V 3.0

Autonome Provinz Bozen – Südtirol

Regelung zur Nutzung der IT-Dienste

Provincia autonoma di Bolzano – Alto Adige

Disciplinare per l'utilizzo dei servizi informatici

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.

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.

Artikel 2
Begriffsbestimmung

1. In dieser Regelung bezeichnet der Ausdruck:
   a) ***ISAPB (Informationssystem der Autonomen Provinz Bozen):***
   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) ***Nutzer***:
   alle Nutzerinnen und Nutzer des ISAPB, sowohl im lokalen Netzwerk innerhalb der Landesverwaltung als auch über einen Internet-Zugang,
   c) ***Cloud Computing*** (Datenwolke):
   Speicherung, Bearbeitung und Nutzung der Daten auf Remote Computern und ihre Nutzung über Internet,
   d) ***SIAG***:
   Südtiroler Informatik AG – Informatica Alto Adige S.p.A.,
   e) ***BYOD***:

Articolo 2
Definizioni

1. Ai fini del presente disciplinare valgono le seguenti definizioni:
   a) ***SIPAB*** (***Sistema Informativo della Provincia Autonoma di Bolzano)***:
   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 disponibili in modalità *cloud computing*, in dotazione e uso all'Amministrazione;
   b) ***utente***:
   chiunque utilizzi il SIPAB, sia che il collegamento avvenga in rete locale che in Internet;
   c) ***cloud computing*** (nuvola informatica):
   archiviazione, elaborazione e uso di dati su computer remoti e relativo utilizzo via Internet;
   d) ***SIAG***:
   Südtiroler Informatik AG – Informatica Alto Adige S.p.A.;
   e) ***BYOD***:

„bring your own device“ – Verwendung des persönlichen Gerätes durch den Nutzer zur Durchführung der eigenen Arbeit.

Artikel 3
Pflichten

1. Die IT-Geräte, die Programme und sämtliche Funktionen, die die Verwaltung ihren Nutzern zwecks Nutzung der ISAPB-Dienste, insbesondere der Internet- und E-Mail-Dienste zur Verfügung stellt, müssen in strikter Einhaltung der Bestimmungen dieser Regelung verwendet werden, um mögliche steuerliche und finanzielle Schäden sowie Image-Schäden für die Verwaltung zu vermeiden.
2. Das von den Bestimmungen dieser Regelung betroffene Personal ist angehalten, das Call Center zu kontaktieren, bevor irgendeine Tätigkeit ausgeführt wird, die nicht ausdrücklich durch diese Bestimmungen geregelt ist. Dadurch soll sichergestellt werden, dass diese Tätigkeit nicht im Widerspruch zu den von der Verwaltung festgelegten Datensicherheitsstandards steht.

Artikel 4
Zuständigkeiten und Verantwortung

1. Die Führungskräfte der verschiedenen Dienste (z.B.: Abteilungsdirektoren und Abteilungsdirektorinnen, Schuldirektoren und Schuldirektorinnen, Datenschutz-verantwortliche...) sind verpflichtet:
   a) das Personal über die Bestimmungen zur zulässigen Nutzung der Ressourcen des ISAPB zu informieren,
   b) zu gewährleisten, dass sich das ihnen zugewiesene Personal an die in dieser Regelung beschriebenen Bestimmungen und Vorgehensweisen hält,
   c) allen Pflichten nachzukommen, die von den geltenden Bestimmungen, insbesondere im Bereich Datenschutz, vorgesehen sind.
2. Jede Führungskraft muss gewährleisten, dass das ihr zugewiesene Personal mit Programmier- und System-administratoraufgaben sich bei der Ausübung seiner Tätigkeit an diese Regelung und insbesondere an die von der Aufsichtsbehörde erlassenen

“bring your own device” – utilizzo da parte dell’utente del proprio dispositivo personale nello svolgimento del proprio lavoro.

Articolo 3
Obblighi

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 Internet e posta elettronica, devono essere utilizzati nel pieno rispetto delle norme del presente disciplinare, al fine di evitare all’Amministrazione possibili danni erariali, finanziari e di immagine.
2. Tutto il personale interessato dalle prescrizioni del presente disciplinare è tenuto a contattare il Call Center prima di intraprendere qualsiasi attività non espressamente regolamentata nelle seguenti disposizioni, in modo da assicurarsi che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall’Amministrazione.

