Autonome Provinz Bozen - Südtirol

Regelung zur Nutzung der IT-Dienste

Artikel 1
Anwendungsbereich

1. Diese Regelung betrifft alle Landesbediensteten, das Personal der Schulen staatlicher Art, Praktikanten und Praktikantinnen sowie andere Personen, die von der Südtiroler Landesverwaltung zeitweilig ein Benutzerkonto (Account) erhalten.

Artikel 2
Begriffsbestimmung

1. Soweit in dieser Regelung personenbezogene Bezeichnungen von Funktionen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

2. Für die Anwendung der vorliegenden Verordnung versteht man:
   a) Als ***Informationssystem der Autonomen Provinz Bozen (ISAPB)***:
   "Die Gesamtheit der IT-Infrastruktur bestehend aus Netzwerkgeräten, Apparaten, Software, Datenbeständen und alle, aus beliebigem Grund, in digitaler Form gespeicherten oder mittels *cloud computing* genutzten IT-Ressourcen, die der Verwaltung zur Verfügung stehen und von dieser genutzt werden";
   b) Als ***Nutzer***:
   "Jeder der ISAPB nutzt, sowohl im lokalen Netzwerk innerhalb der Landesverwaltung als auch über einen Internet-Zugang";
   c) Als ***cloud computing*** (Datenwolke):

Provincia Autonoma di Bolzano – Alto Adige

Disciplinare organizzativo per l'utilizzo dei servizi informatici

Articolo 1
Ambito di applicazione

1. Il presente disciplinare contiene le prescrizioni a cui devono attenersi tutti i dipendenti provinciali, il personale delle scuole a carattere statale, i tirocinanti nonché le altre persone che ricevono temporaneamente un account dall'Amministrazione provinciale.

Articolo 2
Definizione

1. Le denominazioni di funzioni riferite a persone, riportate nella sola forma maschile nel presente regolamento, si riferiscono indistintamente a persone sia di sesso maschile che di sesso femminile.

2. Ai fini dell'applicazione del presente Regolamento deve intendersi:
   a) per ***Sistema Informativo della Provincia Autonoma di Bolzano (SIPAB)***:
   "L'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale o fruiti in modalità *cloud computing*, in dotazione ed uso all'amministrazione";

   b) per ***utente***:
   "Chiunque utilizzi il SIPAB, sia che il collegamento avvenga in rete locale che in internet";

Landhaus 3a, Silvius-Magnago-Platz 4 • 39100 Bozen
Tel. +39 0471 41 10 40 • Fax +39 0471 41 10 49
http://www.provinz.bz.it/ressorts/generaldirektion/
generaldirektion.direzionegenerale@pec.prov.bz.it
generaldirektion@provinz.bz.it
Steuernr./Mwst.Nr. 00390090215

Palazzo 3a, Piazza Silvius Magnago 4 • 39100 Bolzano
Tel. +39 0471 41 10 40 • Fax +39 0471 41 10 49
http://www.provincia.bz.it/dipartimenti/direzione-generale/
generaldirektion.direzionegenerale@pec.prov.bz.it
direzionegenerale@provincia.bz.it
Codice fiscale/Partita Iva 00390090215

"Die Speicherung, die Bearbeitung und die Nutzung der Daten auf remote Computern und deren Nutzung über Internet";

d) Als ***SIAG***:
"Südtiroler Informatik AG - Informatica Alto Adige S.p.A";

e) Als ***BYOD***:
"bring your own device - Nutzung des persönlichen Gerätes durch den Nutzer zur Durchführung der eigenen Arbeit".

c) per ***cloud computing*** (nuvola informatica):
"L'archiviazione, l'elaborazione e l'uso di dati su computer remoti e il relativo utilizzo via Internet";

d) per ***SIAG***:
"Südtiroler Informatik AG - Informatica Alto Adige S.p.A";

e) per ***BYOD***:
"bring your own device - utilizzo da parte dell'utente del proprio dispositivo personale nello svolgimento del proprio lavoro".

Artikel 3
Zielsetzung

1. Die Computeranlagen, die Programme und sämtliche Funktionen, die die Verwaltung den Benutzern zwecks Nutzung des ISAPB und insbesondere der Dienste des Internets/elektronische Post zur Verfügung stellt, müssen unter strikter Einhaltung der Bestimmungen dieser Verordnung verwendet werden, um mögliche steuerrechtliche und finanzielle Schäden sowie Image-Schäden für die Verwaltung zu vermeiden.

2. Das von den Bestimmungen dieses Reglements betroffene Personal, muss sich mit dem Call Center in Verbindung setzen, bevor es Aktivitäten durchführt, die nicht ausdrücklich in den nachfolgenden Bestimmungen enthalten sind, um sicherzustellen, dass diese Aktivitäten nicht im Widerspruch zu den von der Verwaltung festgelegten Standards der IT-Sicherheit stehen.

Articolo 3
Finalità

1. Le apparecchiature informatiche, i programmi, e tutte le varie funzionalità che l'amministrazione mette a disposizione dei suoi utenti al fine di usufruire dei servizi del SIPAB, ed in particolar modo dei servizi di tipo Internet/posta elettronica, devono essere utilizzate nel pieno rispetto delle norme del presente Regolamento al fine di evitare possibili danni erariali, finanziari e di immagine all'Ente stesso.

2. Tutto il personale interessato dalle disposizioni del presente Regolamento, è tenuto a contattare il Call Center prima di intraprendere qualsiasi attività non esplicitamente compresa nelle disposizioni che seguono, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente.

Artikel 4
Zuständigkeiten und Verantwortung

1. Die Zuständigkeiten und die Verantwortung des Verwaltungspersonals, welches die ISAPB-Dienste nutzt, sind in den nachfolgenden Absätzen definiert.

