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 diese Verordnung gelten folgende Begriffsbestimmungen:

a) 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) Nutzer: Jeder der ISAPB nutzt, sowohl im lokalen Netzwerk innerhalb der Landesverwaltung als auch über einen Internet-Zugang,

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/le dipendenti provinciali, il personale delle scuole a carattere statale, i/le 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 sensi del presente regolamento si intende per:

a) 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) utente: chiunque utilizzi il SIPAB, sia che il collegamento avvenga in rete locale che in internet;

c) *cloud computing* (Datenwolke):
Die Speicherung, die Bearbeitung und die Nutzung der Daten auf remote Computern und deren Nutzung über Internet,

d) SIAG: Südtiroler Informatik AG - Informatica Alto Adige S.p.A,

e) BYOD "*bring your own device*" - Verwendung eigener Privatgeräte zur Erbringung der Arbeitsleitung auch im Smart Working Modus,

f) Smart Working: eine Form der Durchführung der Arbeitsleistungen ohne Regelungszwänge bezüglich Arbeitsorten und flexiblen Arbeitszeiten, wobei die Arbeitsorganisation nach Zielen gegliedert ist, die in einer Vereinbarung zwischen Bediensteten und der zuständigen Führungskraft festgehalten werden und auch eigene persönliche IT-Instrumente verwendet werden.

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

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

e) BYOD "*bring your own device*" - utilizzo da parte dell'utente del proprio dispositivo personale nello svolgimento del proprio lavoro, anche in modalità smart working;

f) smart working: una modalità di svolgimento della prestazione lavorativa caratterizzata da flessibilità oraria e assenza di vincoli spaziali improntata al raggiungimento di obiettivi, le cui effettive modalità vengono determinate da un accordo individuale tra dipendente e dirigente, anche mediante l'utilizzo di strumenti di informazione e comunicazione elettronica di proprietà personale.

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 dieser Verordnung 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'amministrazione stessa.

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'amministrazione.

Artikel 4
Zuständigkeiten und Verantwortung

Articolo 4
Competenze e responsabilità

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 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:

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’Amministrazione provinciale;

b) garantire che il personale a loro assegnato si uniformi alle regole ed alle procedure descritte nel presente regolamento;

c) adempiere a tutti gli obblighi previsti dalla normativa vigente, ed 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, nonché 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*”, ed 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) Ausarbeitung von Regelungen, die eine angemessene sichere Nutzung der Informatiksysteme und der Informationssysteme vonseiten des Endnutzers garantieren,

a) elaborazione delle regole per un utilizzo ragionevolmente sicuro dei sistemi informatici e dei sistemi informativi, da parte dell'utente finale;

b) Unterstützung bei der Vorbereitung von spezifischem und allgemein verständlichem Informationsmaterial zur Datensicherheit.

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

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 bei Datenschutzverletzungen (*data breach*),

c) jeden Gebrauch der ihm anvertrauten Zugangsdaten (Benutzername, Kennwörter).

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 particolare nei casi di violazione di dati (*data breach*);

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

Artikel 5
Inhaberschaft

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. Dem Benutzer wird zu Arbeitszwecken in der Regel nur ein Gerät (PC oder Notebook) von der Verwaltung zur Verfügung gestellt, welches, auch in öffentlich zugänglichen Stätten, sorgfältig aufbewahrt werden muss.

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.

Articolo 6
Utilizzo di hardware e software

1. L'utente sarà dotato da parte dell'amministrazione, per scopi lavorativi, di regola, di un solo device (PC o notebook), che dovrà essere adeguatamente custodito, anche in luoghi pubblici.

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. 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. Für den Zugriff auf die SIPAB-Ressourcen von einem nicht vernetzten Standort aus, d.h. aus der Ferne (z.B. von zu Hause mit dem eigenen Internet-Netzwerk oder von einem beliebigen WLAN-Netzwerk aus), ist die Verwendung des Multi-Faktor-Authentifizierungssystems (MFA) erforderlich. Das System kann mittels der Eintragung auf der entsprechenden Seite benutzt werden, eventuell mit Hilfe des entsprechenden Handbuchs.

