni previste nel presente regolamento. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento europeo 2016/679.

14. Kontrollen können nach den Bestimmungen dieser Verordnung durchgeführt werden. Die auf diese Weise gesammelten Informationen können auch für alle Zwecke im Zusammenhang mit dem Arbeitsverhältnis verwendet werden, einschließlich der Überprüfung der Einhaltung dieser Verordnung, die eine angemessene Information über die Verwendung der Geräte und die Durchführung der Kontrollen gemäß der Europäischen Verordnung 2016/679 darstellt.

Art. 13

Utilizzo delle periferiche, delle risorse di rete

1. Per razionalizzare, ottimizzare e gestire in maniera adeguata il patrimonio informativo digitalizzato e le risorse *hardware* aziendali, la rete informatica di ASSB è configurata per consentire

Art. 13

Benutzung der Peripheriegeräte und der Netzwerkressourcen

1. Um die digitalisierten Informationsressourcen und die Hardwareressourcen angemessen rationalisieren, optimieren und verwalten zu können wurde das betriebliche Netzwerk so

l'utilizzo di risorse *hardware* centralizzate e condivise. L'utilizzo di periferiche locali (stampanti, *scanner*, dischi locali, ecc.) costituisce un'eccezione che, opportunamente motivata, è consentita solo se autorizzata dal/la proprio/a Dirigente e dal/la Responsabile del CED.

konfiguriert, dass die Hardwareressourcen zentral und gemeinsam benutzt werden können. Die Benutzung von lokalen Peripheriegeräten (Drucker, Scanner, Festplatten, usw.) bildet eine Ausnahme, die nur mit Ermächtigung von Seiten der Führungskraft und des Verantwortlichen der EDV-Dienststelle zulässig ist.

2. Il/la dipendente è tenuto/a ad archiviare tutti i dati nel sistema di gestione documentale D3 e a utilizzare le applicazioni aziendali, appositamente installate per la produzione e archiviazione dei documenti informatici. Sulle risorse locali del pc non è impostata alcuna procedura di salvataggio dei dati e non è consentito archiviare informazioni attinenti l'attività lavorativa.

2. Die Bediensteten müssen sämtliche Daten im Dokumentenverwaltungssystem D3 abspeichern und sind dazu angehalten, die Anwendungen zu verwenden, die vom BSB für die Herstellung und für die Archivierung von digitalen Unterlagen entwickelt und zur Verfügung gestellt werden. Die lokalen Ressourcen der Rechner wurden ohne Datensicherungsverfahren konfiguriert; es ist den Bediensteten untersagt, Informationen im Zusammenhang mit der Arbeitstätigkeit zu archivieren.

Art. 14
Amministrazione digitale e domicilio digitale

Art. 14
Digitale Verwaltung und digitales Domizil

1. In conformità alla normativa in materia di amministrazione digitale, ASSB si è dotata di un *software* di gestione documentale e protocollo informatico (D3). L'accesso a tale sistema avviene mediante l'utilizzo di credenziali nel rispetto della procedura degli accessi descritta nel precedente articolo 7 del presente regolamento.

1. In Übereinstimmung mit den Vorschriften zur digitalen Verwaltung hat der BSB eine Software zur Dokumentenverwaltung und digitalen Protokollierung eingeführt (D3). Der Zugang zu diesem System erfolgt über Zugangsdaten, die im vorhergehendem Art. 7 dieser Verodnung beschrieben sind.

2. La configurazione dei gruppi di accesso al sistema documentale è di competenza del CED. La creazione dei fascicoli è, invece, demandata alle direttive dei/delle Dirigenti stessi/e, che vigilano e permettono l'accesso ai dipendenti/collaboratori/collaboratrici nel rispetto delle disposizioni vigenti anche a livello di ente in tema di *privacy.*

2. Die Konfiguration der Zugriffsgruppen auf das Dokumentensystem liegt in der Verantwortung der EDV-Dienststelle. Das Anlegen von Dateien hingegen wird an die Führungskräfte selbst delegiert, die den Zugang den Bediensteten/Mitarbeitern unter Einhaltung der geltenden Datenschutznormen, auch auf Betriebsebene, überwachen und erlauben.

3. Ciascun dipendente autorizzato/a alla

3. Jeder/Jede Mitarbeiter/in, der befugt ist,

produzione di documenti informatici è abilitato/a all'utilizzo del relativo *software* e accede ai gruppi e fascicoli a lui/lei assegnati dopo specifica richiesta da parte del/la Dirigente del servizio.

EDV-Dokumente zu erstellen, muss in die Lage versetzt werden, die entsprechende Software zu nutzen und hat nach ausdrücklicher Aufforderung durch die Führungskraft des Dienstes, Zugriff auf die ihm zugewiesenen Gruppen und Dateien.

4. Sui *server* aziendali sono archiviati dati e documenti strettamente professionali e relativi all'attività lavorativa. I/le dipendenti hanno la responsabilità di accedervi, evitandone l'utilizzo per scopi privati.

4. Auf den betrieblichen Servereinheiten sind alle strikt mit den Arbeitstätigkeiten verbundenen Daten und Unterlagen gespeichert. Die Bediensteten haben die Pflicht, im Zugang große Sorgfalt walten zu lassen und müssen die Nutzung aus privaten Zwecken unterlassen.

5. In ottemperanza alle disposizioni in materia di amministrazione digitale, l'utilizzo del fax per la trasmissione/il ricevimento di documenti è ridotta ai soli casi previsti. Tutti i documenti cartacei che ne derivano sono opportunamente digitalizzati, autenticati e archiviati.

5. Im Rahmen der Umsetzung der Vorschriften zur digitalen Verwaltung ist die Nutzung von Faxgeräten für den Erhalt und die Versendung von Unterlagen auf die strikt dafür vorgesehenen Fälle einzuschränken. Alle Papierunterlagen müssen in angemessener Form digitalisiert, beglaubigt und archiviert werden.

6. In forza della Legge 11.09.2020, n. 120, di conversione del Decreto Legge 16.07.2020, n. 76 (cd. Decreto Semplificazioni), sono divenute operative le disposizioni normative che hanno il fine di ridisegnare la governance del digitale, accelerare la digitalizzazione dei servizi pubblici e semplificare i rapporti tra cittadini e pubblica amministrazione in un'ottica di diffusione della cultura dell'innovazione e di superamento del divario digitale, con un'attenzione anche all'accesso agli strumenti informatici delle persone con disabilità.

6. Mit dem Gesetz 11.09.2020, Nr. 120, zur Umwandlung des Gesetzes 16.07.2020, Nr. 76 (das sogenannte Vereinfachungsdekret), sind die gesetzlichen Bestimmungen in Kraft getreten, die darauf abzielen, die digitale Verwaltung neu zu gestalten, die Digitalisierung öffentlicher Dienstleistungen zu beschleunigen und die Beziehungen zwischen Bürgern und öffentlicher Verwaltung zu vereinfachen, um die Innovationskultur zu verbreiten und die digitale Kluft zu überwinden, wobei auch der Zugang zu Informatikinstrumenten für Menschen mit Behinderungen im Fokus steht.

7. L'art. 37 del Decreto Semplificazioni, con riguardo al Codice dell'Amministrazione Digitale (CAD), sostituisce il riferimento all'indirizzo PEC con quello di domicilio digitale.

7. In Artikel 37 des Vereinfachungsdekrets wird in Bezug auf den digitalen Verwaltungscode (EGovG) der Verweis auf die ZEP-Adresse durch den des digitalen Domizils ersetzt.

8. Il domicilio digitale è un indirizzo elettronico eletto presso un servizio di

8. Das digitale Domizil ist eine elektronische Adresse, die bei einem zertifizierten

posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, valido ai fini delle comunicazioni elettroniche aventi valore legale ai sensi dell'art. 1, comma 1, lett. n-ter del CAD.

elektronischen Postdienst oder einem qualifizierten zertifizierten elektronischen Zustelldienst gewählt wurde und für die Zwecke der elektronischen Kommunikation mit Rechtswirkung gemäß Art. 1, Absatz 1, Buchstabe n-ter der EGovG gültig ist.

9. L'identificazione digitale è equiparata all'esibizione di un documento d'identità ed è estesa per l'accesso ai servizi dei concessionari pubblici e delle società a partecipazione pubblica.

9. Die digitale Identifikation ist gleichbedeutend mit der Vorlage eines Ausweises und wird auf den Zugang zu den Dienstleistungen öffentlicher Konzessionäre und öffentlicher Unternehmen erweitert.

10. Sono previste misure di semplificazione per il sistema di qualificazione dei conservatori di documenti informativi e dei prestatori di servizi fiduciari e di valorizzazione del patrimonio informativo pubblico attraverso la piattaforma digitale nazionale dati.

10. Es sind Vereinfachungsmaßnahmen für das System der Qualifizierung der Verwalter von Informationsdokumenten und der Anbieter von Treuhanddiensten sowie die Aufwertung der öffentlichen Informationsbestände durch die nationale digitale Datenplattform vorgesehen.

CAPO III

DISPOSIZIONI SULL'UTILIZZO DELLA POSTA ELETTRONICA

Art. 15 – Utilizzo della posta elettronica

1. Le regole, di seguito specificate, sono adottate ai sensi delle *Linee guida del Garante per posta elettronica e internet*, citate nelle premesse.

2. Ciascun dipendente/collaboratore/collaboratrice si deve attenere alle seguenti regole di utilizzo dell'indirizzo di posta elettronica. La stretta osservanza delle disposizioni del presente articolo risulta condizione essenziale per ottenere e mantenere l'attribuzione in uso di una casella e-mail nominativa nel dominio dell'ASSB (@aziendasociale.bz.it), generalmente coerente con il modello iniziale nome e

ABSCHNITT III

ANORDNUNGEN ZUR BENUTZUNG DER E-MAIL

Art. 15 – Benutzung der E-Mail

1. Die nachstehend angeführten Regeln werden in Übereinstimmung mit den in der Einleitung zitierten Richtlinien des *"Garantiegebers für E-Mail und Internet"* erlassen.

2. Jeder/Jede Bedienstete/Mitarbeiter/in muss die folgenden Regeln für die Nutzung der E-Mail-Adresse einhalten. Die strikte Einhaltung der Bestimmungen dieses Artikels ist eine wesentliche Voraussetzung für die Erlangung und Aufrechterhaltung der Zuweisung bei der Nutzung einer nominativen E-Mail-Adresse in der Domäne des BSB (@sozialbetrieb.bz.it), die in der Regel mit dem Vor- und Nachnamen übereinstimmt.

cognome.

3. L'utilizzo della posta elettronica istituzionale è stato fornito al personale dell'ASSB per incrementare la propria produttività a beneficio sia dell'organizzazione, sia - e soprattutto - di tutti i soggetti con cui l'ente intrattiene rapporti di comunicazione. Il personale ha, pertanto, la responsabilità di utilizzare la posta elettronica per finalità legittime ed etiche, strettamente connesse allo svolgimento delle proprie mansioni lavorative.

3. Die Nutzung der institutionellen E-Mail wurde den BSB-Mitarbeitern zur Verfügung gestellt, um ihre Produktivität zu steigern, was sowohl dem Betrieb als auch - vor allem - all denjenigen zugute kommt, mit denen der Betrieb Kommunikationsbeziehungen unterhält. Die Mitarbeiter/innen sind daher dafür verantwortlich, elektronische Post für legitime und ethische Zwecke zu nutzen, die strikt mit der Erfüllung ihrer Arbeitsaufgaben zusammenhängen.

4. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa, nonché di conservare e modificare frequentemente la *password* (almeno una volta ogni tre mesi), secondo le medesime indicazioni fornite per la gestione dell'*account* di accesso alle pdl.

4. Der/Die Nutzer/in, dem ein E-Mail-Postfachs zugewiesen wurde, ist für die korrekte Nutzung desselben sowie für die Aufbewahrung und häufige Änderung des Passworts (mindestens einmal alle drei Monate) verantwortlich, gemäß denselben Angaben, die für die Verwaltung des Zugangscodes zum betrieblichen Arbeitsplatz vorgesehen sind.

5. L'ASSB fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro, il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati destinati all'ufficio / al gruppo.

5. BSB stellt außerdem E-Mail-Postfächer zur Verfügung, die jeder Organisationseinheit, jedem Büro oder jeder Arbeitsgruppe zugeordnet sind und deren Nutzung bei Mitteilungen von kollektivem Interesse den benannten E-Mails vorzuziehen ist. Damit soll vermieden werden, dass einzelne Benutzer die Exklusivität über die für das Büro/die Gruppe bestimmten Daten behalten.