2. Die Führungskräfte sind verpflichtet:
   a) das Personal über die Bestimmungen zur Nutzung der Ressourcen des Informationssystems der Landesverwaltung zu informieren,
   b) zu gewährleisten, dass sich das ihnen zugewiesene Personal den in dieser

Articolo 4
Competenze e responsabilità

1. Le competenze e le responsabilità del personale dell'amministrazione per ciò che concerne l'utilizzo del SIPAB, sono definite nei commi seguenti.

2. I dirigenti sono tenuti a:
   a) informare il personale sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'Ente;

   b) assicurare che il personale a loro assegnato si uniformi alle regole ed alle

Verordnung beschriebenen Regelungen und Verfahren anpasst,
c) allen Pflichten nachzukommen, die von den geltenden Bestimmungen, insbesondere von den Datenschutzbestimmungen, vorgesehen sind.

3. Darüber hinaus muss jede Führungskraft für das ihr als Programmierer und/oder Systemadministrator zugeordnete Personal sicherstellen, dass die von der Aufsichtsbehörde erlassenen Bestimmungen zum Schutz der persönlichen Daten und insbesondere der Vorgaben in Bezug auf die Systemadministratoren („*Provvedimento del Garante del 27/11/2008*“) eingehalten und umgesetzt werden.

4. Alle Führungskräfte sind dazu verpflichtet sicherzustellen, dass die Lieferanten und das eventuelle externe Personal, die Regelungen und Verfahren der vorliegenden Verordnung und die geltenden Bestimmungen, im Besonderen zum Schutz der persönlichen Daten, einhalten.

5. SIAG in ihrer Eigenschaft als „*in house*“ Gesellschaft, Lieferant von IT-Leistungen in „*outsourcing*“ und als solche zum externen Auftragsverarbeiter ernannt, ist zur Einhaltung der geltenden Rechtsvorschriften und im Besonderen jener zum Schutz der personenbezogenen Daten verpflichtet.

6. Der Sicherheitsdienst der Abteilung Informationstechnik ist zu folgenden Aufgaben verpflichtet:
a) Ausarbeitung von Regelungen, die eine angemessene sichere Nutzung der Informatiksysteme und der Informationssysteme vonseiten des Endnutzers garantieren,
b) Unterstützung bei der Vorbereitung von spezifischem und allgemein verständlichem Informationsmaterial zur Datensicherheit.

7. Das Landespersonal ist verantwortlich für:

a) die Einhaltung der Verwaltungsregelungen für die Nutzung des ISAPB,

b) die sofortige Meldung jeglicher nicht autorisierten Handlung, im Besonderen

procedure descritte nel presente regolamento;
c) adempiere a tutti gli obblighi previsti dalla normativa vigente, e in particolare in materia di protezione dei dati personali.

3. Ogni dirigente è tenuto ad assicurare che il personale a lui assegnato con funzioni di programmatore e/o amministratore di sistema uniformi le proprie attività alle regole ed alle procedure descritte nel presente regolamento, e in particolar modo alle disposizioni emanate dall'Autorità Garante per la protezione dei dati personali; in particolare vengono attuati gli accorgimenti previsti dal Provvedimento 27/11/2008 del Garante relativamente agli amministratori di sistema.

4. Tutti i dirigenti sono tenuti ad assicurare che i fornitori ed eventuale personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente regolamento e alla normativa vigente, e in particolare in materia di protezione dei dati personali.

5. SIAG nella sua qualità di società "*in house*" fornitrice di servizi IT in "*outsourcing*", e in quanto tale nominata responsabile esterno del trattamento, è tenuta al rispetto delle normative vigenti in particolare in materia di protezione dei dati personali.

6. Il Servizio sicurezza istituito presso la Ripartizione Informatica è tenuto a svolgere le seguenti attività:
a) elaborazione delle regole per un utilizzo ragionevolmente sicuro dei sistemi informatici e dei sistemi informativi, da parte dell'utente finale;

b) supporto nella predisposizione del materiale informativo e divulgativo in materia di sicurezza informatica.

7. Il personale provinciale è responsabile per ciò che concerne:
a) il rispetto delle regole dell'amministrazione per l'uso consentito del SIPAB;
b) la segnalazione senza ritardo di ogni eventuale attività non autorizzata, in

bei Datenschutzverletzungen (*data breach*),
c) jeden Gebrauch der ihm anvertrauten Zugangsdaten (Benutzername, Kennwörter).

particolare nei casi di violazione di dati (*data breach*);
c) ogni uso che venga fatto delle credenziali (nome utente, password) assegnategli.

Artikel 5
Rechtsinhaber

1. Die Landesverwaltung ist Inhaberin des gesamten ISAPB. Jeder Nutzer muss darüber informiert werden, welche Nutzung von Ressourcen erlaubt und welche verboten ist.

Articolo 5
Titolarità

1. L'amministrazione provinciale è titolare di tutte le risorse del SIPAB. Ogni utente dovrà essere informato su quali siano gli usi consentiti e proibiti di tali risorse.

Artikel 6
Benutzung der Hardware und Software

1. Der Benutzer verpflichtet sich für die eigene Arbeit in der Regel Computer im Eigentum der Landesverwaltung zu verwenden. Diese Geräte werden für Arbeitszwecke verwendet.

2. Ein Password gilt als komplex, wenn es folgende Mindesteigenschaften vorweist:
   a) Mindestlänge von 10 Zeichen,
   b) es muss Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (z.B. '$', '.', '!', usw.) enthalten,
   c) das Password muss sich von den fünf vorangegangenen Passwörtern unterscheiden.