Articolo 4
Competenze e responsabilità

1. Le direttrici e i direttori dei vari servizi (p. es. direttrici e direttori di ripartizione, dirigenti scolastici, responsabili del trattamento dei dati ecc.) sono tenuti a:
   a) informare il personale sulle disposizioni in merito all’uso consentito delle risorse del SIPAB;
   b) assicurare che il personale a loro assegnato si uniformi alle regole ed alle procedure descritte nel presente disciplinare;
   c) adempiere a tutti gli obblighi previsti dalla normativa vigente, in particolare in materia di protezione dei dati personali.
2. Ogni dirigente deve garantire che il personale a lei/a lui assegnato con funzioni di programmatore e/o amministratore di sistema uniformi le proprie attività alle regole ed alle procedure descritte nel presente disciplinare, e in particolar modo alle disposizioni emanate dall’Autorità

Datenschutzbestimmungen hält; im Besonderen sind die Vorgaben der Maßnahme der Datenschutzbehörde („*Provvedimento del Garante del 27/11/2008*“) in Bezug auf die Systemadministratoren umzusetzen.

3. Alle Führungskräfte haben sicherzustellen, dass die Lieferanten und etwaiges beauftragtes externes Personal die vorliegende Regelung und die geltenden Bestimmungen, im Besonderen die Datenschutzbestimmungen, beachten.

4. Die SIAG in ihrer Eigenschaft als *In-House-Gesellschaft*, die IT-Leistungen im „O*utsourcing*“ liefert und als solche zum externen Verantwortlichen für die Verarbeitung ernannt, ist zur Einhaltung der geltenden Rechtsvorschriften verpflichtet, insbesondere der Datenschutzbestimmungen.
5. Der in der Abteilung Informationstechnik eingerichtete Sicherheitsdienst hat folgende Aufgaben:
   a) Ausarbeitung von Regelungen, die eine sichere Nutzung der Informatiksysteme und der Informationssysteme durch den Endanwender garantieren;
   b) Unterstützung bei der Vorbereitung von spezifischem und allgemein verständlichem Informationsmaterial zur IT-Sicherheit.
6. Die Nutzer sind verantwortlich für:

   a) die Einhaltung der Regelungen der Verwaltung für die zulässige Nutzung des ISAPB,
   b) die sofortige Meldung jeglicher nicht autorisierter Handlung, von der sie Kenntnis erlangt haben, im Besonderen bei Datenschutzverletzungen (*data breach*),
   c) jeden Gebrauch der ihnen anvertrauten Zugangsdaten (Benutzername, Kennwort).

Artikel 5
Rechtsinhaber

1. Die Landesverwaltung ist Inhaberin der gesamten ISAPB-Ressourcen.
2. Die Verwaltung informiert alle Nutzer über die zulässige und unzulässige Nutzung der genannten Ressourcen.

Garante per la protezione dei dati personali; in particolare devono essere attuati gli accorgimenti previsti dal Provvedimento del Garante del 27.11.2008 relativamente agli amministratori di sistema.

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

5. Il Servizio di sicurezza IT istituito presso la Ripartizione Informatica è tenuto a svolgere le seguenti attività:
   a) elaborazione delle regole per un utilizzo 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.

6. Gli utenti sono responsabili per quanto concerne:
   a) il rispetto delle regole dell’Amministrazione per l’uso consentito del SIPAB;
   b) la segnalazione immediata di ogni attività non autorizzata di cui siano venuti a conoscenza, in particolare nei casi di violazione di dati (*data breach*);

   c) ogni uso che venga fatto delle credenziali (nome utente, password) loro assegnate.

Articolo 5
Titolarità

1. L’Amministrazione provinciale è titolare di tutte le risorse del SIPAB.
2. L’Amministrazione informa ogni utente sugli usi consentiti e non consentiti di tali risorse.