6. Tutta la corrispondenza con cittadini, imprese e altra pubblica amministrazione relativa a procedimenti amministrativi è necessario transiti attraverso il protocollo dell'ente e venga gestita con i canali telematici ufficiali.

6. Die gesamte Korrespondenz mit Bürgern, Unternehmen und anderen öffentlichen Verwaltungen, die sich auf Verwaltungsverfahren bezieht, muss über das Protokoll der Einrichtung laufen und über offizielle Telematikkanäle abgewickelt werden.

7. L'iscrizione a *mailing list* o *newsletter* esterne con il proprio indirizzo dell'ente è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre

7. Das Abonnieren von externen Mailinglisten oder Newslettern mit der eigenen Adresse ist ausschließlich aus beruflichen Gründen erlaubt. Vor der

verificare anticipatamente l'affidabilità del sito che offre il servizio.

Registrierung muss die Zuverlässigkeit der Seite, die den Dienst anbietet, vorab geprüft werden.

8. Allo scopo di garantire sicurezza alla rete dell'ente, è opportuno evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità, con i quali non sussiste alcun rapporto lavorativo o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.*exe*, *.*com*, *.*vbs*, *.*htm*, *.*scr*, *.*bat*, *.*js*, *.*xlse*, *.*xlsx* e *.*pif*.

8. Um die Sicherheit des Netzwerks des Betriebes zu gewährleisten, ist es ratsam, das Öffnen eingehender Mails von Absendern zu vermeiden, deren Identität unbekannt ist, mit denen keine Arbeitsbeziehung besteht oder die verdächtige oder ungewöhnliche Inhalte haben oder die Anhänge wie *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js, *.xlse, *.xlsx und *.pif enthalten.

9. È necessario porre molta attenzione alla credibilità del messaggio e del mittente per evitare casi di *phishing*, frodi informatiche, o installazione involontaria di *software* malevolo. A titolo esemplificativo, si citano i solleciti di pagamento delle fatture per le quali esiste un'apposita procedura riguardante la fattura elettronica. In qualunque situazione di incertezza, prima di eseguire qualsiasi azione, è opportuno contattare il CED per una valutazione dei singoli casi.

9. Es muss sorgfältig auf die Glaubwürdigkeit der Nachricht und des Absenders geachtet werden, um Fälle von *Phishing*, Informatikbetrug oder die unbeabsichtigte Installation von Schadsoftware zu vermeiden. Beispiele hierfür sind Mahnungen für Rechnungen, für die es ein spezielles Verfahren zur elektronischen Rechnungsstellung gibt. In jeder unsicheren Situation ist es ratsam, sich vor dem Ergreifen von Maßnahmen mit der EDV-Dienststelle in Verbindung zu setzen, um eine Einschätzung des Einzelfalls zu erhalten.

10. Non é consentito diffondere messaggi cd *catena di S. Antonio* o di tipologia simile, anche se il contenuto sembra meritevole di attenzione; in particolare, gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus.

10. Es ist nicht gestattet, als Kettenbriefe bekannte Nachrichten (sog. *catena di S. Antonio)* zu verbreiten, auch wenn der Inhalt beachtenswert erscheint; insbesondere Solidaritätsaufrufe und Nachrichten, die über die Existenz neuer Viren informieren.

11. Nel caso fosse necessario inviare allegati "pesanti" (oltre i 20 MB), è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato *.zip* o equivalente. Nel caso di allegati ancora più voluminosi, è necessario rivolgersi al personale del CED per la valutazione delle soluzioni.

11. Wenn es erforderlich ist, *"schwere"* Anhänge (über 20 MB) zu versenden, ist es ratsam, die Originaldateien zunächst in ein .zip- oder gleichwertiges Archiv zu komprimieren. Bei noch größeren Anbauten ist es notwendig sich an die EDV-Dienststelle für die Bewertung von Lösungen zu wenden.

12. Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati particolari, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso criptazione con apposito *software* (archiviazione e compressione con *password*). La *password* di criptazione deve essere comunicata al destinatario attraverso un canale diverso dalla *mail* (ad esempio per lettera o per telefono) e mai assieme ai dati criptati.

12. Wenn es notwendig ist, Nachrichten, die Anhänge mit personenbezogenen Daten oder sensiblen Daten enthalten, an externe Empfänger zu senden, ist es zwingend erforderlich, dass diese Anhänge zuvor durch Verschlüsselung mit spezieller Software (Archivierung und Komprimierung mit Passwort) unverständlich gemacht werden. Das Verschlüsselungspasswort muss dem Empfänger über einen anderen Kanal als E-Mail
(z. B. per Brief oder Telefon) und niemals zusammen mit den verschlüsselten Daten mitgeteilt werden.

13. Tutte le informazioni dell'ente, i dati personali e/o particolari di competenza dell'ente possono essere inviati soltanto a destinatari - persone o enti – qualificati e competenti, e nell'ambito di un procedimento amministrativo, preferendo allo scopo i canali di comunicazione istituzionali.

13. Alle Informationen der Einrichtung, persönliche und/oder sensible Daten der Einrichtung dürfen nur an qualifizierte und zuständige Empfänger - Personen oder Einrichtungen - und im Rahmen eines Verwaltungsverfahrens übermittelt werden, wobei zu diesem Zweck institutionelle Kommunikationskanäle bevorzugt werden

14. La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del/la Direttore/trice dell'Ufficio competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo e indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn), se la tipologia del messaggio lo consente. È in ogni caso preferibile utilizzare il servizio di invio *newsletter*, più idoneo a gestire comunicazioni/avvisi/inviti ad una pluralità di soggetti.

14. Die massenhafte Verbreitung von E-Mail-Nachrichten darf ausschließlich aus dienstlichen Gründen erfolgen, ggf. mit Genehmigung des Direktors des zuständigen Amtes. Um zu vermeiden, dass eventuelle Antworten an alle weitergeleitet werden, was zu übermäßigem und unerwünschtem Datenverkehr führt, müssen die Empfänger in eine versteckte Kopie (Bcc oder Ccn) gesetzt werden, wenn die Typologie der Nachricht dies zulässt. In jedem Fall ist es vorzuziehen, den Newsletter-Dienst zu verwenden, der für die Verwaltung von Mitteilungen/Bekanntmachungen/Einladungen an eine Vielzahl von Subjekten besser geeignet ist.

15. Le comunicazioni, anche elettroniche e i documenti elettronici allegati possono avere rilevanza procedimentale e devono essere conservati per la durata prevista dalla normativa vigente.

15. Mitteilungen, einschließlich elektronischer Mitteilungen, und angehängte elektronische Dokumente können verfahrensrelevant sein und müssen für den Zeitraum aufbewahrt

werden, den die aktuelle Gesetzgebung vorsieht.

16. ASSB non controlla sistematicamente il flusso di comunicazioni *mail* né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail.*

16. BSB kontrolliert nicht systematisch den Fluss der E-Mail-Kommunikation und ist auch nicht mit Systemen zum systematischen Lesen oder Analysieren von E-Mail-Nachrichten oder der entsprechenden externen Daten ausgestattet, die über das hinausgehen, was technisch notwendig ist, um den E-Mail-Dienst durchzuführen.

17. È vietato inviare posta elettronica in nome e per conto di un altro utente.

17. Es ist verboten, E-Mails im Namen und im Auftrag eines anderen Nutzers zu versenden.

18. La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo il salvataggio della e-mail completa degli allegati in formato .eml nel sistema di gestione documentale. Tale formato è un'estensione di file che identifica un messaggio di posta elettronica salvato nel formato standard MIME RFC 822 da Lotus Notes o da altri programmi di posta elettronica. I file EML contengono testo ASCII che mantiene la formattazione dell'email originale per le intestazioni e il corpo del messaggio principale, nonché collegamenti ipertestuali e allegati. In questo modo, riaprendo il messaggio di posta elettronica sarà esattamente corrispondente all'originale.

18. Persönliche E-Mail-Postfächer müssen aufgeräumt werden, indem Nachrichten und Dokumente, deren Aufbewahrung nicht mehr notwendig ist, gelöscht werden. Auch das Speichern von Nachrichten mit umfangreichen Anhängen sollte möglichst vermieden werden, stattdessen sollte die E-Mail komplett mit Anhängen im .eml-Format im Dokumentenverwaltungssystem gespeichert werden. Dieses Format ist eine Dateierweiterung, die eine E-Mail-Nachricht kennzeichnet, die im Standardformat MIME RFC 822 von Lotus Notes oder anderen E-Mail-Programmen gespeichert wird. EML-Dateien enthalten ASCII-Text, der die Formatierung der Original-E-Mail für die Kopfzeilen und den Hauptteil der Nachricht sowie für Hyperlinks und Anhänge beibehält. Auf diese Weise entspricht das erneute Öffnen der E-Mail-Nachricht genau dem Original.

19. I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione/segnalazione dello *spam*. I messaggi che dovessero contenere virus, se individuati, vengono eliminati dal sistema di controllo e il mittente/destinatario viene avvisato mediante messaggio specifico.

19. Eingehende Nachrichten werden routinemäßig auf Viren und Malware sowie auf *Spam* analysiert. Nachrichten, die Viren enthalten, werden, wenn sie erkannt werden, vom Kontrollsystem gelöscht und der Absender/Empfänger wird durch eine spezielle Nachricht benachrichtigt.

20. La posta elettronica può essere gestita sia dalla pdl in dotazione che da qualsiasi dispositivo connesso a *internet*, utilizzando il portale raggiungibile all'indirizzo e le credenziali personali della casella.

20. Die elektronische Post kann sowohl über den zugewiesenen Arbeitsplatz als auch über ein beliebiges mit dem Internet verbundenes Gerät verwaltet werden, wobei das Portal unter der Adresse und den persönlichen Zugangsdaten des Mail-Postfachs zugänglich ist.

21. In casi particolari e su esplicita richiesta al CED, possono essere configurati ed utilizzati dispositivi personali (es. *smartphone/tablet*) per la gestione della posta elettronica.

21. In besonderen Fällen und auf ausdrückliche Anfrage an die EDV-Dienststelle können persönliche Geräte (z. B. Smartphones/Tablets) konfiguriert und zur Verwaltung von E-Mails verwendet werden.

Art. 16
Assenze e cessazione dal servizio

1. Durante i periodi di assenza (es. ferie, malattia, infortunio ecc.) non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un inoltro automatico delle e-mail entranti). In caso di assenza, è preferibile utilizzare l'inoltro automatico ad altre caselle dell'ente e/o un messaggio di risposta automatica *Assenza dall'Ufficio/Out of Office*, facendo menzione di chi, all'interno dell'ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo, anche di tipo collettivo, tipo ufficioX@aziendasociale.bz.it (cfr. allegato n. 1).

2.In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione di risposta automatica o l'inoltro automatico su altre caselle dell'ente e si debba conoscere il contenuto dei messaggi di posta elettronica, il/la titolare della

ART. 16
Abwesenheiten und Beendigung des Dienstes

1. Während Zeiten der Abwesenheit (z. B. Urlaub, Krankheit, Unfall, etc.) ist es nicht erlaubt, E-Mails automatisch an die private E-Mail-Adresse zu senden (z. B. durch Aktivierung der automatischen Weiterleitung eingehender E-Mails). Im Falle einer Abwesenheit ist es vorteilhaft, die automatische Weiterleitung an andere Mailboxen des Betriebes und/oder eine automatische Antwortnachricht Abwesenheit vom Dienst/*Out of Office* zu verwenden, in der erwähnt wird, wer innerhalb der Einrichtung die Aufgaben während der Abwesenheit übernimmt, oder eine alternative E-Mail-Adresse, auch vom Typ Sammeladresse, wie z. B. AmtX@sozialbetrieb.bz.it anzugeben (siehe Anlage Nr. 1).

2. Bei plötzlicher oder längerer Abwesenheit und bei unvorhersehbaren Erfordernissen im Zusammenhang mit der Arbeitstätigkeit, wenn es nicht möglich ist, die Funktion der automatischen Antwort oder der automatischen Weiterleitung an andere Mailboxen der Einrichtung zu aktivieren, und es notwendig ist, den Inhalt der E-Mail-

casella di posta può delegare l'amministratore di sistema (cd fiduciario/a) per verificare il contenuto di messaggi e per inoltrare al(la responsabile di settore quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa (cfr. allegato n. 2). Sarà compito dello stesso assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore/la lavoratrice interessato/a alla prima occasione utile (cfr. allegato n. 3). È possibile l'accesso alla propria casella di posta elettronica da qualsiasi dispositivo connesso a *internet* e dotato di *browser*.