5. In gleicher Weise, um eine effizientere und schnellere Verwaltung des eigenen Passwords zu ermöglichen, ist jeder Benutzer angehalten, sich am Dienst „Self Service Password Reset“ zu registrieren.
6. Der Benutzer ist dazu ermächtigt, für die Durchführung der eigenen Arbeit, persönliche Geräte zu verwenden (BYOD), auch zwecks der Durchführung seiner Arbeitsleistung im Smart Working Modus, sofern unter der eigenen Verantwortung eine Nutzungsumgebung mit Mindestsicherungsmaßnahmen wie:
   a. Sperrung des Geräts mit PIN oder komplexem Password oder mit biometrischen Merkmalen (z. B. Fingerabdruck)
   b. regelmäßig installierte und aktualisierte Antivirensoftware/Firewall gemäß den Anweisungen des Dokuments.
   c. rechtzeitige Aktualisierung des Betriebssystems,
   d. Passwortverwaltung über Passwortmanager, gewährleistet wird.

7. Die oben genannten Regeln können sich nach der bevorstehenden Einführung von Tools zur Verwaltung mobiler Geräte ändern.

8. Wird das zur Arbeit genutzte persönliche Gerät (BYOD) verloren oder gestohlen, muss dies vom Benutzer umgehend dem Call Center mitgeteilt werden, damit die

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. Ai fini dell'accesso alle risorse del SIPAB da una postazione non in rete, ovvero da remoto (es. da casa con la propria rete Internet o da qualunque rete WiFi) è richiesto l'utilizzo del sistema di autenticazione a più fattori (MFA). L'utilizzo avviene previa registrazione alla pagina apposita, con l'eventuale ausilio del relativo manuale.

5. In modo analogo, per una gestione più snella ed efficiente della propria password, ogni utente provinciale è tenuto a registrarsi al servizio "Self Service Password Reset".
6. L'utente è autorizzato all'utilizzo di un dispositivo di proprietà personale per il proprio lavoro (BYOD), anche ai fini dello svolgimento della prestazione lavorativa in modalità smart working, purché garantisca, sotto la propria responsabilità, un ambiente d'uso rispondente a misure di sicurezza minime quali:
   a. il blocco del dispositivo con PIN o password complessa o tramite la biometria (per es. impronta digitale),
   b. antivirus/firewall regolarmente installato ed aggiornato come da indicazioni del documento;
   c. l'aggiornamento sistematico del relativo sistema operativo;
   d. la gestione delle password tramite Password Manager.

7. Le regole di cui sopra sono suscettibili di variazioni in seguito alla prossima adozione di strumenti di gestione dei dispositivi mobili.

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

erforderlichen Sicherheitsmaßnahmen getroffen werden können.

9. In gleicher Weise ist jeder Benutzer angehalten, eine Nutzungsumgebung mit einem Mindestmaß an Sicherheitsvorkehrungen für mobile Geräte (Smartphone und Tablet), welche von der Landesverwaltung dem eigenen Personal zur Verfügung gestellt werden, zu garantieren.

10. 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.

11. 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.

12. 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 werden gelöscht. Dieses Verfahren wird in dem eigenen Dokument beschrieben.

13. 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 oben angeführten,

adozione di ulteriori contromisure di sicurezza.

9. 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.

10. 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.

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

12. 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. Questa procedura è descritta nell'apposito documento.

13. 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 punti di memorizzazione diversi da quelli di cui sopra.

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
Geistiges Eigentum und 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 mobilen Geräten (Smartphone und Tablet), sowohl für jene des Typs BYOD als auch für die Dienstgeräte erfolgt, auch im Falle von Smart Working, 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 CD/DVD stammende Software als Beilage von Zeitschriften und Zeitungen oder sonstige unter jedem beliebigen Titel erworbene Software.

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, anche in caso di smart working, avviene sotto la completa responsabilità e gestione autonoma dell'utente stesso.

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 eventuale 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. Die Landesverwaltung haftet nicht für die rechtswidrige Nutzung von Software auf persönlichen Geräten zur Durchführung der eigenen Arbeit (BYOD) auch im Smart Working Modus.

2. L'Amministrazione provinciale non risponde di un utilizzo illecito di software su dispositivi di proprietà personale nello svolgimento del proprio lavoro (BYOD), anche in modalità smart working.