Artikel 6
Benutzung der Hardware und Software

1. Der Nutzer verpflichtet sich, für die eigene Arbeit in der Regel Computer in Landeseigentum zu verwenden. Diese Geräte werden für Arbeitszwecke verwendet; jeder Missbrauch ist verboten.
2. Für den Zugriff auf die Hard- und Software ist ein komplexes Kennwort erforderlich. Ein Kennwort gilt dann als komplex, wenn es folgende Mindesteigenschaften hat:

   a) Mindestlänge von 10 Zeichen,
   b) es muss Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (z.B. '$', '.', '!' usw.) enthalten,
   c) das Kennwort muss sich von den fünf vorhergehenden Kennwörtern unterscheiden.
3. Das Kennwort verfällt nach drei Monaten und kann vom Nutzer jederzeit geändert werden; es muss verpflichtend geändert werden, wenn der Verdacht besteht, dass das Kennwort nicht mehr vertraulich und sicher ist.
4. Der Nutzer ist zur Abwicklung der eigenen Arbeit ermächtigt, persönliche Geräte zu verwenden (BYOD), sofern eine Benutzungsumgebung mit Mindestsicherheitsmaßnahmen gewährleistet wird, wie: Sperre des Geräts mit PIN oder komplexem Kennwort, installierte aktuelle Antivirensoftware. Wird das zur Arbeit genutzte persönliche Gerät (BYOD) verloren oder gestohlen, ist dies vom Nutzer umgehend dem Call Center zu melden, damit die eventuell erforderlichen zusätzlichen Maßnahmen zur Wahrung der Sicherheit ergriffen werden können.
5. Der Zugang zu Applikationen der Landesverwaltung wird durch entsprechende Nutzungsvorgaben (Disclaimer) geregelt, die angenommen und sorgsam befolgt werden müssen; ist dies nicht der Fall, wird der entsprechende Zugang verwehrt.

6. Der Nutzer darf weder die eigenen Benutzerdaten für den Zugang zum ISAPB-System preisgeben noch den Benutzernamen und das Kennwort von anderen Nutzern verwenden und darf keine Informationen weitergeben, die dem Amtsgeheimnis unterliegen.
7. Aus Sicherheitsgründen sind die Führungskräfte angehalten, für die Bediensteten, die mehr als einen Monat

Articolo 6
Utilizzo di hardware e software

1. L'utente si impegna ad utilizzare di regola, per il proprio lavoro, computer di proprietà provinciale. Dette macchine saranno utilizzate per scopi lavorativi; ogni abuso è vietato.
2. Per l'accesso all'hardware e al software è necessaria una password complessa. Per password complessa si intende una password con le seguenti caratteristiche minime:
   a) lunghezza minima di 10 caratteri;
   b) deve contenere caratteri maiuscoli, minuscoli, cifre e caratteri speciali (p.es. '$', '.', '!', ecc.);
   c) la password deve essere diversa dalle cinque password precedenti.

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

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

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

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

7. Per motivi di sicurezza le dirigenti e i dirigenti sono tenuti a richiedere tempestivamente al Call Center la

vom Dienst abwesend sind oder aus dem Dienst ausscheiden, schnellstmöglich die Deaktivierung des Accounts für den Zugang zum ISAPB zu beantragen. Meldet sich ein Nutzer für sechs Monate in Folge nicht bei der ISAPB–Domäne an, wird der entsprechende Account automatisch deaktiviert. Nach einem Jahr der Deaktivierung des Accounts, ausgenommen bei anderslautenden Anweisungen der Führungskraft, werden die im Intranet in der Rubrik „IT-Sicherheit“ in einem eigenen Dokument aufgelisteten Daten gelöscht.

8. Auf Anweisung der Abteilung Informationstechnik oder der SIAG verpflichtet sich der Nutzer, spezifische regelmäßige Backups der eigenen Arbeit auf elektronischen Datenträgern und/oder autorisierten Geräten durchzuführen. Es ist nicht erlaubt, zusätzliche Backups auf anderen als den genannten Speichergeräten und/oder Datenträgern vorzunehmen.

disattivazione dell’account d’accesso alle risorse del SIPAB per il personale assente dal servizio per più di un mese o che lascia il servizio definitivamente. Se un utente non esegue alcun login al dominio del SIPAB per sei mesi continuativi, il relativo account viene comunque disattivato automaticamente. Dopo un anno dalla disattivazione dell’account, e salvo diverse indicazioni del/della dirigente, i dati riportati in un apposito documento in Intranet, nella sezione “Sicurezza IT”, verranno cancellati.