Nachrichten zu kennen, kann der Eigentümer der Mailbox den Systemadministrator (sog. Treuhänder) damit beauftragen, den Inhalt der Nachrichten zu überprüfen und diejenigen an den Verwalter des Sektors weiterzuleiten, die für die Ausübung der Arbeitstätigkeit als relevant angesehen werden (siehe Anhang Nr. 2). Es ist Aufgabe des Treuhänders, dafür zu sorgen, dass ein Protokoll erstellt wird, in dem die Vorkommnisse festgehalten werden, und dass der betroffene Arbeitnehmer so schnell wie möglich informiert wird (siehe Anhang Nr. 3). Es ist möglich von jedem Gerät aus, das mit dem Internet verbunden und mit einem *Browser* ausgestattet ist, auf die Mailbox zuzugreifen.

3. Qualora, in caso di assenza improvvisa o prolungata - programmata o meno - e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, il lavoratore/la lavoratrice deve delegare, anche preventivamente, l'amministratore di sistema (cd fiduciario/a) a verificare il contenuto dei messaggi e ad inoltrare al/la titolare del trattamento, rappresentata legalmente dalla Direzione Generale di ASSB, o suo delegato, quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

3. Sollte es bei plötzlichen oder verlängerten, geplanten und nicht geplanten Abwesenheiten unbedingt notwendig sein, aus Arbeitsgründen in den Inhalt von E-Mails Einsicht zu nehmen, müssen die Bediensteten auch vorab den Systemadministrator (Treuhänder) dazu ermächtigen, in die E-Mails Einsicht zu nehmen und diejenigen Nachrichten an den Rechtsinhaber der Verarbeitung, gesetzlich vertreten durch die Generaldirektion des BSB oder seinen Stellvertreter, weiterzuleiten, die für die Arbeitstätigkeiten als relevant eingestuft werden.

4. Il/la fiduciario/a provvederà a verbalizzare tale attività e a informare il lavoratore/la lavoratrice interessato/a alla prima occasione utile.

4. Der Treuhänder muss über diese Tätigkeit Protokoll führen und die betroffenen Bediensteten bei der ersten Gelegenheit darüber in Kenntnis setzen.

5. In caso di cessazione del rapporto lavorativo, la *mail* dell'ente affidata all'incaricato verrà bloccata per un periodo di 6 mesi e successivamente eliminata. Nel periodo di sospensione, l'account rimarrà attivo e visibile a un soggetto incaricato dall'ASSB solo in

5. Im Falle der Beendigung des Arbeitsverhältnisses wird die dem Beauftragten anvertraute Unternehmens-E-Mail für einen Zeitraum von 6 Monaten gesperrt und anschließend gelöscht. Während des Zeitraums der Sperrung bleibt das Konto aktiv und nur für eine von BSB

ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'ente, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema, in ogni caso, genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail dell'ASSB.

für den Empfang benannte Person sichtbar, die die erhaltenen Daten und Informationen für organisatorische und produktionstechnische Erfordernisse, für die Arbeitssicherheit und für den Schutz des Eigentums des Betriebes verarbeitet und die Inhalte an andere Mitarbeiter/innen weiterleitet (wenn die Nachricht einen Arbeitsinhalt hat) oder löscht (wenn die Nachricht keinen Arbeitsinhalt hat). In jedem Fall generiert das System eine automatische Antwort an den Absender mit der Aufforderung, die Nachricht erneut an eine andere BSB-E-Mail-Adresse zu senden.

6. Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/2016.

6. Die eventuell gesammelten Informationen sind auch für alle Zwecke im Zusammenhang mit dem Arbeitsverhältnis verwendbar, einschließlich der Überprüfung der Einhaltung dieser Vorschriften, was angemessene Informationen über die Methoden der Verwendung der Arbeitsmittel und die Durchführung von Kontrollen gemäß der europäischen Verordnung 2016/679 darstellt.

Art. 17
***Disclaimer* di posta**

1. I messaggi di posta elettronica dovranno contenere un avvertimento ai destinatari (*disclaimer* di posta) nel quale venga dichiarata la natura non personale della comunicazione stessa, ma con la specifica precisazione circa la possibilità di conoscenza del suo oggetto nell'ambito dell'organizzazione di appartenenza del mittente e del destinatario. (cfr. allegato n. 4)

Art. 17
E-mail Verwaltungsausschuss
(Disclaimer)

1. Alle E-Mails müssen eine Warnung für die Empfänger enthalten (Verwaltungsausschluss oder sogenannter *Disclaimer*), in der die nicht persönliche Natur der Nachricht angegeben und spezifisch die Möglichkeit der Kenntnisnahme ihres Inhalts von Seiten der Organisation des Absenders und des Empfängers definiert wird (siehe Anhang Nr. 4).

Art. 18
Proprietà dei sistemi

1. Tutte le informazioni archiviate negli elaboratori e nei sistemi di comunicazione aziendali (inclusi

Art. 18
Eigentum der Systeme

1. Alle Informationen in den Archiven der Rechner und in den Kommunikationssystemen des BSB

documenti, altri file, messaggi di posta elettronica) sono di proprietà dell'ente.

2. Ciò vale anche per la posta elettronica di tutti gli *account* con suffisso @aziendasociale.bz.it (es. nome.cognome@aziendasociale.bz.it) che, in quanto equiparata alla corrispondenza epistolare, rappresenta una forma di comunicazione equipollente a quella su carta intestata.

3. Gli/le utenti di rete devono quindi essere consapevoli che tutte le comunicazioni inviate o ricevute mediante i sistemi di posta elettronica aziendale per finalità di lavoro sono di proprietà di ASSB e devono essere considerate informazioni di carattere non riservato nei confronti del datore di lavoro.

Art. 19
Modalità e precauzioni per l'utilizzo della posta elettronica da parte del/la dipendente

1. L'attribuzione degli *account* di posta elettronica è fornita per un uso esclusivamente professionale. Gli/le utenti di rete:
a) sono tenuti/e a utilizzare i sistemi di posta elettronica esclusivamente per condurre affari istituzionali ufficiali, nonché per comunicazioni in ogni caso correlate agli affari condotti dall'ente. Non possono essere utilizzati tali sistemi per scopi personali;
b) non possono tassativamente mai utilizzare i sistemi di posta istituzionale per creare o trasmettere materiale con contenuti sessuali espliciti, denigratori, diffamatori, osceni o offensivi, quali, a titolo esemplificativo, insulti, epiteti ovvero qualsiasi altro contenuto o testo che possa essere

(einschl. Dokumente, andere Dateien, E-Mails, und Aufzeichnungen von Sprachnotizen) sind Eigentum des BSB.

2. Dies gilt auch für die E-Mails aller Nutzerkonten (*„Accounts"*) mit dem Suffix „@sozialbetrieb.bz.it" (z.B. Name.Nachname@ozialbetrieb.bz.it), da diese dem gewöhnlichen Briefverkehr gleichzustellen sind und demnach in jeder Hinsicht als Kommunikation auf Briefpapier des BSB gelten.

3. Die Nutzer/innen müssen sich der Tatsache bewusst sein, dass mit E-Mails empfangene und verschickte Nachrichten aus Arbeitsgründen ebenfalls Eigentum des BSB sind und vom Arbeitgeber als *„nicht vertraulich"* eingestuft werden.

Art. 19
Modalitäten und Vorsichtsmassnahmen für die Benutzung der E_Mails von Seiten der Bediensteten

1. Die Zuteilung von Accounts zur Benutzung der betrieblichen E-Mail erfolgt ausschließlich aus beruflichen Zwecken.
Die Nutzer/innen:
a) sind dazu angehalten, die E-Mails ausschließlich zur Führung von offiziellen und institutionellen Geschäften und zur Führung des Briefverkehrs zu benutzen, der auf alle Fälle mit den Geschäften des BSB zusammenhängen muss. Die Bediensteten dürfen die E-Mails nicht für persönliche Zwecke benutzen;
b) dürfen die institutionellen E-Mails nicht für die Schaffung oder Entsendung von Materialien mit explizit sexuellem, verleumderischem, obszönem oder beleidigendem Inhalt wie z.B. mit Beleidigungen, Schimpfnamen oder einem anderen Inhalt bzw. Text benutzen, der als Belästigung oder Diskriminierung aufgrund der Rasse, Hautfarbe, Staatsbürgerschaft,

considerato una molestia ovvero una discriminazione fondata sull'origine razziale, il colore della pelle, la nazionalità, il sesso, le preferenze sessuali, l'età, le infermità fisiche o psichiche, lo stato di salute, lo stato civile, le convinzioni politiche o religiose;
c) sono comunque responsabili in via esclusiva del contenuto di messaggi, file di testo, immagini, file audio da essi pubblicati o trasmessi attraverso i sistemi di posta elettronica;
d) non possono utilizzare i sistemi di posta elettronica aziendali per inviare o ricevere materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie o altro materiale appartenente ad organizzazioni diverse da ASSB, salvo per l'esecuzione di attività di natura professionale. A tal fine, la mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre alle azioni disciplinari previste dal capo ultimo del presente regolamento ovvero ad azioni legali da parte dei legittimi titolari del diritto d'autore.

des Geschlechts, der sexuellen Neigung, des Alters, der körperlichen oder geistigen Beeinträchtigungen, des Gesundheitszustands, des Familienstands, der politischen oder religiösen Überzeugungen eingestuft werden kann;
c) sind auf alle Fälle alleinig für den Inhalt von Nachrichten, Textdateien, Bildern, Audiodateien verantwortlich, die von ihnen veröffentlicht oder durch E-Mails übermittelt werden;
d) dürfen die betrieblichen E-Mails nicht für den Empfang oder die Entsendung von urheberrechtlich geschützten Materialien, von Geschäftsgeheimnissen, von finanziellen und eigentumsrechtlichen Informationen oder von anderen Materialien benutzen, die Eigentum von betriebsexternen Subjekten sind, außer wenn dies für die Erledigung von Arbeitstätigkeiten notwendig ist. In diesem Zusammenhang wird darauf hingewiesen, dass die Missachtung des Urheberrechts oder von Lizenzverträgen zur Verhängung von Disziplinarmaßnahmen gemäß letztem Abschnitt der vorliegenden Benutzungsordnung und zu Rechtshandlungen von Seiten der rechtmäßigen Inhaber des Urheberrechtes führen kann.

2. Tutti i/le dipendenti, collaboratori/collaboratrici, anche nell'ambito dell'utilizzo della posta elettronica di ASSB, sono comunque tenuti/e a prestare particolare cautela nel trattamento dei dati personali e particolari ai quali sono preposti nel pieno rispetto del D. Lgs. n. 196/2003 e ss.mm.ii., delle Linee guida incaricati di ASSB e del presente regolamento. Gli/le stessi/e si impegnano ad adottare ogni precauzione necessaria per evitare ed escludere il trattamento, la comunicazione e/o la diffusione di dati personali e/o particolari

2. Alle Bediensteten und Mitarbeiter/innen sind - auch bei der Benutzung der betrieblichen E-Mails - dazu angehalten, im Rahmen der Verarbeitung von personenbezogenen und sensiblen Daten gemäß gesetzesvertretendem Dekret Nr. 196/2003 i.g.F. der betrieblichen Richtlinien für Beauftragte und der vorliegenden Benutzungsordnung besondere Sorgfalt walten zu lassen. Die Bediensteten und Mitarbeiter/innen müssen alle Vorbeugemaßnahmen ergreifen, um die Verarbeitung, Übermittlung und/oder Verbreitung von personenbezogenen

non necessari per l'espletamento delle proprie competenze istituzionali.

3. A tal fine, salvo casi eccezionali e urgenti, gli stessi devono fare tutto il possibile per evitare l'inoltro, a mezzo *mail*, se non in modalità protetta (cifrata), di allegati contenenti dati particolari. L'utilizzo della casella di posta relativa al sistema di archiviazione D3 è da ritenersi la modalità corretta e normale di inoltro dei documenti interni, come prescritto dal manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi di ASSB.

4. È vietato l'invio di materiale di proprietà di ASSB a caselle di posta elettronica personali o a destinatari terzim non necessario nello svolgimento delle attività lavorative.