3. Das Password verfällt nach drei Monaten und kann vom Benutzer jederzeit geändert werden; es muss verpflichtend geändert werden, wenn der Verdacht besteht, dass das Password nicht mehr vertraulich und sicher ist.

4. Um eine effizientere und schnellere Verwaltung des eigenen Passwords zu ermöglichen, ist jeder Benutzer angehalten, sich am Dienst „Self Service Password Reset" zu registrieren (http://office.provinz.bz.it/).

5. Der Benutzer ist dazu ermächtigt, für die Abwicklung der eigenen Arbeit, persönliche Geräte zu verwenden (BYOD), sofern eine Nutzungsumgebung mit Mindestsicherungsmaßnahmen, wie Sperrung des Geräts mit PIN oder komplexem Password und installierte und aktuelle

Articolo 6
Utilizzo di hardware e software

1. L'utente s'impegna ad utilizzare di regola, per il proprio lavoro, computer di proprietà provinciale. Detti strumenti saranno utilizzate per scopi lavorativi.

2. Una password viene ritenuta complessa se ha le seguenti caratteristiche minime:
   a) lunghezza minima di 10 caratteri;
   b) deve contenere caratteri maiuscoli, minuscoli, cifre e caratteri speciali (p.e. '$', '.', '!', ecc.);
   c) la password deve essere diversa dalle cinque precedenti.

3. La password scade dopo tre mesi e può essere cambiata dall'utente in ogni momento; deve essere cambiata obbligatoriamente quando si ritiene che la password non sia più riservata o sicura.

4. Per una gestione più snella ed efficiente della propria password, ogni utente provinciale è tenuto a registrarsi al servizio "Self Service Password Reset" (http://office.provinz.bz.it/).

5. L'utente è autorizzato all'utilizzo di un dispositivo di proprietà personale per il proprio lavoro (BYOD), purché garantisca un ambiente d'uso con misure di sicurezza minime quali il blocco del dispositivo con PIN o password complessa e antivirus/firewall installato e aggiornato. In

Antivirensoftware/Firewall gewährleistet wird. Wird das zur Arbeit genutzte persönliche Gerät (BYOD) verloren oder gestohlen, muss dies vom Benutzer umgehend dem Call Center mitgeteilt werden, damit die erforderlichen Sicherheitsmaßnahmen getroffen werden können.

caso di smarrimento o furto del dispositivo di proprietà personale in uso BYOD, l'utente deve tempestivamente segnalarlo al Call Center per l'eventuale adozione di ulteriori contromisure di sicurezza.

6. In gleicher Weise ist jeder Benutzer angehalten, eine Nutzungsumgebung mit Mindestsicherungsmaßnahmen für mobile Geräte (smartphone und tablet), welche von der Landesverwaltung dem eigenen Personal zur Verfügung gestellt werden, zu garantieren.

6. In modo analogo ogni utente è tenuto a garantire un ambiente d'uso con misure di sicurezza minime sui dispositivi mobili di servizio (smartphone e tablet) affidati dalla Provincia al proprio personale.

7. Der Zugang zu Applikationen der Landesverwaltung wird durch entsprechende Nutzungsvorgaben (disclaimer), die angenommen und sorgsam befolgt werden müssen, geregelt; bei Nichtannahme oder Nichteinhaltung der Vorgaben wird der entsprechende Zugang verwehrt.

7. L'accesso ad applicativi di proprietà provinciale è disciplinato per mezzo di corrispondenti regole d'uso (disclaimer), le quali devono essere accettate e scrupolosamente seguite; in caso contrario l'utilizzo del relativo applicativo viene precluso.

8. Das Personal ist verpflichtet, die eigenen Benutzerdaten für den Zugang zum ISAPB-System geheim zu halten, den Benutzernamen sowie das Password von anderen Nutzern nicht zu verwenden und keine Informationen, die dem Amtsgeheimnis unterliegen, weiterzugeben.

8. Il personale è tenuto a non rivelare ad alcuno le proprie credenziali per l'accesso ai servizi del SIPAB, e a non utilizzare il nome utente e la password di altri utenti, ed a non rivelare notizie, dati o informazioni legate al segreto d'ufficio.

9. Aus Sicherheitsgründen sind die Führungskräfte angehalten, für jene Mitarbeiter, welche mehr als einen Monat vom Dienst abwesend sind oder den Dienst definitiv verlassen, schnellstmöglich die Deaktivierung des Accounts für den Zugang zum ISAPB zu beantragen. Aus denselben Gründen erfolgt eine automatische Deaktivierung jener Zugangs-Accounts zur Domäne des ISPAB, welche für sechs Monate keine Anmeldung vollziehen. Sollte ein Nutzer hingegen mehr als ein Jahr lang keine Anmeldung an der Domäne des ISPAB durchführen, wird dessen Account definitiv deaktiviert und alle dessen Nutzerinhalte, deren Art in einem eigenen Dokument in der Sektion „IT-Sicherheit" im Intranet aufgelistet sind, werden gelöscht.

9. I dirigenti, per motivi di sicurezza, sono tenuti a richiedere al Call Center in modo tempestivo la disattivazione dell'account d'accesso alle risorse del SIPAB per il collaboratore fuori servizio per più di un mese o che lascia il servizio definitivamente. Per lo stesso motivo se un utente non esegue un login al dominio del SIPAB per sei mesi, l'account corrispondente viene disattivato in modo automatico. Se, invece, un utente non esegue un login al dominio del SIPAB per un anno, l'account corrispondente viene definitivamente disattivato e ne vengono cancellati tutti i dati indicati nell'apposito documento nella sezione "sicurezza IT" in Intranet.