8. Su indicazione della Ripartizione Informatica o di SIAG, l’utente si impegna ad effettuare backup specifici periodici del proprio lavoro su supporti magnetici e/o su dispositivi autorizzati. Non è consentito effettuare backup aggiuntivi su dispositivi e/o supporti diversi da quelli di cui sopra.

Artikel 7
Anschaffung von Hardware und Software

1. Zum Schutz vor Viren und anderen Schadprogrammen und um die Integrität des Landesnetzes aufrechtzuerhalten, wird die gesamte bereitgestellte Hard- und Software von der Abteilung Informationstechnik und der SIAG genehmigt und verwaltet, falls nicht anders vereinbart. Persönliche Hardware zur Durchführung der eigenen Arbeit (BYOD) muss der Nutzer unter eigener Verantwortung selbst verwalten.

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 da SIAG, salvo se concordato diversamente. L’uso di hardware privato per il proprio lavoro (BYOD) avviene sotto la completa responsabilità e gestione dell’utente stesso.

Artikel 8
Geistiges Eigentum und Lizenzen

1. Die gesamte genutzte Software muss nach den Vorgehensweisen und den Richtlinien der Verwaltung erworben und auf den Namen der Landesverwaltung oder der SIAG registriert werden. Jeder Nutzer ist zur Einhaltung der Gesetze im Bereich Schutz des geistigen Eigentums (Copyright) verpflichtet und darf sämtliche Software außerhalb der Lizenzbestimmungen weder installieren noch kopieren oder nutzen.

Articolo 8
Proprietà intellettuale e licenze

1. Tutto il software in uso deve essere acquisito seguendo le procedure e le linee guida dell’Amministrazione 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.

Artikel 9
Nutzung privater Software auf Geräten der Landesverwaltung

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

Artikel 10
Elektronische Post

1. Jedem Nutzer wird ein persönliches Postfach für die elektronische Post zugeteilt. Eventuelle andere Postfächer für die elektronische Post werden auf Anfrage der Führungskräfte erstellt.
2. Die Zuweisung der E-Mail-Accounts verpflichtet zur Nutzung dieses Kommunikationsmittels für die Wahrnehmung der Dienstpflichten. Jeder Missbrauch dieses Mittels ist verboten.
3. Nicht erlaubt ist das Senden von E-Mail-Nachrichten zu Arbeitszwecken über private E-Mail-Adressen, die nicht von der Verwaltung bereitgestellt werden.
4. Bei geplanten Abwesenheiten muss der Nutzer die Funktion der automatischen Antwort bei Abwesenheit aktivieren, mit Angabe einer E-Mail-Adresse und/oder Telefonnummer der eigenen Organisationseinheit für dringende Angelegenheiten.
5. Bei ungeplanten Abwesenheiten und auf jeden Fall bei unaufschiebbarer und tatsächlicher Notwendigkeit, den Dienst aufrechtzuerhalten, wird der Führungskraft der Zugang zum E-Mail-Postfach des abwesenden Nutzers ermöglicht, sofern dies vom zuständigen Abteilungsdirektor/von der zuständigen Abteilungsdirektorin beantragt wird. Diese Maßnahme wird dokumentiert.

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

1. Al fine di proteggere l'integrità del SIPAB, nessun utente può utilizzare software di proprietà personale su dispositivi forniti e gestiti dall'Amministrazione provinciale. 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 e/o giornali o altro software posseduto a qualsiasi titolo.
2. L'Amministrazione provinciale non risponde dell'utilizzo illecito di software su dispositivi di proprietà personale nello svolgimento del proprio lavoro (BYOD).

Articolo 10
Posta elettronica

1. A ogni utente viene assegnata una casella di posta elettronica personale. Eventuali altre caselle di posta elettronica vengono create su richiesta delle e 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. È vietato qualsiasi abuso di detto strumento.
3. Non è consentito inviare messaggi di posta elettronica per scopi lavorativi utilizzando indirizzi di posta elettronica privati non forniti dall'Amministrazione.
4. In caso di assenza programmata, l'utente deve utilizzare l'apposita funzione di risposta automatica con l'avviso di assenza, indicante un indirizzo e-mail e/o un 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 del servizio, il/la dirigente può avere accesso alla casella postale dell'utente assente, su richiesta del direttore/della direttrice di ripartizione competente. Tale attività è documentata.