5. Nel pieno rispetto dell'art. 2 dell'accordo di comparto per i dipendenti dei Comuni, delle Comunità Comprensoriali e delle A.P.S.P. del 14.10.2013 e ss.mm.ii., il flusso di informazioni tra le organizzazioni sindacali e gli enti nonché dalle organizzazioni sindacali ai dipendenti viene assicurato anche a mezzo *e-mail* ai rispettivi indirizzi di posta elettronica.

und/oder sensiblen Daten zu verhindern, die nicht strikt für die jeweils zugeteilten Arbeitstätigkeiten notwendig sind.

3. Zu diesem Zweck müssen die Bediensteten/Mitarbeiter/innen - unbeschadet etwaiger Ausnahmen und Dringlichkeiten - alle Maßnahmen ergreifen, damit über E-Mails keine Anhänge mit sensiblen Daten weitergeleitet werden, sofern diese nicht verschlüsselt sind. Die Nutzung der Mailbox im Zusammenhang mit dem D3-Ablagesystem ist als korrekte und normale Art der Weiterleitung interner Dokumente anzusehen, wie sie im Handbuch für die Verwaltung von Computerprotokollen, Dokumentenflüssen und Archiven von BSB vorgeschrieben ist.

4. Es ist verboten, Material, das BSB gehört, an persönliche E-Mail-Postfächer oder an Dritte zu senden, die nicht für die Ausübung der Arbeitstätigkeit notwendig sind.

5. In voller Beachtung des Art. 2 des Bereichsabkommens für die Bediensteten der Gemeinden, Bezirksgemeinschaften und ÖBPB vom 14.10.2013 i.g.F. kann der Informationsfluss zwischen den Gewerkschaftsorganisationen und den Körperschaften sowie von den Gewerkschaften an die Bediensteten auch mittels E-Mail erfolgen.

CAPO IV

UTILIZZO DELLA RETE *INTERNET*

Art. 20
Ambito di applicazione

1. L'accettazione e la stretta osservanza delle prescrizioni che seguono sono condizioni essenziali per l'ottenimento e l'attribuzione in uso del servizio di accesso a *internet* mediante IP pubblici

ABSCHNITT IV

INTERNET NUTZUNG

Art. 20
Anwendungsbereich

1. Die Annahme und strikte Einhaltung der folgenden Anforderungen sind wesentliche Voraussetzungen für die Erlangung und Nutzung des Dienstes des Zugangs zum Internet über öffentliche IP, die der

attribuiti alla responsabilità dell'ente.

Verantwortung des Betriebs zugewiesen sind.

Art. 21
Responsabilità

1. L'accesso alla rete *internet* è fornito al personale di ASSB a beneficio dell'intera Azienda.

2. Tutti gli/le utenti di rete sono, quindi, responsabili dell'applicazione rigorosa del presente regolamento.

3. Il Direttore/la Direttrice competente ha l'obbligo di vigilare, ai sensi dell'art. 4, L. n. 300/1970 (Statuto dei lavoratori), sul rispetto della procedura, indicata nel presente capo, da parte di tutto il personale preposto al proprio ufficio.

Art. 21
Verwaltung

1. Der Internetzugang wird den Betriebsbediensteten zum Vorteil des gesamten BSB zugeteilt.

2. Alle Nutzer sind demnach für die strikte Einhaltung der vorliegenden Verordnung verantwortlich und haften dafür.

3. Die zuständigen Führungskräfte haben gemäß Art. 4 des Gesetzes vom 20. Mai 1970, Nr. 300 (Arbeiterstatut) die Pflicht, die Einhaltung der Vorgaben in diesem Abschnitt der Benutzungsordnung von Seiten der jeweils untergeordneten Bediensteten zu beaufsichtigen.

Art. 22
Accesso e utilizzo di *internet*

1. Gli utenti hanno accesso alla rete *internet*, nei limiti di quanto agli stessi consentito esclusivamente per ragioni professionali e durante l'orario di lavoro.

2. Inoltre:

a) è vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'ente (introduzione di virus informatici), ad esempio, il *download* o l'*upload* di *file* audio e/o video e l'uso di servizi di rete estranei all'attività lavorativa;
b) è vietato a chiunque il *download* di qualunque tipo di *software* gratuito (*freeware*) o *shareware* prelevato da siti *internet,* se non

Art. 22
Zugang zum *Internet* und Benutzung

1. Die Nutzer/innen haben - im Rahmen der ihnen zugeteilten Befugnisse - ausschließlich aus Arbeitsgründen und während der Arbeitszeiten Zugang zum Internet.

2. Außerdem:

a) ist es verboten, Handlungen auszuführen, die potenziell in der Lage sind, dem Betrieb Schaden zuzufügen (Einschleusen von Computerviren), z. B. *download* oder *upload* von Audio- und/oder Videodateien und die Nutzung von Netzwerkdiensten, die nicht mit der Arbeitstätigkeit zusammenhängen;
b) das Herunterladen von kostenloser Software *(Freeware)* oder *Shareware* jeglicher Art von Internet-Seiten ist verboten, es sei denn, es liegt eine

espressamente autorizzato dal CED,

c) é vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di *remote banking*, acquisti *on-line* e simili, a fini estranei all'attività dell'ente.

d) non possono utilizzare i sistemi di posta elettronica aziendali per inviare o ricevere materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie o altro materiale appartenente ad organizzazioni diverse da ASSB, salvo per l'esecuzione di attività di natura professionale. A tal fine, la mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre alle azioni disciplinari previste dal capo ultimo del presente regolamento ovvero ad azioni legali da parte dei legittimi titolari del diritto d'autore.

3. L'ente non effettua la memorizzazione sistematica delle pagine *web* visualizzate dal singolo utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

4. Tuttavia al fine di garantire il servizio *internet* e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio di ASSB, l'ente registra per 7 giorni i dati di navigazione (*file* di *log* riferiti al traffico *web*) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di utenti, mediante opportune aggregazioni.

5. Solo in casi eccezionali e di

ausdrückliche Genehmigung von der EDV-Dienststelle vor,

c) es ist verboten, jegliche Art von Finanztransaktionen, einschließlich *remote banking*, Online-Einkäufe und ähnliches, für Zwecke durchzuführen, die nicht mit der Tätigkeit des Betriebes in Zusammenhang stehen.

d) dürfen die E-Mail-Systeme des Betriebes nicht verwenden, um urheberrechtlich geschütztes Material, Geschäftsgeheimnisse, geschützte Finanzinformationen oder anderes Material, das anderen Organisationen als BSB gehört, zu versenden oder zu empfangen, es sei denn, es handelt sich um die Ausübung von Tätigkeiten professioneller Natur. Zu diesem Zweck kann die Nichteinhaltung von Urheberrechts- oder Lizenzvereinbarungen zu disziplinarischen Maßnahmen gemäß dem letzten Kapitel dieser Vorschriften oder zu rechtlichen Schritten seitens der rechtmäßigen Urheberrechtsinhaber führen.

3. Der Betrieb speichert weder systematisch die vom einzelnen Nutzer betrachteten Webseiten, noch überprüft er die Navigationsdaten des Nutzers mit automatischen Systemen.

4. Zur Gewährleistung des Internetdienstes und der Sicherheit der Informationssysteme sowie aus organisatorischen und produktionstechnischen Erfordernissen, zur Arbeitssicherheit und zum Schutz des Eigentums von BSB speichert der Betrieb jedoch 7 Tage lang Navigationsdaten (Logfiles, die sich auf den Webverkehr beziehen) mit Methoden, die zunächst darauf abzielen, die unmittelbare und direkte Identifizierung der Nutzer auszuschließen, durch angemessene Aggregationen.

5. Nur in Ausnahmefällen und bei

comprovata urgenza rispetto alle finalità sopra descritte, l'Azienda può trattare i dati di navigazione, riferendoli specificatamente ad un singolo nome utente.

nachgewiesener Dringlichkeit in Bezug auf die oben beschriebenen Zwecke kann der Betrieb Navigationsdaten verarbeiten, die sich speziell auf einen einzelnen Nutzernamen beziehen.

Art 23
Utilizzo dei telefoni, cellulari, fax, fotocopiatrici, *scanner* e stampanti

1. Gli strumenti di stampa così come anche il telefono in dotazione sono di proprietà di ASSB e sono resi disponibili all'utente esclusivamente per rendere la prestazione lavorativa.

2. Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa.

3. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità e urgenza.

4. Qualora sia assegnato da parte dell'ente un cellulare all/alla utente, l'utilizzo e la custodia saranno sotto la sua responsabilità.

5. Particolare attenzione dovrà essere prestata nella ricezione di sms, *chat* o altre comunicazioni immediatamente visibili sullo schermo che, se contenenti dati personali o particolari, potrebbero essere visibili da persone che si trovino nelle vicinanze dell'apparecchio.

6. Il cellulare non deve essere mai affidato ad altri e deve essere protetto da *password* o altro sistema di sicurezza affinchè nessuno possa accedere ad

Art. 23
Nutzung von Telefonen, *Handys*, Faxgeräten, Kopierern, Scannern und Druckern

1. Die Druckergeräte sowie das mitgelieferte Telefon sind Eigentum von BSB und werden dem Nutzer ausschließlich zum Zwecke der Erbringung der Arbeitsleistung zur Verfügung gestellt.

2. Das dem Nutzer anvertraute Telefon ist ein Arbeitsmittel. Die Nutzung des Telefons wird ausschließlich für die Ausübung der Arbeitstätigkeit gewährt und daher sind persönliche Kommunikationen, die nicht strikt mit der Arbeitstätigkeit selbst zusammenhängen, nicht erlaubt.

3. Die Entgegennahme oder Ausführung von Mitteilungen persönlicher Natur ist nur in Fällen nachgewiesener Notwendigkeit und Dringlichkeit zulässig.

4. Wenn die Institution dem Nutzer ein Mobiltelefon zuweist, ist der/die Nutzer/in für dessen Verwendung und Aufbewahrung verantwortlich.

5. Besondere Vorsicht ist beim Empfang von Textnachrichten, Chats oder andere Mitteilungen geboten, die unmittelbar auf dem Bildschirm sichtbar sind und die, wenn sie persönliche oder sensible Daten enthalten, von Personen in der Nähe des Geräts gesehen werden könnten.

6. Das Mobiltelefon darf niemals anderen anvertraut werden und muss durch ein Passwort oder ein anderes Sicherheitssystem geschützt werden, damit

informazioni, rubriche, e-mail o sms relativi alla sfera lavorativa.

niemand auf Informationen, Adressbücher, E-Mails oder Textnachrichten zugreifen kann, die die Arbeit betreffen.

7. Ai telefoni, fax, fotocopiatrici, *scanner* e stampanti dell'ente si applicano le medesime regole previste per gli altri dispositivi informatici, per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica.

7. Für die Telefone, Faxgeräte, Fotokopierer, Scanner und Drucker des Betriebes gelten hinsichtlich der Aufrechterhaltung eines angemessenen Informatiksicherheitsniveaus die gleichen Regeln wie für andere Informatikgeräte.

8. Per *smartphone* e *tablet* dell'ente è vietata l'installazione e l'utilizzo di applicazioni diverse da quelle autorizzate.

8. Die Installation und Nutzung von anderen als den autorisierten Anwendungen ist für die Smartphones und Tablets des Betriebes untersagt.

9. È vietato l'utilizzo delle fotocopiatrici dell'ente per fini personali.

9. Die Nutzung der Fotokopierer des Betriebes für persönliche Zwecke ist verboten.

10. Per quanto concerne l'uso delle stampanti, gli/le utenti sono tenuti ad adoperare due alternative modalità d'utilizzo:
a) stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
b) prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (*toner* e altri consumabili).

10. Was die Verwendung von Druckern betrifft, so müssen die Nutzer diese auf zwei alternative Arten verwenden:
a) Dokumente nur drucken, wenn dies für die Erfüllung ihrer betrieblichen Aufgaben unbedingt erforderlich ist;
b) die gemeinsam genutzten Netzwerkdrucker gegenüber lokalen/persönlichen Druckern bevorzugen, um den Verbrauch von Verbrauchsmaterialien (Toner und andere Verbrauchsmaterialien) zu reduzieren.