10. Auf Anweisung der Abteilung Informationstechnik oder der SIAG verpflichtet sich der Nutzer, spezifische

10. Su indicazione della Ripartizione Informatica o di SIAG l'utente si impegna ad effettuare backup specifici periodici del

regelmäßige Backups der eigenen Arbeit auf elektronischen Datenträgern und/oder autorisierten Geräten durchzuführen. Es ist nicht erlaubt, zusätzliche Backups auf anderen als den oben angeführten, Speichergeräten oder Datenträgern, vorzunehmen.

Artikel 7
Anschaffung von Hardware und Software

1. Zur Vorbeugung gegen Viren und anderen schädlichen Programmen und zum Schutz der Integrität des Landesnetzes wird die gesamte bereitgestellte Hard- und Software von der Abteilung Informationstechnik und der SIAG genehmigt und verwaltet, falls nicht anders vereinbart.

Artikel 8
Geistigen Eigentums und der Lizenzen

1. Die gesamte genutzte Software muss nach den Verfahren und den Richtlinien der Behörde erworben und im Namen der Landesverwaltung oder der SIAG registriert werden. Jeder Nutzer ist zur Einhaltung der Gesetzesnormen im Rahmen der Wahrung des geistigen Eigentums (Copyright) verpflichtet und darf sämtliche Software außerhalb der Lizenzbestimmungen weder installieren, kopieren, noch nutzen.

2. Die Installation und Nutzung von Software (Apps) auf mobile Geräte (smartphone und tablet), sowohl für jene des Typs BYOD als auch für die Dienstgeräte, erfolgt unter der vollständigen Verwaltung und Verantwortung des Nutzers selbst.

Artikel 9
Nutzung der Software in Privateigentum auf Geräten der Landesverwaltung

1. Um die Integrität des ISAPB zu schützen, darf kein Nutzer Software aus dem Privateigentum auf Geräten, die von der Landesverwaltung bereitgestellt werden, benutzen. Dies umfasst auch jene Anwendungen, die rechtmäßig gekauft und registriert worden sind, Shareware- sowie Freeware-Programme, jegliche vom Internet herunter geladene oder von einer

proprio lavoro su supporti magnetici e/o su dispositivi autorizzati. Non è consentito effettuare backup aggiuntivi su dispositivi e/o punti di memorizzazione diversi da quelli di cui sopra.

Articolo 7
Acquisto di hardware e software

1. Per prevenire l'introduzione di virus e/o altri programmi dannosi e per proteggere l'integrità della rete provinciale, tutto l'hardware ed il software in dotazione è autorizzato e gestito dalla Ripartizione Informatica e SIAG, salvo se concordato diversamente.

Articolo 8
Proprietà intellettuale e delle licenze

1. Tutto il software in uso deve essere ottenuto seguendo le procedure e le linee guida dell'Ente e deve essere registrato a nome dell'amministrazione provinciale o di SIAG. Ogni utente è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright), e non può installare, duplicare o utilizzare i vari software al di fuori di quanto consentito dagli accordi di licenza.

2. L'installazione e l'uso di software (App) sui dispostivi mobili (smartphone e tablet), sia BYOD che quelli di servizio, avviene sotto la completa responsabilità e gestione autonoma dell'utente stesso.

Articolo 9
Utilizzo del software di proprietà personale su dispositivi dell'ente

1. Al fine di proteggere l'integrità del SIPAB, nessun utente può utilizzare eventuale software di proprietà personale su dispositivi forniti e gestiti dall'Ente. Ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste

CD/DVD stammende Software als Beilage von Zeitschriften und Zeitungen oder sonstige unter jedem beliebigen Titel erworbene Software.

2. Die Landesverwaltung haftet nicht für die rechtswidrige Nutzung von Software auf persönlichen Geräten zur Durchführung der eigenen Arbeit (BYOD).

e/o giornali o altro software posseduto a qualsiasi titolo.

2. L'Ente non risponde di un utilizzo illecito di software su dispositivi di proprietà personale nello svolgimento del proprio lavoro (BYOD).

Artikel 10
Elektronische Post

1. Jedem Landesbediensteten wird ein Postfach für die persönliche elektronische Post zugeteilt. Eventuelle andere Postfächer für die elektronische Post werden auf Anfrage der Führungskräfte erstellt.

2. Die Zuweisung der E-Mail-Accounts schließt die Pflicht zur Nutzung dieses Kommunikationsmittels für die Abwicklung der eigenen Dienstanforderungen ein. Dies bedeutet, dass jede Nutzung desselben Mittels, welche nicht den Zielsetzungen der Verwaltung entspricht, verboten ist.

3. Der Versand von E-Mail-Nachrichten zu Arbeitszwecken mittels privater E-Mail-Dienste, die nicht von der Verwaltung bereitgestellt werden, ist nicht erlaubt.

4. Bei geplanten Abwesenheiten muss der Nutzer die Funktionalität der automatischen Antwort bei Abwesenheit aktivieren, mit Angabe der E-Mail-Adresse und/oder der Telefonnummer der eigenen Organisationseinheit für dringende Angelegenheiten.

5. Bei ungeplanten Abwesenheiten und auf jeden Fall bei unaufschiebbarer und unbedingter Notwendigkeit zur Aufrechterhaltung der Dienste, wird der Führungskraft des Nutzers die Zugangsmöglichkeit zu dessen E-Mail-Postfach ermöglicht, sofern dies vom zuständigen Abteilungsdirektor angefragt wird. Diese Maßnahme wird dokumentiert.

Articolo 10
Posta elettronica

1. A ogni dipendente provinciale viene assegnata una casella di posta elettronica personale. Eventuali altre caselle di posta elettronica vengono create su richiesta dei dirigenti.