Artikel 11
Internet

1. Die Nutzer sind verpflichtet, die von der Landesverwaltung zur Verfügung gestellte Internetverbindung vorwiegend zur Ausübung ihrer Dienstpflicht zu verwenden. Daher ist Folgendes verboten:
   a) das Surfen auf Internetseiten für Zwecke, die nicht den Dienstanforderungen entsprechen, von erlaubten Ausnahmen abgesehen. Hierfür können für die IT-Infrastruktur potenziell schädigende Webdienste und/oder Websites gesperrt werden,
   b) die Sicherheit des ISAPB in irgendeiner Form zu gefährden, auch über die Abwicklung jeglicher Tätigkeit mit der Absicht, die Zugangssysteme und/oder die Sicherheitssysteme zu täuschen oder zu umgehen,
   c) die Speicherung im ISAPB von Dateien, die nicht für dienstliche Zwecke verwendet werden.

Artikel 12
Cloud Computing

1. Die Landesverwaltung wird Instrumente für das Cloud Computing zur Verfügung stellen, dessen Nutzungsweise getrennt geregelt und in einem eigenen Dokument im Intranet in der Rubrik „IT-Sicherheit“ zur Verfügung gestellt wird.
2. Die Nutzung zusätzlicher Dienste des Cloud Computings (Anwendungen und/oder Storage) für Arbeitszwecke ist nur unter der Bedingung erlaubt, dass die Mindestsicherheitsmaßnahmen eingehalten werden und die Nutzung vorab vom Dienst für die IT-Sicherheit der Landesverwaltung genehmigt wird.

Artikel 13
Aufbewahrung von Verkehrsdaten

1. Folgende Daten über den Internetverkehr werden über Logs des Systems gespeichert: Datum und Uhrzeit der Aktivität, IP und Port der Quelle, IP und Port der Zieladresse, Dauer der Kommunikation und während der Kommunikation ausgetauschte Bytes.
2. Folgende Daten über den E-Mail-Verkehr werden über Logs des Systems gespeichert: Datum und Uhrzeit der

Articolo 11
Internet

1. Gli utenti sono tenuti ad utilizzare il collegamento ad Internet fornito dall'Amministrazione provinciale principalmente per motivi legati ai propri doveri di ufficio. È pertanto vietato:
   a) navigare su siti non legati ad esigenze di tipo lavorativo ad eccezione di usi consentiti. A tal fine possono essere 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.

Articolo 12
Cloud computing

1. L'Amministrazione provinciale mette a disposizione strumenti in cloud computing, le cui regole d'utilizzo saranno disciplinate separatamente in un apposito documento consultabile in Intranet nella sezione "Sicurezza IT".
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 e previa autorizzazione da parte del Servizio di sicurezza IT dell'Amministrazione provinciale.

Articolo 13
Conservazione dei dati di traffico

1. I dati relativi al traffico Internet conservati attraverso i log di sistema sono i seguenti: data e ora dell'attività, IP sorgente, porta sorgente, IP di destinazione, porta di destinazione, durata della comunicazione e byte scambiati durante la comunicazione.

2. I dati relativi al traffico di posta elettronica conservati attraverso i log di sistema sono i seguenti: data e ora dell'attività, indirizzi di

Aktivität, E-Mail-Adresse des Absenders und des Empfängers sowie Betreff der E-Mail.

3. Die Dauer der Aufbewahrung, gemäß den geltenden Rechtsbestimmungen, der Daten betreffend den Internet- und den E-Mail-Verkehr ist in einem eigenen Dokument in der Rubrik „IT-Sicherheit“ im Intranet angegeben.

posta del mittente e del destinatario nonché oggetto della posta elettronica.

3. Il periodo di conservazione, ai sensi della normativa vigente, dei dati relativi al traffico Internet e alla posta elettronica è indicato in un apposito documento consultabile in Intranet nella sezione “Sicurezza IT”.