11. Nel caso in cui si rendesse necessaria la stampa di informazioni riservate o dati particolari, l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

11. Für den Fall, dass es notwendig wird, vertrauliche Informationen oder sensible Daten auszudrucken, muss der Nutzer das Druckgerät bewachen, um den möglichen Verlust oder die Weitergabe solcher Informationen an unbefugte Dritte zu verhindern.

Art. 24
Assistenza agli utenti e manutenzioni

Art. 24
Technischer Beistand an die Nutzer/innen und Wartung

1. Il CED e le aziende incaricate di effettuare attività di manutenzione sul

1. Die EDV-Dienststelle und die mit der Wartung von Software und Systemen im

software e sui sistemi in generale, possono accedere ai dispositivi informatici dell'ente sia direttamente, sia mediante *software* di accesso remoto, per i seguenti scopi:

• verifica e risoluzione di problemi sistemistici ed applicative, su segnalazione dell'utente finale
• verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete
• richieste di aggiornamento *software* e manutenzione preventiva di *hardware* e *software.*

Allgemeinen beauftragten Unternehmen können zu folgenden Zwecken entweder direkt oder über eine Fernzugriffssoftware auf die Informatikgeräte des Betriebes zugreifen:
- Überprüfung und Behebung von System- und Anwendungsproblemen, nach Angabe des Endnutzers;
- Überprüfung der korrekten Funktion der einzelnen Geräte bei festgestellten Problemen im Netzwerk;
- Anfragen für Software-Aktualisierungen und vorbeugende Wartung von Hardware und Software.

2. Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, i soggetti sopra indicati sono autorizzati a effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

2. Technische Eingriffe können mit Zustimmung des Nutzers erfolgen, wenn der Eingriff selbst den Zugriff auf die persönlichen Bereiche des Nutzers erfordert. Wenn der technische Eingriff vor Ort oder aus der Ferne keinen Zugang durch Nutzerzugangsdaten erfordert, sind die oben genannten Subjekte berechtigt, die Eingriffe ohne Zustimmung des Nutzers, dem die Ressource zugewiesen ist, durchzuführen.

3. L'accesso in teleassistenza sulle pdl della rete dell'ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'ente e soggetto alle verifiche, da parte del CED, delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

3. Der von Dritten (Lieferanten und/oder anderen) beantragte Fernzugriff auf die Arbeitsplätze des Betriebsnetzwerks muss vom Betrieb genehmigt werden und unterliegt der Überprüfung der Eingriffsverfahren für den ersten Zugriff durch die EDV-Dienststelle. Nachfolgende Anfragen, die auf die gleiche Weise gestellt werden, können vom Endnutzer selbständig verwaltet werden.

4. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o un suo delegato deve presenziare alla sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento e assicurarsi della corretta disconnessione al termine

4. Bei Fernwartungseingriffen durch Drittbetreiber muss der anfragende Nutzer oder sein Delegierter während der Fernwartungssitzung anwesend sein, um ein nicht regelkonformes Verhalten zu überprüfen und zu verhindern sowie die korrekte Abschaltung der Verbindung am Ende des Eingriffs sicherzustellen.

dell'intervento.

CAPO V

CONTROLLI E GARANZIE

Art. 25
Controlli

1. Il Regolamento UE 2016/679 pone l'accento sulla responsabilizzazione di titolari e responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento UE. Viene affidato ai/alle titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e di alcuni criteri specifici indicati nel Regolamento UE 2016/679.

2. Ai sensi e per gli effetti del D. Lgs. n. 196/2003 e dell'ulteriore normativa vigente, ASSB è obbligata a effettuare periodicamente controlli e ispezioni sul rispetto delle prescrizioni del presente regolamento.

3. I documenti o messaggi di posta elettronica recanti la dicitura *riservato* sono inaccessibili alla maggior parte degli/delle utenti, ma rimangono nella disponibilità dell'organizzazione.

4. La cancellazione di un documento o di un messaggio non può impedire il diritto di ispezione da parte di ASSB ovvero la definitiva eliminazione del documento o del messaggio dal sistema, qualora quest'ultimo risultasse dannoso per l'ente.

ABSCHNITT V

KONTROLLEN UND GARANTIEN

Art. 25
Kontrollen

1. Die EU-Verordnung 2016/679 legt den Schwerpunkt auf die Befähigung der Rechtsinhaber der Datenverarbeitung und der Verantwortlichen, d. h. auf die Annahme proaktiver Verhaltensweisen, die die konkrete Annahme von Maßnahmen zur Sicherstellung der Anwendung der EU-Verordnung belegen sollen. Den Rechtsinhabern der Datenverarbeitung wird die Aufgabe übertragen, autonom über die Modalitäten, Garantien und Grenzen derVerarbeitung personenbezogener Daten zu entscheiden, unter Einhaltung der gesetzlichen Bestimmungen und einiger spezifischer Kriterien, die in der EU-Verordnung 2016/679 angegeben sind.

2. Gemäß und im Sinne des Gesetzesdekrets Nr. 196/2003 und anderer geltender Vorschriften ist BSB verpflichtet, regelmäßige Kontrollen und Überprüfungen der Einhaltung der Bestimmungen dieser Verordnung durchzuführen.

3. Dokumente oder E-Mail-Nachrichten mit dem Vermerk "*Vertraulich"* sind für die meisten Nutzer unzugänglich, bleiben aber für den Betrieb verfügbar.

4. Die Löschung eines Dokuments oder einer Nachricht kann das Recht auf Einsichtnahme durch BSB oder die endgültige Beseitigung des Dokuments oder der Nachricht aus dem System nicht verhindern, sollte sich letztere als schädlich für den Betrieb erweisen.

Art. 26
Modalità

1. È vietata ogni attività finalizzata al monitoraggio automatizzato e continuativo delle attività del lavoratore.

2. L'accesso ai *log (*cfr. art.12, comma 14, del presente regolamento*)* e ai contenuti dei sistemi di posta elettronica e *internet*, consentito nel pieno rispetto del già citato provvedimento dell'Autorità garante per la protezione dei dati personali n. 13 del 01.03.2007 e successive modifiche, è permesso solo ed esclusivamente nei seguenti casi:

- richiesta dell'Autorità Giudiziaria;
- richiesta dell'Autorità di Pubblica Sicurezza;
- attività ispettive preventive e/o difensive di eventuali organi/ Autorità di vigilanza;
- soluzione di incidenti informatici o telematici;
- esigenze di continuità operativa (recupero dati in caso di assenza prolungata dell'interessato), come da capo III del presente regolamento.

3. Ogni richiesta di accesso ai *log,* nei termini sopra indicati, dovrà essere preventivamente autorizzata da parte della Direzione Generale di ASSB.

4. Ai sensi del provvedimento dell'Autorità garante per la protezione dei dati personali n. 13 dd. 01.03.2007 e successive modifiche, è comunque attivo un sistema di archiviazione dell'accesso al sistema di posta elettronica. I *file* di *log* vengono aggiornati giornalmente e sono disponibili per 3 giorni di *retention time* e non vengono archiviati nel sistema di *backup*.

Art. 26
Modalitäten

1. Jede Tätigkeit, die auf eine automatisierte und kontinuierliche Überwachung der Tätigkeiten des Arbeitnehmers abzielt, ist verboten.

2. Der Zugang zu den Logs (siehe Art. 12, Abs. 14 dieser Verordnung) und zu den Inhalten der E-Mail- und Internetsysteme, der in voller Übereinstimmung mit der bereits erwähnten Bestimmung der Garantiebehörde für den Schutz der persönlichen Daten Nr. 13 vom 01.03.2007 i.g.F. erlaubt ist, ist nur und ausschließlich in den folgenden Fällen erlaubt:

- Anforderung von Seiten der Gerichtsbehörden;
- Anforderung von Seiten der öffentlichen Sicherheitsbehörden;
- Inspektionstätigkeiten zur Vorbeugung und/oder zur Verteidigung eventueller Aufsichts- und Kontrollbehörden;
- Überwindung von Informatik- und Kommunikationsstörungen;
- Bedürfnisse im Zusammenhang mit der Tätigkeitskontinuität (Rückgewinnung/Wiederherstellung der Daten bei verlängerter Abwesenheit des Betroffenen) gemäß Abschnitt III der vorliegenden Verordnung.

3. Jeder Antrag auf Zugang zu den Logs gemäß den oben beschriebenen Sachverhalten muss vorab von der Generaldirektion genehmigt werden.

4. Gemäß der Maßnahme der Datenschutzbehörde Nr. 13 vom 1.03.2007 i.g.F. wurde ein System zur Archivierung der Zugänge zu den E-Mails aktiviert. Die Log - Dateien werden täglich aktualisiert und stehen für drei Tage (*Retention Time* = 3 Tage) zur Verfügung. Die Log - Dateien werden nicht im Backup - System archiviert.

Art 27
Informazioni generali in merito ai controlli

1. Nel rispetto del provvedimento del Garante per la protezione dei dati personali n. 13 dd. 01.03.2007 e successive modifiche, nonché dell'art. 4 della Legge n. 300/1970, come novellato dall'art. 23, comma 1, del D. Lgs. 14.09.2014, n. 151 (cd. *Jobs Act*) e del Regolamento UE 2016/679, in caso di controlli in merito al rispetto delle regole aziendali e dovuti a esigenze di continuità, il lavoratore/la lavoratrice interessato/a dovrà essere preventivamente informato/a.

2. ASSB ha predisposto il proprio sistema informativo e *internet* per esclusive esigenze organizzative e/o produttive. A tal fine, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi e/o attività – anche discontinue - che consentono indirettamente un controllo a distanza (controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori/alle lavoratrici.

3. Le attività di controllo potranno essere esercitate nel caso in cui si rivelino anomalie di funzionamento o si rendano necessarie attività di manutenzione o, comunque, in tutte le ipotesi in cui sia a rischio la sicurezza dei beni aziendali e/o la sicurezza sul lavoro in generale.

4. Nell'espletare controlli e verifiche dovrà essere garantita la massima riservatezza dei dati conosciuti, anche incidentalmente, in occasione della verifica, pena l'applicazione di sanzioni

Art. 27
Allgemeine Informationen hinsichtlich der Kontrollen

1. In Übereinstimmung mit der Vorschrift des Garanten für den Schutz personenbezogener Daten Nr. 13 vom 01.03.2007, sowie mit Art. 4 des Gesetzes Nr. 300/1970, erneuert durch Art. 23, Abs. 1, des Gesetzesdekrets 14.09.2014, Nr. 151 (sog. *Jobs Act*) und der EU-Verordnung 2016/679, muss im Falle von Kontrollen der Einhaltung der Unternehmensregeln und aufgrund von Kontinuitätserfordernissen der betroffene Mitarbeiter im Voraus informiert werden.

2. BSB hat sein Informations- und Internetsystem für ausschließliche organisatorische und/oder produktionstechnische Anforderungen eingerichtet. Zu diesem Zweck bedient er sich in Übereinstimmung mit dem Arbeitnehmerstatut (Art. 4, Abs. 2) legitimerweise an Systemen und/oder Aktivitäten - auch diskontinuierlich -, die indirekt eine Fernsteuerung (präintentionale Kontrolle) ermöglichen und die Verarbeitung personenbezogener Daten, die sich auf Arbeitnehmer beziehen oder beziehen können, bestimmen.

3. Kontrolltätigkeiten können durchgeführt werden, wenn Betriebsanomalien aufgedeckt werden oder Wartungsarbeiten erforderlich sind, oder in jedem Fall in allen Fällen, in denen die Sicherheit von Unternehmenseigentum und/oder die Sicherheit am Arbeitsplatz im Allgemeinen gefährdet ist.

4. Bei der Durchführung von Kontrollen und Inspektionen muss unter Androhung disziplinarischer Sanktionen je nach Schwere des Vorfalls, die größtmögliche Vertraulichkeit der bei der Inspektion auch

disciplinari in base alla gravità dell'accaduto, ferma restando ogni altra ulteriore responsabilità.

nur zufällig bekannt gewordenen Daten gewährleistet werden, unbeschadet jeglicher sonstiger Verwaltung.

5. I dati potranno essere comunicati solo ed esclusivamente a soggetti interni o esterni all'organizzazione aziendale per i quali la comunicazione sia necessaria in relazione alle finalità perseguite con l'accesso (per esempio, nei casi indicati, alle Forze dell'ordine, a incaricati di funzioni aziendali preposte alle azioni legali o alla soluzione dei problemi tecnici).