2. L'assegnazione degli account di posta elettronica implica l'obbligo di utilizzo di tale mezzo di comunicazione per lo svolgimento dei propri doveri di ufficio, ciò significa che sono vietati tutti gli utilizzi di detto strumento non in conformità con gli scopi dell'Ente.

3. Non è consentito inviare messaggi di posta elettronica per scopi lavorativi utilizzando indirizzi di posta elettronica privati non forniti dall'Ente.

4. In caso di assenza programmata, l'utente deve utilizzare apposita funzionalità di risposta automatica con l'avviso di assenza dell'utente, indicante indirizzo e-mail e/o numero telefonico della struttura di appartenenza, per eventuali urgenze.

5. In caso di assenza non programmata e comunque per un'effettiva e improrogabile necessità di assicurare la continuità lavorativa, si rende possibile al dirigente l'accesso alla casella postale dell'utente assente, su richiesta da parte del direttore di ripartizione. Tale attività é documentata.

Artikel 11
Internet

1. Die Nutzer sind verpflichtet, die von der Landesverwaltung zur Verfügung gestellte

Articolo 11
Internet

1. Gli utenti sono tenuti ad utilizzare il collegamento ad Internet, fornito

Internetverbindung, hauptsächlich für die Ausübung ihrer Dienstpflicht zu verwenden. Daher ist verboten:

a) der Missbrauch bzw. andauerndes und wiederholtes Surfen auf Internetseiten, das nicht mit der Dienstausübung in Verbindung steht, von erlaubten Ausnahmen abgesehen. Die Landesverwaltung aktiviert über den technischen Zugriff von SIAG, Zugangsfilter für die Navigation im Internet. Dadurch wird der Zugang zu bestimmten Internetseiten beschränkt. Eventuelle zukünftige Änderungen der Zugangsfilter werden von der Generaldirektion bewertet. Zudem können aus Sicherheitsgründen eventuelle für die IT-Infrastruktur schädigende Webdienste und/oder Webseiten gesperrt werden;
b) die Sicherheit des ISAPB in irgendeiner Form zu gefährden, auch über die Abwicklung jeglicher Tätigkeit mit dem Ziel der Täuschung und Umgehung der Zugangssysteme und/oder der Sicherheitssysteme;
c) die Speicherung von Dateien in ISAPB, welche nicht dem Dienstgebrauch entsprechen.

2. Die Nutzung der Social Media durch das Landespersonal ist mit einer eigenen Leitlinie, welche von der Landesregierung mit Beschluss Nr. 282 vom 27.03.2018 festgelegt wurde, geregelt.

Artikel 12
Cloud computing

1. Die Landesverwaltung wird Instrumente für das cloud computing zur Verfügung stellen, dessen Nutzungsweise getrennt und in spezifischer Art und Weise in einem eigenen Dokument in der Sektion „IT-Sicherheit“ im Intranet spezifiziert ist.

2. Die Nutzung zusätzlicher Dienste des cloud computing für Arbeitszwecke ist erlaubt, sofern die Mindestsicherungsmaßnahmen respektiert werden und diese Nutzung vorab vom Dienst für die Sicherheit in der Informationstechnik der Landesverwaltung genehmigt wir.

dall’amministrazione provinciale, principalmente per motivi legati ai propri doveri di ufficio. Sono pertanto vietati:

a) L’abuso, ossia la prolungata e reiterata navigazione su siti non legati ad esigenze di tipo lavorativo ad eccezione di usi consentiti. L’amministrazione provinciale attiva, tramite l’intervento tecnico di SIAG, filtri di navigazione in internet. Di conseguenza l’accesso a determinate categorie di siti viene limitato. Eventuali variazioni dei filtri nel futuro verranno valutate dalla Direzione generale. Per motivi di sicurezza possono essere altresì inibiti i servizi web e/o la consultazione dei siti web potenzialmente lesivi per l’infrastruttura;
b) compromettere la sicurezza del SIPAB in qualsiasi modo anche tramite lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di sicurezza e/o accesso;
c) il salvataggio su SIPAB di file non legati ad un uso d’ufficio.

2. L’uso di social media da parte del personale provinciale è regolato dalle specifiche linee guida deliberate dalla Giunta Provinciale (Nr. 282 del 27/03/2018).

Articolo 12
Cloud computing

1. L’amministrazione provinciale mette a disposizione degli strumenti in cloud computing, le cui regole d’utilizzo saranno disciplinate separatamente in modo specifico nell’apposito documento nella sezione “sicurezza IT” in Intranet.

2. L’utilizzo di ulteriori servizi di cloud computing (applicativi e/o storage) per motivi lavorativi è ammesso a condizione che vengano rispettate le misure minime di sicurezza previa autorizzazione da parte del servizio di sicurezza informatica dell’amministrazione provinciale.

Artikel 13
Aufbewahrung der Verkehrsdaten

1. Gemäß Gesetz Nr. 167 vom 20.11.2017 bezüglich "Bestimmungen zur Erfüllung der sich aus der Mitgliedschaft Italiens in der Europäischen Union ergebenden Verpflichtungen", ist SIAG dazu verpflichtet, Informationen über den Internetverkehr und E-Mails für 72 Monate aufzubewahren, um wirksame Ermittlungsinstrumente, unter Berücksichtigung der außerordentlichen Erfordernisse der Terrorismusbekämpfung, einschließlich des internationalen Terrorismus, zur Aufklärung und Verfolgung von Straftaten, zu gewährleisten.

2. Zu diesem Zweck werden folgende Daten zum Internetverkehr (über Logs des Systems) gespeichert: Datum und Uhrzeit der Aktivität, IP und Port der Quelle, IP und Port der Zieladresse, Dauer der Kommunikation und ausgetauschte Byte der Kommunikation.