Artikel 14
Verstöße

1. Die Landesverwaltung behält sich das Recht vor, die korrekte Nutzung der informationstechnischen Instrumente und der Kommunikationsnetzwerke durch die Nutzer zu überwachen, um die Verfügbarkeit und Integrität der eigenen Systeme der Informationstechnik und Kommunikation sicherzustellen. Dazu werden Maßnahmen ergriffen, welche nicht reguläres Verhalten erkennen lassen und auch im Nachhinein, Sicherheits-verletzungen, Verletzungen der Sicherheitsvorgaben oder betrügerische Aktivitäten überprüfen lassen. Dies alles erfolgt unter Beachtung der geltenden Datenschutzbestimmungen.
2. Das Monitoring wird auf aggregierten Daten vorgenommen; immer dann, wenn es die Art einer Anomalie oder die Analyse eines Problems erforderlich machen, werden Kontrollen auch auf der Basis individueller Daten durchgeführt.
3. Wird ein Verstoß gegen die Bestimmungen dieser Regelung festgestellt, werden die Maßnahmen angewandt, die von der Personalordnung und der Disziplinarordnung bzw. von den geltenden einschlägigen Bestimmungen vorgesehen sind.

Articolo 14
Violazioni

1. L’Amministrazione si riserva il diritto di monitorare 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 verificare comportamenti anomali e identificare, anche a posteriori, incidenti di sicurezza, violazioni delle policy o attività fraudolente. Ciò avviene comunque nel pieno rispetto della normativa vigente in materia di protezione dei dati personali.
2. L’attività di monitoraggio si effettua su dati aggregati; laddove il tipo di anomalia e l’analisi del problema lo richiedesse, il controllo avviene anche su base individuale.
3. Nei casi di accertata violazione delle disposizioni del presente disciplinare, si applicano le misure previste dall’ordinamento del personale e dall’ordinamento disciplinare, nonché dalla normativa vigente in materia.

Direktor der Abteilung Informationstechnik / Direttore della Ripartizione informatica
Kurt Pöhl
(mit digitaler Unterschrift unterzeichnet / sottoscritto con firma digitale)

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

Anlage A
Information

Information über die Verarbeitung der personenbezogenen Daten im Zusammenhang mit der Nutzung der informationstechnischen Dienste, des Internets und der elektronischen Post gemäß den geltenden Datenschutzbestimmungen

Mit Bezugnahme auf die Regelung zur Nutzung der IT-Dienste wird das Personal der Landesverwaltung darüber informiert, dass die Verarbeitung der eigenen personenbezogenen Daten gemäß folgenden Vorschriften erfolgt:

a) *Gegenstand der Verarbeitung* – Informationen bezüglich Nutzung des Internets, der elektronischen Post sowie der informationstechnischen Geräte, einschließlich „BYOD“. Eventuelle Eingriffe des Rechtsinhabers auf mobilen Endgeräten, die für Arbeitszwecke verwendet werden, dienen nicht der Überwachung der Arbeitstätigkeit an sich, sondern haben zum Ziel, die Vertraulichkeit der Daten auf dem Endgerät zu sichern; diese Eingriffe werden ausschließlich auf Hinweis des/der Bediensteten bei Verlust oder Diebstahl des mobilen Endgerätes vorgenommen.
b) *Zweck der Verarbeitung* – Überprüfung der korrekten Nutzung des Internets, der elektronischen Post und der informationstechnischen Geräte zur Sicherstellung der Integrität, des reibungslosen Funktionierens und der Sicherheit der Informationssysteme sowie Kontrollen, um rechtswidrige Handlungen der Bediensteten festzustellen (Schutzkontrollen).
c) *Art der Verarbeitung* – automatisch und manuell; die Verarbeitung wird von Beauftragten durchgeführt, die dazu ermächtigt und über die Beschränkungen laut den geltenden Bestimmungen informiert wurden; bei der Verarbeitung werden geeignete Maßnahmen zur Gewährleistung des Datenschutzes und zur Vermeidung von unbefugtem Zugriff durch Dritte getroffen.
d) *Pflicht zur Weiterleitung von Daten* – da die Weiterleitung der Daten für die Erfüllung der obengenannten Pflichten unerlässlich ist, kann bei Weigerung das