5. Die Daten dürfen nur und ausschließlich an Subjekte innerhalb oder außerhalb der Betriebsorganisation weitergegeben werden, für die die Weitergabe im Zusammenhang mit dem Zugang verfolgten Zwecken notwendig ist (zum Beispiel in den angegebenen Fällen an die Polizei, an Beauftragte von Betriebsfunktionen, die für rechtliche Schritte oder die Lösung technischer Probleme zuständig sind).

Art. 28
Controlli sugli strumenti

1. In riferimento all'art. 6.1 del provvedimento del Garante per la protezione dei dati personali n. 13 dd. 01.03.2007 e successive modifiche, a integrazione dell'informativa prevista dall'art. 13 del Regolamento UE 2016/679, in caso di violazioni contrattuali e/o giuridiche, sia ASSB, sia il/la singolo/a utente e/o videoterminalista, sono potenzialmente perseguibili con sanzioni, anche di natura penale.

Art. 28
Kontrolle über die Arbeitsmittel

1. Unter Bezugnahme auf Art. 6.1 der Bestimmung des Garanten für den Schutz personenbezogener Daten Nr. 13 vom 01.03.2007 i.g.F., als Ergänzung zu den Informationen von Art. 13 der EU-Verordnung 2016/679, können sowohl BSB als auch dem einzelne Nutzer und/oder Video-Terminalist im Falle von vertraglichen und/oder gesetzlichen Verstößen Sanktionen, einschließlich strafrechtlicher Sanktionen, auferlegt werden.

2. ASSB verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto del presente regolamento e l'integrità del proprio sistema informatico.

2. BSB wird im Rahmen der gesetzlichen und vertraglichen Bestimmungen die Einhaltung dieser Verordnung und die Integrität seines Computersystems überprüfen

3. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori/lavoratrici e delle organizzazioni sindacali in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività

3. Die Verfahren zur Unterrichtung und Anhörung von Arbeitnehmern und Gewerkschaften im Zusammenhang mit der Einführung oder Änderung von automatisierten Systemen zur Sammlung und Nutzung von Daten sowie im Falle der Einführung oder Änderung von technischen Verfahren zur Kontrolle der Bewegungen oder der Produktivität von Arbeitnehmern müssen weiterhin eingehalten werden.

dei lavoratori/delle lavoratrici.

4. I controlli devono essere effettuati nel rispetto del presente regolamento e dei seguenti principi:

- **proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alle finalità perseguite, ma resterà sempre entro i limiti minimi;
- **trasparenza:** l'adozione del presente regolamento ha l'obiettivo di informare gli utenti sui diritti e i doveri di entrambe le parti;
- **pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori/delle lavoratrici, così come la possibilità di controlli prolungati, costanti o indiscriminati.

4. Die Kontrollen werden in Übereinstimmung mit dieser Verordnung und den folgenden Grundsätzen durchgeführt:

- **Verhältnismäßigkeit:** Die Überwachung und ihr Umfang müssen in jedem Fall angemessen, sachdienlich und im Hinblick auf die verfolgten Ziele nicht übertrieben sein, müssen aber immer innerhalb der Mindestgrenzen bleiben;
- **Transparenz:** Der Zweck der Verordnung ist es, die Nutzer über die Rechte und Pflichten beider Parteien zu informieren;
- **Relevanz und Nicht-Übermäßigkeit:** d.h. Vermeidung von ungerechtfertigten Eingriffen in die Grundrechte und -freiheiten von Arbeitnehmern sowie der Möglichkeit längerer, ständiger oder wahlloser Kontrollen.

5. Qualora risulti necessario l'accesso agli strumenti e alle risorse informatiche e relative informazioni descritte ai punti precedenti, il/la titolare del trattamento dei dati personali, tramite il CED, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo strumento oggetto di controllo):

I. Avviso generico a tutti/e i/le dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente regolamento.

II. Se il comportamento anomalo persiste, l'ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti precedenti, con possibilità di rilevare

5. Wenn der Zugriff auf die in den vorstehenden Punkten beschriebenen Informatikgeräte und -Ressourcen und die damit verbundenen Informationen erforderlich ist, befolgt der Rechtsinhaber der Datenverarbeitung über die EDV-Dienststelle das nachstehend beschriebene Verfahren (wenn und soweit dies mit dem zu überwachenden Gerät vereinbar ist):

I. Allgemeine Warnung an alle Mitarbeiter/innen vor abnormalem Verhalten, das die Sicherheit des Informationssystems gefährden kann, und Erinnerung an die Notwendigkeit, diese Vorschriften einzuhalten.

II. Wenn das anomale Verhalten anhält, kann der Betrieb das mit der Kontrolle beauftragte Personal ermächtigen, auf die in den vorhergehenden Punkten beschriebenen Informationen zuzugreifen, mit der Möglichkeit, während der Arbeitstätigkeit verarbeitete Dateien,

file trattati, siti *web* visitati, *software* installati, documenti scaricati, statistiche sull'uso di risorse, ecc. nel corso dell'attività lavorativa.

III. Qualora il rischio di compromissione del sistema informativo dell'ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti precedenti, il/la titolare del trattamento, unitamente al CED può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

besuchte Websites, installierte Software, heruntergeladene Dokumente, Statistiken über die Nutzung der Ressourcen usw. zu ermitteln.

III. Wenn das Risiko einer Kompromittierung des Informationssystems des Betriebes unmittelbar bevorsteht und so schwerwiegend ist, dass die für die in den vorherigen Punkten beschriebenen Verfahrensschritte erforderliche Zeit nicht zur Verfügung steht, kann der Rechtsinhaber der Datenverarbeitung zusammen mit der EDV-Dienststelle unverzüglich in das Gerät eingreifen, von dem die potenzielle Bedrohung ausgeht.

Art. 29
Conservazione dei dati

1. In riferimento agli articoli 5 e 6 del Regolamento UE 2016/679, e in applicazione dei principi di diritto di accesso, legittimità, proporzionalità, sicurezza e accuratezza e conservazione dei dati, le informazioni relative all'accesso a *internet* e al traffico telematico (es. *log* di sistema e del *server proxy*), la cui conservazione non sia necessaria, saranno cancellate entro i termini previsti dalla normativa salvo:

a) esigenze tecniche o di sicurezza;
b) per l'indispensabilità dei dati rispetto all'esercizio;
c) per difesa di un diritto in sede giudiziaria;
d) per l'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria.

Art. 29
Datenspeicherung

1. Unter Bezugnahme auf Artikel 5 und 6 der Verordnung (EU) 2016/679 und in Anwendung der Grundsätze des Auskunftsrechts, der Rechtmäßigkeit, der Verhältnismäßigkeit, der Sicherheit und der Richtigkeit sowie der Datenspeicherung werden die Informationen über den Internetzugang und den Telematikverkehr (z.B. System- und *Proxy-Server*-Logs), deren Speicherung nicht erforderlich ist, innerhalb der von der Gesetzgebung vorgesehenen Fristen gelöscht, außer:

a) für technische oder Sicherheitsanforderungen;
b) für die Unerlässlichkeit der Daten im Hinblick auf die Ausübung;
c) zur Verteidigung eines Rechts vor Gericht;
d) für die Verpflichtung, die Daten aufzubewahren oder zu liefern, um einer spezifischen Anfrage der Gerichtsbehörde oder der Gerichtspolizei nachzukommen.

2. ASSB si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di

2. BSB verpflichtet sich, bei der Verarbeitung und Speicherung dieser Art von Daten Sicherheitsmaßnahmen zu

dati alla luce di quanto stabilito dal Legislatore.

Art. 30
Partecipazione a *social media*

1. L'utilizzo a fini promozionali e commerciali di *social media*, di *blog* e di *forum*, anche professionali, e altro è gestito e organizzato esclusivamente da ASSB, attraverso specifiche direttive e istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte di singoli utenti o collaboratori/collaboratrici.

2. Fermo restando il diritto alla libertà di espressione, con riguardo all'utilizzo di *social media*, ASSB prevede di seguito alcune regole comportamentali, al fine di tutelare tanto la propria immagine e il patrimonio, anche immateriale, quanto i/le propri/e collaboratori/collaboratrici, i propri clienti e fornitori, gli altri partner, oltre che gli stessi utenti utilizzatori dei *social media*. È peraltro vietata la partecipazione agli stessi *social media* durante l'orario di lavoro, qualora non attinente, anche indirettamente, all'attività lavorativa.

3. La condivisione dei contenuti nei *social media* deve sempre rispettare e garantire la segretezza delle informazioni considerate riservate da ASSB e in generale, a titolo esemplificativo e non esaustivo, delle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovranno essere effettuate nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'ente. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della

ergreifen, die den Vorgaben des Gesetzgebers entsprechen.

Art. 30
Teilnahme an *social media*

1. Die Nutzung von sozialen Medien, Blogs und Foren, einschließlich professioneller, und anderer, zu Werbe- und kommerziellen Zwecken wird ausschließlich von BSB verwaltet und organisiert, und zwar durch spezifische Richtlinien und Betriebsanweisungen an das ausdrücklich damit beauftragte Personal, unter Ausschluss individueller Initiativen einzelner Nutzer oder Mitarbeiter.

2. Unbeschadet des Rechts auf freie Meinungsäußerung sieht BSB im Hinblick auf die Nutzung sozialer Medien die folgenden Verhaltensregeln vor, um sein Image und seine Eigentumswerte, einschließlich immaterieller Werte, sowie seine Mitarbeiter, Kunden, Lieferanten, andere Partner und Nutzer sozialer Medien zu schützen. Die Teilnahme an den sozialen Medien während der Arbeitszeit ist, wenn sie nicht, auch nicht indirekt, mit der Arbeit zusammenhängt, ebenfalls verboten.

3. Das Teilen von Inhalten in sozialen Medien muss immer die Geheimhaltung von Informationen respektieren und gewährleisten, die von BSB als vertraulich angesehen werden, und im Allgemeinen, als Beispiel aber nicht ausschließlich, auf Informationen, die sich auf Aktivitäten, Buchhaltungs- und Finanzdaten, Projekte und Verfahren beziehen, die in den Büros durchgeführt werden oder im Gange sind. Darüber hinaus muss jede Kommunikation und Offenlegung von Inhalten in vollem Umfang unter Beachtung der gewerblichen Schutzrechte und Urheberrechte, sowohl Dritter als auch des Betriebes, erfolgen. Von den vorstehenden Bestimmungen kann nur

Direzione Generale di ASSB.

mit ausdrücklicher Genehmigung der Generaldirektion von BSB abgewichen werden.

4. L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi/e e in genere di collaboratori/trici, se non con il preventivo personale consenso di questi/e, e comunque non potrà postare nei *social media* immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del/la responsabile d'ufficio.

4. Der Nutzer muss den Schutz der Vertraulichkeit und der Würde von Personen gewährleisten; folglich darf er keine persönlichen Daten (wie z. B. personenbezogene Daten, Bilder, Videos, Töne und Stimmen) von Kollegen und im Allgemeinen von Mitarbeitern ohne die vorherige persönliche Zustimmung der letzteren kommunizieren oder verbreiten und auf keinen Fall Bilder, Videos, Töne und Stimmen, die am Arbeitsplatz aufgenommen wurden, ohne die vorherige Zustimmung des Verantwortlichen des Amtes auf sozialen Medien veröffentlichen.

5. Qualora l'utente intenda usare *social network*, *blog*, *forum* su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.), egli esprimerà unicamente le proprie opinioni personali; pertanto, dove necessario od opportuno per la possibile connessione con ASSB, in particolare in *forum* professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'ente.

5. Beabsichtigt der Nutzer die Nutzung von sozialen Netzwerken, Blogs, Foren zu auch nur mittelbar beruflichen Themen (z.B. Beiträge zu Produkten, Dienstleistungen, Lieferanten, Partnern, etc.), wird er nur seine persönliche Meinung äußern; daher muss der Nutzer, wo es für die mögliche Verbindung mit BSB notwendig oder angebracht ist, insbesondere in beruflichen Foren, angeben, dass die geäußerten Meinungen ausschließlich persönlich sind und nicht dem Betrieb zugerechnet werden können.