3. Zu diesem Zweck werden folgende Daten zum E-Mail-Verkehr über Logs des Systems gespeichert: Datum und Uhrzeit der Aktivität, E-Mail-Adresse des Absenders und des Empfängers sowie den Betreff der E-Mail.

4. Der Landesverwaltung ist es in jedem Fall untersagt, Zugang zu den gemäß diesem Artikel gespeicherten Daten zu erhalten. Die Verarbeitung der Daten durch SIAG beschränkt sich auf die für die technische Verwaltung der Informationssysteme unbedingt erforderlichen Vorgänge.

Artikel 14
Verstöße

1. Um die Verfügbarkeit und Integrität der Informations- und Kommunikations-systeme der Landesverwaltung zu gewährleisten behält sie sich das Recht vor, die korrekte Nutzung der informationstechnischen Instrumente und der Kommunikationsnetzwerke durch die Nutzer zu überprüfen. Dazu werden Maßnahmen ergriffen, die es ermöglichen abnormales Verhalten zu erkennen und auch nachträglich Sicherheitsverletzungen, Datenschutzverletzungen oder

Articolo 13
Conservazione dei dati di traffico

1. Ai sensi della L. 20.11.2017, n. 167, recante “Disposizioni per l’adempimento degli obblighi derivanti dall’appartenenza dell’Italia all’Unione europea”, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità di accertamento e della repressione dei reati, SIAG è tenuta a conservare le informazioni relative al traffico Internet e alla posta elettronica per un periodo pari a 72 mesi.

2. A tal fine le informazioni conservate relative al traffico internet (attraverso i log di sistema) sono: data e ora dell’evento, IP sorgente, porta sorgente, IP di destinazione, porta di destinazione, durata della comunicazione e byte scambiati durante la comunicazione.

3. A tal fine le informazioni conservate attraverso i log di sistema relative al traffico di posta elettronica sono: data e ora dell’evento, indirizzi di posta del mittente e del destinatario nonché oggetto della posta elettronica.

4. All’amministrazione provinciale è in ogni caso precluso l'accesso ai dati conservati in conformità del presente articolo. Il trattamento dei dati da parte di SIAG si limita alle operazioni strettamente necessarie alla gestione tecnica dei sistemi informatici.

Articolo 14
Violazioni

1. L’amministrazione si riserva il diritto di verificare il corretto impiego degli strumenti informatici e delle reti telematiche da parte degli utenti per garantire la disponibilità e l’integrità dei propri sistemi informativi e di comunicazione, adottando misure che consentano di individuare comportamenti anomali ed identificare anche a posteriori incidenti di sicurezza, violazioni delle policy o attività fraudolente e comunque nel pieno rispetto della normativa vigente in tema di protezione dei dati personali.

betrügerische Aktivitäten, in jedem Fall unter vollständiger Einhaltung der geltenden Rechtsvorschriften zum Schutz personenbezogener Daten, zu identifizieren.

2. Das Monitoring erfolgt auf aggregierte Daten; immer dann, wenn die Analyse einer Anomalie oder eines Problems es erforderlich machen, werden Kontrollen auch auf der Basis individueller Daten durchgeführt.

3. In Fällen eines festgestellten Verstoßes besagter Normen, ist die Anwendung der erforderlichen Disziplinarmaßnahmen den jeweiligen Führungskräften übertragen, mit der Verpflichtung etwaige Verstöße, die einen Strafbestand darstellen, der zuständigen Justizbehörde zu melden.

2. L'attività di monitoraggio si effettua su dati aggregati; laddove il tipo di anomalia e l'analisi del problema lo richiedesse, il controllo può avvenire anche su base individuale.

3. Nei casi di accertata violazione delle disposizioni del presente regolamento, è demandata ai rispettivi dirigenti l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituente reato.

V 4.4

Direktorin des Amtes für strategische IT-Ausrichtung und Planung
Direttrice dell'Ufficio orientamento stretegico e pianificazione IT
Daniela Secchi
(mit digitaler Unterschrift unterzeichnet / sottoscritto con firma digitale)

Generaldirektor / Direttore generale
Hanspeter Staffler
(mit digitaler Unterschrift unterzeichnet / sottoscritto con firma digitale)

Anlage A:
Information im Bezug zur Verarbeitung der personenbezogenen Daten

Allegato A:
Informativa relativa al trattamento dei dati personali

Anlage A
Information

Information im Bezug zur Verarbeitung der personenbezogenen Daten bezüglich der Nutzung von informationstechnische Dienste, dem Internet-Netzwerk und der elektronischen Post gemäß geltender Datenschutzbestimmungen (Datenschutz-grundverordnung EU Nr. 2016/679)

Mit Bezugnahme zur Organisationsrichtlinie zur Nutzung der informationstechnischen Dienste – einschließlich der persönlichen Software-anwendungen zur Nutzung für die Arbeit, bezeichnend „Bring your own device“ beziehungsweise „BYOD“ -, im Besonderen die Nutzung von Internet und der elektronischen Post, wird das Personal der Landesverwaltung darüber informiert, dass jede Verarbeitung ihrer personenbezogenen Daten gemäß folgender Vorschriften erfolgen wird:

1. *Objekt der Verarbeitung*: Informationen bezüglich der Nutzung von Internet, der elektronischen Post sowie der informationstechnischen Geräte, einschließlich der Geräte vom Typ “BYOD”. Eventuelle Aktionen vonseiten des Rechtsinhabers auf mobile Endgeräte, die für Arbeitszwecke verwendet werden, dienen nicht der Überwachung der Arbeitstätigkeit, sondern haben zum Ziel, die Vertraulichkeit der Daten auf dem Endgerät zu sichern. Diese Aktivitäten erfolgen ausschließlich auf Hinweis des Mitarbeiters bei Verlust oder Diebstahl des Endgerätes.
2. *Zweck der Datenverarbeitung*: Überprüfung der korrekten Internetnutzung, der elektronischen Post und der informationstechnischen Geräte zur Sicherstellung der Integrität, des reibungslosen Funktionierens, der Sicherheit der Informationssysteme und der Arbeit, sowie Kontrolle zur Feststellung von unrechtmäßigen Handeln der Mitarbeiter.
3. *Art der Datenverarbeitung*: Automatisch und manuell; die Verarbeitung wird von beauftragen Personen, in Kenntnis der geltenden gesetzlichen Bestimmunen, mittels geeigneten Maßnahmen zur Gewährleistung des Datenschutzes und zur Vorbeugung vor unbefugtem Zugriff durch Dritte, durchgeführt.
4. *Dauer der Aufbewahrung der Daten*: Auf der Intranetseite unter folgendem Pfad

Allegato A
Informativa

Informativa relativa al trattamento dei dati personali relativi all’utilizzo dei servizi informatici, della rete internet e della posta elettronica ai sensi della normativa vigente sulla protezione dei dati (regolamento europeo sulla protezione dei dati personali EU Nr. 2016/679)

Con riferimento al Disciplinare organizzativo per l’utilizzo dei servizi informatici - compresi gli applicativi di proprietà personale qualora adibiti ad uso lavorativo, segnatamente “Bring your own device” ovvero “BYOD” -, in particolare di Internet e della posta elettronica si informano i dipendenti che ogni trattamento dei loro dati personali avverrà nel rispetto delle seguenti disposizioni:

1. *Oggetto del trattamento*: informazioni relative all’utilizzo di Internet, della posta elettronica nonché degli strumenti informatici, comprensivi di “BYOD”. Le eventuali azioni da parte del titolare del trattamento su dispositivi mobili usato in ambito lavorativo, non sono finalizzate al controllo dell’attività lavorativa ma sono dirette a proteggere la riservatezza dei dati conservati sul device, e avvengono esclusivamente su segnalazione del dipendente in caso di smarrimento o furto del dispositivo mobile.

2. *Finalità del trattamento*: verifica del corretto utilizzo di Internet, posta elettronica e degli strumenti informatici a garanzia dell’integrità, del regolare funzionamento, della sicurezza dei sistemi informativi e del lavoro, nonché controlli diretti ad accertare comportamenti illeciti da parte dei dipendenti.

3. *Modalità del trattamento*: informatizzato e manuale, effettuato da soggetti autorizzati all’assolvimento di tali compiti, edotti dei vincoli imposti dalla normativa vigente e con misure atte a garantire la riservatezza dei dati ed evitare l’accesso ai dati stessi da parte di soggetti terzi non autorizzati.

4. *Durata di conservazione dei dati*: indicato nella pagina Intranet seguendo il seguente

angegeben: „IT Sicherheit / Unterlagen / Regelung Nutzung IT Dienste / Gestione dati utenti2“.

5. *Pflicht zur Übermittlung der Daten*: Für die Ausführung der oben genannten Pflichten notwendig, die Weigerung zur Datenverarbeitung kann zur Aufhebung des Vertragsverhältnisses führen.

6. *Rechte der Mitarbeiter*: Der/die Mitarbeiter/in hat das Recht, auf Zugang zu den eigenen Daten – auch durch Dritte, die bzw. den er/sie dazu ermächtigt oder spezifische Vollmacht erteilt hat, es steht ihm/ihr zudem das Recht auf Berichtigung oder Vervollständigung unrichtiger bzw. unvollständiger Daten zu; sofern die gesetzlichen Voraussetzungen gegeben sind, kann er/sie sich der Verarbeitung widersetzen oder die Löschung der Daten oder die Einschränkung der Verarbeitung verlangen. Das entsprechende Antragsformular steht auf der Webseite http://www.provinz.bz.it/de/transparente-verwaltung/zusaetzliche-infos.asp zur Verfügung. Im letztgenannten Fall dürfen die personenbezogenen Daten, die Gegenstand der Einschränkung der Verarbeitung sind, von ihrer Speicherung abgesehen, nur mit Einwilligung des Mitarbeiters/der Mitarbeiterin, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Rechtsinhabers, zum Schutz der Rechte Dritter oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden. Erhält der Mitarbeiter/die Mitarbeiterin auf seinen/ihren Antrag innerhalb von 30 Tagen nach Eingang keine Rückmeldung, – diese Frist kann um weitere 60 Tage verlängert werden, wenn dies wegen der Komplexität oder wegen der hohen Anzahl von Anträgen erforderlich ist - kann er/sie Beschwerde bei der Datenschutzbehörde oder Rekurs bei Gericht einlegen.

7. *Rechtsinhaber der Datenverarbeitung*: Die Autonome Provinz Bozen – Südtirol mit Sitz in Silvius-Magnago-Platz Nr. 4, Landhaus 3a, 39100, Bozen.
   E-Mail: generaldirektion@provinz.bz.it
   PEC: generaldirektion.direzionegenerale@pec.prov.bz.it

8. *Datenschutzbeauftragte (DSB)*: Die Kontaktdaten der DSB der Autonomen Provinz Bozen sind folgende: Autonome Provinz Bozen, Landhaus 1, Organisationsamt, Silvius-Magnago-Platz Nr. 1, 39100 Bozen.

percorso: “Sicurezza IT / Materiale / Disciplinare uso servizi IT / Gestione dati utenti2”.

5. *Obbligatorietà del conferimento dati*: in quanto indispensabile per l’assolvimento degli obblighi di cui sopra; pertanto, l’opposizione al trattamento potrebbe comportare l’impossibilità di prosecuzione del rapporto.