Allegato A
Informativa

Informativa sul 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

Con riferimento al disciplinare per l'utilizzo dei servizi informatici si informano le dipendenti e i dipendenti dell'Amministrazione provinciale che il trattamento dei loro dati personali avviene nel rispetto delle seguenti disposizioni:
a) *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 usati 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/della dipendente in caso di smarrimento o furto del dispositivo mobile.

b) *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, nonché controlli diretti ad accertare comportamenti illeciti da parte delle e dei dipendenti (controlli difensivi).

c) *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 e a evitare l'accesso ai dati stessi da parte di soggetti terzi non autorizzati.

d) *Obbligatorietà del conferimento dati* – in quanto indispensabile per l'assolvimento degli obblighi di cui sopra, l'opposizione al trattamento può comportare l'impossibilità

Vertragsverhältnis unterbrochen werden.

e) *Der/Die Bedienstete hat das Recht,* auf Anfrage – auch durch eine dritte natürliche Person, eine Körperschaft, einen Verein, die bzw. den er/sie dazu bevollmächtigt hat, Zugang zu den eigenen Daten, Auszüge und Auskunft darüber zu erhalten, und, sofern die gesetzlichen Voraussetzungen vorliegen, sich der Verarbeitung zu widersetzen, deren Aktualisierung, Richtigstellung, Löschung, Anonymisierung oder Sperrung zu verlangen.

f) *Rechtsinhaber der Datenverarbeitung* ist die Autonome Provinz Bozen – Südtirol mit Sitz am Silvius-Magnago-Platz 1 in 39100 Bozen.

g) *Verantwortliche* für die Verarbeitung der personenbezogenen Daten sind, je nach Zuständigkeits- bzw. Aufgabenbereich,
   - die Abteilungsdirektoren / Abteilungs-direktorinnen,
   - die Amtsdirektoren/Amtsdirektorinnen,
   - die Führungskräfte, einschließlich jener der Hilfskörperschaften des Landes,
   - die „Südtiroler Informatik AG“, (externer) Verantwortlicher für die von ihr vorgenommene Datenverarbeitung zum Zweck der Verwaltung der Informationssysteme der Autonomen Provinz Bozen.

h) *Beauftragter der Verarbeitung* ist jene natürliche Person, die vom Rechtsinhaber zur Verarbeitung der personenbezogenen Daten ermächtigt wird. Der Beauftragte muss sich an die Vorgaben des Rechtsinhabers und des für die Verarbeitung Verantwortlichen halten. Die Beauftragung erfolgt schriftlich und definiert im Einzelnen den erlaubten Verarbeitungsbereich.

di prosecuzione del rapporto contrattuale.

e) *Il/La dipendente ha diritto* di ottenere, su richiesta, anche tramite una terza persona fisica, un ente, un'associazione cui abbia conferito delega o procura specifica, l'accesso ai propri dati, l'estrapolazione ed informazioni su di essi nonché, ricorrendone gli estremi di legge, opporsi al trattamento, richiederne l'aggiornamento, la rettifica, la cancellazione, la trasformazione in forma anonima o il blocco.

f) *Titolare del trattamento* è la Provincia autonoma di Bolzano - Alto Adige, con sede in piazza Silvius Magnago, 1 – 39100 Bolzano.

g) *Responsabili* del trattamento dei dati personali sono, per le materie di rispettiva competenza e le rispettive funzioni:
   - le direttrici e i direttori di ripartizione,
   - le direttrici e i direttori di ufficio,
   - le dirigenti e i dirigenti, compresi quelli degli enti strumentali della Provincia,
   - la Società "Alto Adige Informatica Spa", responsabile (esterno) dei trattamenti dalla stessa effettuati ai fini della gestione del Sistema Informativo della Provincia autonoma di Bolzano.

h) *Incaricato del trattamento* è la persona fisica autorizzata dal titolare a compiere le operazioni di trattamento dei dati personali, attenendosi alle istruzioni impartite dal titolare e dal responsabile. L'incarico è affidato per iscritto e individua puntualmente l'ambito del trattamento consentito.