CAPO VI

VIOLAZIONI DEL REGOLAMENTO E DISPOSIZIONI FINALI

ABSCHNITT VI

MISSACHTUNGEN GEGEN DIE VERORDNUNG UND SCHLUSSBESTIMMUNGEN

Art. 31
Responsabilità

1. Responsabili del rispetto e dell'applicazione del presente regolamento sono i/le Direttori/trici di servizio/ufficio/amministrazione di competenza, nella loro qualità di Responsabili *Privacy.* Chiunque acceda, a qualsiasi titolo, alle risorse informatiche

Art. 31
Verantwortung

1. Verantwortlich für die Einhaltung und Anwendung der vorliegenden Verordnung sind die Direktoren der jeweiligen Dienststelle/Behörde/Verwaltung in ihrer Eigenschaft als Datenschutzbeauftragte. Wer, aus welchem Grund auch immer, auf die Computerressourcen von BSB zugreift,

di ASSB è comunque tenuto al rispetto e all'applicazione del presente regolamento.

2. Tutti i/le dipendenti/collaboratori/collaboratrici di ASSB, prima di intraprendere qualsiasi attività non espressamente prevista dal presente regolamento, devono darne comunicazione al/la Dirigente competente, che a sua volta riferisce al/la Dirigente del CED e al Responsabile del CED, il/la quale provvede a valutare che la stessa non sia in contrasto con gli standard di sicurezza informatica stabiliti da ASSB.

ist in jedem Fall verpflichtet, diese Verordnung zu respektieren und anzuwenden.

2. Vor der Aufnahme einer Tätigkeit, die nicht ausdrücklich in dieser Verordnung vorgesehen ist, müssen alle Bediensteten/ Mitarbeiter/innen von BSB die zuständige Führungskraft informieren, die wiederum dem Leiter der EDV-Dienststelle und dem Verantwortlichen der EDV-Dienststelle Bericht erstattet, der beurteilt, ob die Tätigkeit nicht im Widerspruch zu den von BSB festgelegten Informationssicherheitsstandards steht.

Art. 32
Violazioni

1. Qualsiasi utilizzo non conforme alle disposizioni del presente regolamento e/ o alle leggi vigenti è riconducibile a esclusiva responsabilità del personale che risulta utente dei sistemi informatici aziendali, salvo che la violazione non dipenda da fatto non imputabile al medesimo.

2. L'utente è direttamente responsabile, civilmente e penalmente, per l'uso improprio di *internet*, per la violazione di accessi protetti, per il mancato rispetto delle norme sul *copyright* e sulle licenze d'uso.

3. A fronte della notizia di attività illecite determinanti reati perseguibili d'ufficio, ASSB si riserva di denunciare alle Autorità competenti, ai sensi dell'art. 331 c.p.p., anche quando non sia individuata la persona alla quale il reato è riconducibile.

Art. 32
Missachtung

1. Jede Nutzung, die nicht mit den Bestimmungen dieser Verordnung und/oder den geltenden Gesetzen übereinstimmt, unterliegt der ausschließlichen Verantwortung der Bediensteten, die die Computersysteme des Unternehmens nutzen, es sei denn, der Verstoß ist auf ein Ereignis zurückzuführen, das ihnen nicht zugerechnet werden kann.

2. Für die missbräuchliche Nutzung des Internets, für die Verletzung geschützter Zugänge, für die Nichtbeachtung der Regeln zum Urheberrecht und der Nutzungslizenzen ist der Nutzer direkt zivil- und strafrechtlich verantwortlich.

3. Bei Bekanntwerden von rechtswidrigen Handlungen, die zu Straftaten führen, die von Amts wegen verfolgt werden können, behält sich BSB das Recht vor, gemäß Art. 331 der Strafprozessordnung, Anzeige bei den zuständigen Behörden zu erstatten, auch wenn die Person, der die Straftat zugeordnet werden kann, nicht identifiziert wird.

4. Le violazioni del presente regolamento comportano altresì responsabilità disciplinare del/la dipendente ai sensi del vigente Codice disciplinare di ASSB. Chiunque abbia notizia di una qualsiasi violazione è tenuto a darne comunicazione al/la proprio/a Direttore/ Direttrice responsabile.

4. Verstöße gegen diese Verordnung ziehen auch eine disziplinarische Verantwortung des Mitarbeiters nach der aktuellen BSB-Disziplinarverordnung nach sich. Jeder, der von einem Verstoß Kenntnis erlangt, ist verpflichtet, seinen/ihren Direktor/Vorgesetzten zu benachrichtigen.

Art. 33
Violazione *privacy* e *data breach*

1. Ai sensi del Regolamento UE 2016/679, ogni titolare del trattamento dei dati personali deve mettere in atto misure tecniche e organizzative per garantire un idoneo livello di sicurezza dei dati trattati nell'ambito delle proprie attività istituzionali, ovvero agire in modo adeguato e tempestivo, onde evitare che eventuali violazioni possano provocare danni fisici, danni materiali o immateriali alle persone fisiche, quali, ad esempio, la perdita del controllo dei dati personali che le riguardano o la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, la perdita finanziaria, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

2. Il/la titolare del trattamento dei dati personali deve notificare la violazione di dati personali all'Autorità di controllo, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto/a a conoscenza, a meno che non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Art. 33
Verstösse gegen die *Privacy* und *Data breach*

1. Gemäß der EU-Verordnung 2016/679 muss jeder Rechtsinhaber der Datenverarbeitung technische und organisatorische Maßnahmen ergreifen, um ein angemessenes Sicherheitsniveau der im Rahmen seiner institutionellen Tätigkeiten verarbeiteten Daten zu gewährleisten, d.h. angemessen und rechtzeitig zu handeln, um zu verhindern, dass eine Verletzung letzterer physischen, materiellen oder immateriellen Schaden für natürliche Personen verursacht, wie z.B., Verlust der Kontrolle über sie betreffende personenbezogene Daten oder Einschränkung ihrer Rechte, Diskriminierung, Diebstahl oder Aneignung der Identität, finanzieller Verlust, unbefugte Entschlüsselung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit personenbezogener Daten, die durch das Berufsgeheimnis geschützt sind, oder jeder andere wirtschaftliche oder soziale Schaden für die betroffene natürliche Person.

2. Der Rechtsinhaber der Datenverarbeitung meldet der Aufsichtsbehörde die Verletzung des Schutzes personenbezogener Daten unverzüglich und nach Möglichkeit innerhalb von 72 Stunden, nachdem er davon Kenntnis erlangt hat, es sei denn, er kann nachweisen, dass die Verletzung des Schutzes personenbezogener Daten im Einklang mit dem Grundsatz der Rechenschaftspflicht wahrscheinlich kein Risiko für die Rechte und Freiheiten

natürlicher Personen darstellen wird.

3. Ai sensi del Regolamento UE 2016/679, il *data breach* consiste in una violazione di sicurezza che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati. Una violazione di dati personali può compromettere la riservatezza, l'integrità o la disponibilità degli stessi.

3. Gemäß der EU-Verordnung 2016/679 ist ein *data breach* eine Sicherheitsverletzung, die - versehentlich oder unrechtmäßig - zur Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum Zugriff auf übermittelte, gespeicherte oder auf jeden Fall verarbeitete personenbezogene Daten führt. Eine Verletzung des Schutzes personenbezogener Daten kann die Vertraulichkeit, Integrität oder Verfügbarkeit dieser gefährden.

4. Non danno luogo a *data breach* il danno o il furto di dati provocati da soggetti terzi malintenzionati, nè la perdita accidentale di dati personali, ovvero la loro cancellazione cagionata da errore umano o di sistema, o semplicemente l'impossibilità di accesso al dato, per esempio a causa della perdita della *password* di accesso a un archivio protetto o a causa della criptazione provocata da un'infezione da *ramsonware*.

4. Ein *data breach* ergibt sich weder aus der Beschädigung oder dem Diebstahl von Daten durch böswillige Dritte noch aus dem versehentlichen Verlust personenbezogener Daten oder deren Löschung aufgrund von menschlichen oder Systemfehlern oder einfach aus der Unmöglichkeit, auf die Daten zuzugreifen, z. B. aufgrund des Verlusts eines Passworts für den Zugriff auf ein geschütztes Archiv oder aufgrund der Verschlüsselung durch eine *Ramsonware*-Infektion.

5. L'Autorità di controllo a cui segnalare il *data breach* è l'Autorità garante per la protezione dei dati personali, come definito dall'articolo 55 del Regolamento UE 2016/679. L'omessa notifica di *data breach* all'Autorità di controllo, l'omessa comunicazione agli/alle interessati/e della violazione ovvero l'omissione di entrambi gli adempimenti, nel caso in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 del Regolamento UE 2016/679, può comportare l'applicazione di una sanzione amministrativa pecuniaria fino a 10 milioni di euro in capo al/la titolare del trattamento dei dai personali.

5. Die Aufsichtsbehörde, der der *data breach* gemeldet werden sollte, ist die Datenschutzbehörde, wie in Artikel 55 der EU-Verordnung 2016/679 definiert. Das Versäumnis, die Aufsichtsbehörde über den *data breach* zu benachrichtigen, das Versäumnis, die betroffene(n) Person(en) über die Verletzung zu benachrichtigen, oder das Versäumnis, beides zu tun, wenn die Anforderungen der Artikel 33 und 34 der Verordnung (EU) 2016/679 erfüllt sind, kann zur Anwendung einer Verwaltungssanktion in Höhe von bis zu 10 Millionen Euro gegen den Rechtsinhaber der Datenverarbeitung führen.

6. In riferimento all'art. 33 del Regolamento UE 2016/679, al/la titolare

6. Unter Bezugnahme auf Artikel 33 der Verordnung (EU) 2016/679, ist der

del trattamento spetta il compito di valutare l'impatto e la gravità della violazione ed eventualmente avviare una procedura di notifica all'Autorità di controllo avvalendosi dell'Unità *Privacy* di ASSB. Fatte salve le raccomandazioni contenute in questo regolamento relative alla protezione dei dati personali, all'utilizzo dei sistemi e degli strumenti messi a disposizione degli utenti, si riporta un elenco, esemplificativo e non esaustivo, delle possibili violazioni:

a) accesso alla propria postazione di lavoro da parte di persone non autorizzate;
b) accesso alla propria casella di posta elettronica da parte di persone non autorizzate;
c) accesso alla rete dati dell'ente da parte di terzi con dispositivi non autorizzati;
d) perdita o sottrazione di dispositivi di memorizzazione esterni contenenti dati personali;
e) installazione di *software* malevolo o comunque non autorizzato che possa compromettere la sicurezza e l'integrità degli strumenti.

Rechtsinhaber der Datenverarbeitung dafür zuständig, die Auswirkungen und die Schwere der Verletzung zu bewerten und ggf. ein Meldeverfahren bei der Aufsichtsbehörde über die BSB-Datenschutzeinheit einzuleiten. Unbeschadet der in dieser Verordnung enthaltenen Empfehlungen zum Schutz personenbezogener Daten und zur Nutzung der den Nutzern zur Verfügung gestellten Systeme und Geräte ist die folgende eine beispielhafte und nicht vollständige Liste möglicher Verstöße:

a) Zugriff auf den eigenen Arbeitsplatz durch nicht autorisierte Personen;
b) Zugriff auf das eigene E-Mail-Postfach durch Unbefugte;
c) Zugriff auf das Datennetz des Betriebes durch Dritte mit nicht autorisierten Geräten;
d) Verlust oder Diebstahl von externen Speichermedien mit personenbezogenen Daten;
e) die Installation von bösartiger oder in jedem Fall nicht autorisierter Software, die die Sicherheit und Integrität der Geräte beeinträchtigen kann.

7. Le violazioni riscontrate, anche se non basate su elementi concreti, vanno immediatamente segnalate dal/la Dirigente dell'Ufficio che rileva la violazione all'Unità *Privacy* di ASSB seguendo la procedura *data breach* pubblicata sul sito *intranet* aziendale *Aziendanet* >*Privacy* > Documenti > Documenti *Privacy* > *Data Breach* e utilizzando i relativi allegati.

7. Jeder festgestellte Verstoß, auch wenn er nicht auf konkreten Elementen beruht, muss von der Führungskraft des Amtes, das den Verstoß feststellt, unverzüglich an die Datenschutzeinheit von BSB gemeldet werden, und zwar gemäß dem Verfahren für Datenschutzverletzungen, das auf der Intranetseite des Unternehmens *Aziendanet* >*Privacy* > Dokumente > *Privacy* Dokumente > *Data Breach* veröffentlicht ist, und unter Verwendung der entsprechenden Anlagen.

Art. 34
Sanzioni disciplinari

1. Tutti/e i/le dipendenti/collaboratori/collaboratrici/utenti devono obbligatoriamente osservare

Art. 34
Disziplinarstrafen

1. Alle Bediensteten/Mitarbeiter-innen/Nutzer-innen sind verpflichtet, die ihnen durch

le disposizioni portate a conoscenza con il presente regolamento.