6. *Diritto del dipendente*: Il/la dipendente ha diritto di ottenere, con richiesta, anche mediante terzi cui abbia conferito delega o procura specifica, l’accesso ai propri dati, la rettifica o l’integrazione degli stessi qualora siano inesatti o incompleti, e, ricorrendone gli estremi di legge, opporsi al loro trattamento, richiederne la cancellazione o la limitazione del trattamento. Il modulo di richiesta, è disponibile alla seguente pagina web: http://www.provincia.bz.it/it/amministrazione-trasparente/dati-ulteriori.asp. In tale ultimo caso, esclusa la conservazione, i dati personali, oggetto di limitazione del trattamento, potranno essere trattati solo con il consenso del/della dipendente, per l’esercizio giudiziale di un diritto del titolare, per la tutela dei diritti di un terzo ovvero per motivi di rilevante interesse pubblico. In caso di mancata risposta entro il termine di 30 giorni dalla presentazione della richiesta, salvo proroga motivata fino a 60 giorni per ragioni dovute alla complessità o all’elevato numero di richieste, Il/la dipendente può proporre reclamo all’Autorità Garante per la protezione dei dati o inoltrare ricorso all’autorità giurisdizionale.

7. *Titolare del trattamento*: La Provincia autonoma di Bolzano - Alto Adige con sede in piazza Silvius Magnago 4, Palazzo 3a, 39100 Bolzano.
   e-mail: direzionegenerale@provincia.bz.it
   PEC: generaldirektion.direzionegenerale@pec.prov.bz.it

8. *Responsabile della protezione dei dati*: I dati di contatto del responsabile della protezione dei dati della Provincia autonoma di Bolzano sono i seguenti: Provincia autonoma di Bolzano, Palazzo 1, Ufficio Organizzazione, Piazza Silvius Magnago 1, 39100 Bolzano.

E-Mail: dsb@provinz.bz.it
PEC: rpd_dsb@pec.prov.bz.it

9. *Mit der Verarbeitung personenbezogener Daten betraute Personen*: Als solche gelten in Bezug auf die in ihre Zuständigkeit fallenden Angelegenheiten und Funktionen administrativer, finanzieller und technischer Verwaltung auch die Ressortdirektoren, wenn sie die Aufgaben eines Abteilungsleiters wahrnehmen und/oder übernehmen:
   a) die Abteilungsdirektoren,
   b) die Amtsdirektoren,
   c) die Führungskräfte, einschließlich jener der Hilfskörperschaften.
10. *Empfänger der Daten*:
   a) Das Unternehmen „Südtiroler Informatik AG“, als (externer) Auftragsverarbeiter für die Verwaltung des Informationssystems der Autonomen Provinz,
   b) das Unternehmer Microsoft Italia, als (externer) Auftragsverarbeiter für die Datenverarbeitung zum Zweck der Verwaltung von Office 365 und als Cloud-Dienst Provider, welcher sich aufgrund des bestehenden Vertrags verpflichtet hat, personenbezogene Daten nicht außerhalb der Europäischen Union und der Länder des Europäischen Wirtschaftsraums (Norwegen, Island, Lichtenstein) zu übermitteln,
   c) Gerichtsbehörde- oder Polizei im Falle eines besonderen Ersuchens oder zum Zwecke der Vorbeugung oder Feststellung von zivil-, straf- und verwaltungsrechtlichen Straftaten sowie zur Ausübung und Verteidigung eines Rechts in Gerichtsverfahren.
11. *Ermächtigte Mitarbeiter*: Alle Mitarbeiter werden vom Rechtsinhaber zur Verarbeitung der personenbezogenen Daten ermächtigt. Sie müssen sich an die Vorgaben halten. Die Angaben zum erlaubten Verarbeitungsbereiches erfolgen schriftlich.
12. *Automatisierte Entscheidungsfindung*: Die Verarbeitung der Daten stützt sich nicht auf eine automatisierte Entscheidungsfindung.

e-mail: rpd@provincia.bz.it
PEC: rpd_dsb@pec.prov.bz.it

9. *Preposti al trattamento*: di dati personali relative alle materie di rispettiva competenza e alle funzioni di gestione amministrativa, finanziaria e tecnica sono i direttori di dipartimento, nel caso svolgano le funzioni di direttori di ripartizione o avochino a sé atti di spettanza dei direttori di ripartizione:

   a) i direttori di ripartizione;
   b) i direttori di ufficio;
   c) i dirigenti, ivi compresi i dirigenti degli enti strumentali.
10. *Destinatari dei dati*:
   a) la Società “Alto Adige Informatica Spa”, responsabile (esterno) dei trattamenti effettuati ai fini della gestione del Sistema Informatico della Provincia autonoma di Bolzano;
   b) la Società Microsoft Italia, responsabile (esterno) dei trattamenti effettuati in qualità di provider di servizi cloud ai fini della fornitura del servizio di gestione del sistema Office 365, che si è impegnata in base al contratto in essere a non trasferire dati personali al di fuori dell’Unione Europea e i Paesi dell’Area Economica Europea (Norvegia, Islanda e Liechtenstein);

   c) l’autorità o alla polizia giudiziaria in caso di specifica richiesta, ovvero per finalità di prevenzione o accertamento di illeciti civili, penali ed amministrativi, nonché di esercizio e difesa di un diritto in sede giudiziaria.

11. *Dipendenti autorizzati*: Tutti i dipendenti sono autorizzati dal titolare a compiere le operazioni di trattamento di dati personali, attenendosi alle istruzioni loro impartite. L’individuazione dell’ambito del trattamento consentito è effettuata per iscritto.

12. *Processo decisionale automatizzato*: Il trattamento dei dati non si fonda su un processo decisionale automatizzato.