2. L'ente si riserva, in caso di inosservanza, rilevata in seguito ai relativi controlli e verifiche, di procedere con i relativi provvedimenti in relazione alla gravità del danno.

diese Verordnung zur Kenntnis gebrachten Bestimmungen einzuhalten.

2. Bei Nichteinhaltung, die nach den entsprechenden Kontrollen und Überprüfungen festgestellt wird, behält sich der Betrieb das Recht vor, die entsprechenden Maßnahmen in Abhängigkeit der Schwere des Schadens zu ergreifen.

Art. 35
Revisione periodica

1. Il presente regolamento è soggetto a revisione periodica ed entra in vigore con la sua formale adozione con decreto della Direzione Generale di ASSB, previo accordo con le organizzazioni sindacali.

2. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente regolamento. Le proposte verranno esaminate dalla Direzione Generale di ASSB.

3. Il presente regolamento è, inoltre, soggetto a revisione sulla base di modifiche e/o integrazioni stabilite dall'Autorià garante per la protezione dei dati personali e/o da altri enti ufficiali preposti agli argomenti trattati.

4. Per qualsiasi chiarimento si rendesse necessario durante l'utilizzo dei sistemi informatici aziendali, l'utente deve rivolgersi al/la Responsabile CED di ASSB.

Art. 35
Periodische Überprüfung

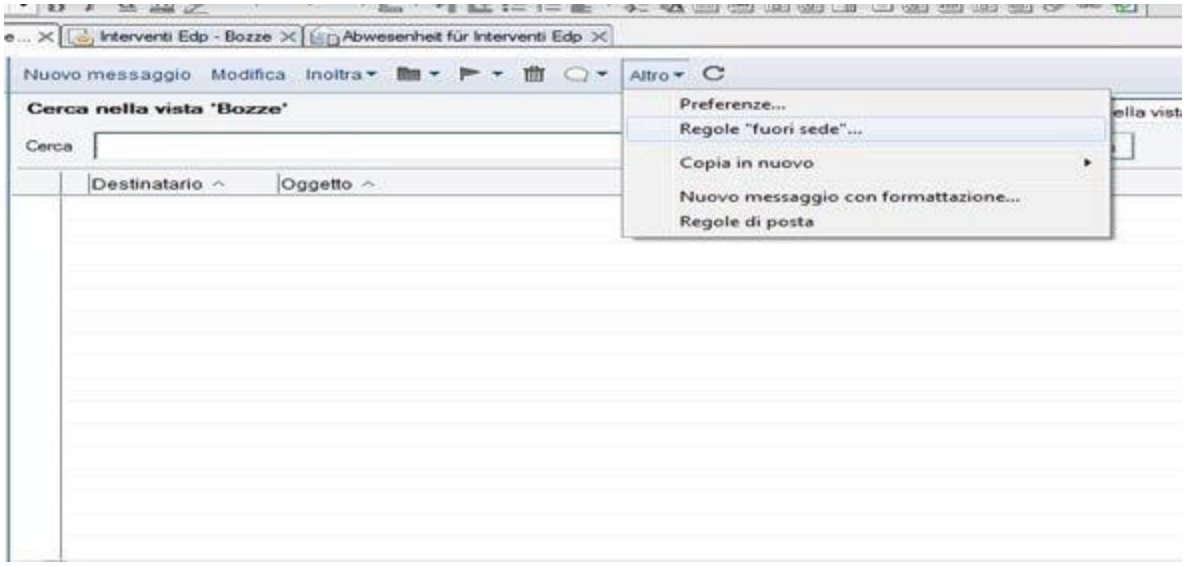
1. Diese Verordnung unterliegt einer regelmäßigen Überprüfung und tritt mit seiner förmlichen Verabschiedung durch Beschluss der Generaldirektion von BSB in Kraft, vorbehaltlich der Zustimmung der Gewerkschaften.

2. Alle Nutzer/innen können, wenn sie es für notwendig halten, begründete Ergänzungen zu den vorliegenden Vorschriften vorschlagen. Die Vorschläge werden von der Generaldirektion von BSB geprüft.

3. Die vorliegende Verordnung unterliegt auch der Überprüfung auf der Grundlage von Änderungen und/oder Ergänzungen, die von der Garantiebehörde für den Schutz personenbezogener Daten und/oder von anderen offiziellen Stellen, die für die behandelten Themen zuständig sind, festgelegt werden.

4. Für jede Klarstellung, die während der Nutzung der Informatiksysteme des Betriebes erforderlich ist, muss sich der/die Nutzer/in an den Verantwortlichen der EDV-Dienststelle von BSB wenden.

ALLEGATO/ANHANG 1) Figura/Bild 1



Figura/Bild 2

ASSB·BSB
Azienda Servizi Sociali di Bolzano
Betrieb für Sozialdienste Bozen

ALLEGATO 2) DELEGA AL FIDUCIARIO A VERIFICARE IL CONTENUTO DI MESSAGGI DI POSTA ELETTRONICA

_____,

_____

Oggetto: Autorizzazione temporanea alla visualizzazione di messaggi di posta elettronica aziendali per garantire la continuità operativa dei processi aziendali

Io sottoscritto/a Sig./Sig.ra _____,
in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto di messaggi di posta elettronica presenti nella *mail box* assegnatami,autorizzo l'amministratore di sistema (*fiduciario/a*) a verificare il contenuto di messaggi e a inoltrare al/la titolare del trattamento o a un/a responsabile competente quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Il/la fiduciario/a provvederà a verbalizzare tale attività, fornendo copia del verbale e a informarmi al rientro in Azienda.
L'accesso all'account di posta elettronica è motivato dalla necessità di garantire la continuità dei processi operativi aziendali.
La *mail box* assegnatami contiene esclusivamente messaggi di posta elettronica a carattere professionale e lavorativo e non contiene messaggi di natura personale.
Autorizzo, altresì, gli/le incaricati/e alla manutenzione ad accedere alla suddetta casella di posta elettronica per gli scopi propri delle loro attività lavorative come individuate nella lettera d'incarico.
Bolzano, li

_____
(firma)

_____
Il/la fiduciario/a, per accettazione

ANHANG 2) Vollmacht an den/die Treuhänder/in, den Inhalt von E-Mail-Nachrichten zu überprüfen

_____,

_____

Betreff: Vorübergehende Berechtigung zur Einsichtnahme in Betriebs-E-Mails zur Gewährleistung der Fortführung von Betriebsabläufen.

Ich, der/die unterzeichnende, Herr/Frau _____, in Anbetracht der Möglichkeit, dass man, im Falle einer plötzlichen oder längeren Abwesenheit und für unvorhersehbare berufsbedingte Erfordernisse, den Inhalt der in der mir zugewiesenen Mailbox vorhandenen E-Mail-Nachrichten erfahren muss, autorisiere ich den/die Systemadministrator/in (Treuhänder/in), den Inhalt der Nachrichten zu überprüfen und diejenigen an den Rechtsinhaber der Datenverarbeitung oder einen dafür zustehenden Verantwortlichen weiterzuleiten, die als relevant für die Durchführung der Arbeitstätigkeit angesehen werden. Der/die Treuhänder/in wird über diesen Vorgang ein Protokoll erstellen, eine Kopie des Protokolls zur Verfügung stellen und mich bei der Rückkehr in den Betrieb informieren. Der Zugriff auf den E-Mail-account ist durch die Notwendigkeit begründet, die Kontinuität der Arbeitsprozesse des Betriebes zu gewährleisten. Die mir zugewiesene Mailbox enthält ausschließlich E-Mail-Nachrichten beruflicher und geschäftlicher Natur und keine persönlichen Nachrichten. Ich ermächtige außerdem die für die Wartung verantwortliche(n) Person(en) zum Zugriff auf die oben genannte Mailbox für die Zwecke ihrer Arbeit, wie es aus dem Auftragsschreiben gemäß Gesetzesdekret vom 30. Juni 2003, Nr. 196, i.g.F., hervorgeht.
Bozen, den

_____
(Unterschrift)

_____
Der/die Treuhänder/in, zwecks Annahme

ASSB·BSB
Azienda Servizi Sociali di Bolzano
Betrieb für Sozialdienste Bozen

ALLEGATO 3)
VERBALE DI ACCESSO ALLA *MAILBOX* DI LAVORATORI/LAVORATRICI ASSENTI DA PARTE DEI/LLE FIDUCIARI/E

_____,
_____

Oggetto: Verbale di accesso alla *mailbox* di lavoratori/lavoratrici assenti da parte dei/lle fiduciari/e per garantire la continuità operativa dei processi aziendali

Io sottoscritto _____,
nella mia funzione di amministratore di sistema, conferita con specifica nomina d.d. XX.XX.XXXX;
in qualità di fiduciario, delegato formalmente dal Sig./dalla Sig.ra _____
ed a seguito dell'assenza improvvisa e prolungata del/la suddetto/a collega, - per improrogabili necessità legate all'attività lavorativa - ho provveduto a verificare il contenuto dei messaggi presenti nella *mailbox* del/la collega. I messaggi di posta elettronica ritenuti rilevanti per lo svolgimento dell'attività lavorativa sono stati inoltrati al/la Direttore/trice Responsabile competente.

Mediante la sottoscrizione della presente relazione provvedo, in esecuzione alla delega formalizzatami, a verbalizzare le attività svolte e ad inviare copia del presente verbale alla funzione controllo.

Al rientro del/della collega, provvederò ad informarlo/la delle attività svolte.
Bolzano, li

_____(firma)

ANHANG 3)
ZUGRIFFSPROTOKOLL DER TREUHÄNDER/INNEN AUF DIE MAILBOX ABWESENDER MITARBEITER/INNEN

_____,
_____

Betreff: Zugriffsprotokoll auf die Mailbox abwesender Mitarbeiter/innen durch Treuhänder/innen zur Gewährleistung der Fortführung von Betriebsabläufen

Ich, der/die Unterzeichnende, _____
in meiner Eigenschaft als Systemadministrator/in, verliehen durch besondere Ernennung mit Datum, XX.XX.XXXX; als Treuhänder, formell bevollmächtigt durch Herrn / Frau _____
und nach der unerwarteten und längeren Abwesenheit des/der oben genannten Kollegen/Kollegin, habe - aufgrund unvorhersehbarer beruflicher Erfordernisse - den Inhalt der Nachrichten in der Mailbox des/der Kollegen/Kollegin überprüft. E-Mails, die als relevant für die Durchführung der Arbeitstätigkeiten angesehen wurden, wurden an den/die zuständige/n Direktor/in-Verantwortliche/n weitergeleitet.

Anhand meiner Unterschrift halte ich in Ausübung der mir übertragenen Befugnisse die durchgeführten Tätigkeiten fest und sende eine Kopie dieses Protokolls an die Kontrollfunktion.

Nach Rückkehr der/des Kollegen/Kollegin, werde ich ihn/sie über die durchgeführten Tätigkeiten informieren.
Bozen, am

_____ (Unterschrift)

ALLEGATO 4)
DISCLAIMER MESSAGGI DI POSTA ELETTRONICA

Ai sensi del Regolamento UE 2016/679 le informazioni contenute e trasmesse sono riservate e destinate esclusivamente alla persona indicata. Diffidiamo di effettuare ogni forma di copia, rivelazione, divulgazione e utilizzo della presente comunicazione da parte di altra persona diversa dal destinatario indicato. Qualora abbiate ricevuto questa e-mail erroneamente, vogliate cortesemente informarci a mezzo telefono e ritornare il messaggio originale all'indirizzo sopra indicato, distruggendo qualunque copia in Vostro possesso.

ANHANG 4)
E-Mail-Haftungsausschluss (Disclaimer)

Gemäß der Verordnung EU 2016/679 sind die übermittelten Daten und Informationen nur für die direkten Empfänger/innen bestimmt und diesen vorbehalten. Es ist allen anderen Personen und Rechtsträgern strengstens untersagt, Kopien der vorliegenden Mitteilung anzufertigen, selbige bekanntzugeben, diese zu verbreiten oder sonst wie zu verwenden. Sollten Sie die vorliegende E-Mail fälschlicherweise erhalten haben, ersuchen wir Sie um eine umgehende, telefonische Verständigung, um Rücksendung der Nachricht und um die Zerstörung aller eventuellen Kopien in Ihrem Besitz.