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. Ad 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'amministrazione.

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 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 è documentata.

Artikel 11
Internet

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

Articolo 11
Internet

1. Gli utenti sono tenuti ad utilizzare il collegamento ad Internet, fornito dall'Amministrazione provinciale,

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 stellt Instrumente für das *cloud computing* zur Verfügung, dessen Nutzungsweise getrennt und in spezifischer Art und Weise in einem eigenen Dokument in der Sektion „IT-Sicherheit“ im Intranet ist.

2. Die Nutzung zusätzlicher Dienste des *cloud computing* (Anwendungs- und/oder Speicherdienste) für Arbeitszwecke ist erlaubt, sofern das Mindestmaß an Sicherheitsvorkehrungen beachtet wird und diese Nutzung vorab vom Dienst für die

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 (n. 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.

Sicherheit in der Informationstechnik der Landesverwaltung genehmigt wird.

Artikel 13
Aufbewahrung der Verkehrsdaten

1. Gemäß Gesetz Nr. 167 vom 20.11.2017 betreffend die "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
Kontrollen für Organisations- und Produktionszwecke, Arbeitssicherheit sowie Schutz des Vermögens des Landes und Verstöße

1. Unbeschadet der Bestimmungen von Artikel 4, Absatz 1 des Gesetzes Nr. 300/1970 (Arbeiterstatut) behält sich die Verwaltung das Recht vor, auf nicht systematische,

Articolo 13
Conservazione dei dati di traffico

1. Ai sensi della legge n. 167 del 20.11.2017, 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 l’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
Attività di controllo per finalità organizzative, produttive, di sicurezza sul lavoro nonché di tutela del patrimonio dell’Amministrazione e violazioni

1. Fermo restando quanto previsto dall’articolo 4, comma 1, della legge n. 300/1970 (Statuto dei lavoratori), l’amministrazione si riserva il diritto di rilevare, in modo non

massive, verlängerte, kontinuierliche oder diskriminierte Weise, für Organisations- , Produktionszwecke (wie zum Beispiel die strategische und optimale Verwaltung der IT-Tools und der damit verbundenen Ressourceninvestitionen, die Überprüfung des reibungslosen Funktionierens, der Effizienz und Robustheit der elektronischen Netze, um die Sicherheit, Integrität, Verfügbarkeit der IT-Systeme zu gewährleisten, sowie um auch nachträglich Sicherheits- und Datenschutzverletzungen zu erkennen und zu identifizieren), Arbeitssicherheit, Schutz des Vermögens des Landes (einschließlich seiner Werte und Feststellung von unrechtmäßigen Handeln der Landesbediensteten bei Verletzung der Policy oder betrügerischen Aktivitäten), Zugangsdaten (logging), auf jeden Fall, immer unter Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten entsprechend der geltenden Bestimmungen, zu erheben.

sistematico, massivo, prolungato, continuativo e indiscriminato i dati relativi agli accessi (*logging*) del dipendente per finalità organizzative e produttive (come ad esempio la gestione strategica e ottimale degli strumenti informatici e dei relativi investimenti di risorse, le verifiche sulle funzionalità, efficienza e robustezza delle reti telematiche, per garantire la sicurezza, l'integrità e disponibilità dei sistemi IT, individuazione dei comportamenti anomali e identificazione, anche a posteriori, degli incidenti di sicurezza), di sicurezza sul lavoro e di tutela del patrimonio provinciale (protezione dei beni provinciali ed accertamento di condotte illecite per violazioni delle policy ed attività fraudolente) e comunque nel rispetto dei principi di trattamento dei dati conformemente alla normativa vigente.

2. Die Erhebung der Daten erfolgt in *anonymisierter oder pseudonymisierter Form* durch geeignete Aggregationen auf kollektiver Basis oder für ausreichend große Gruppen, um die sofortige Identifizierung der Landesbediensteten auszuschließen. Können die Zwecke auf diese Weise nicht erreicht werden, so kann die Erhebung auch auf individueller Basis unter Einhaltung der Grundsätze der Transparenz, Zweckbestimmung und Speicherung sowie der Minimierung personenbezogener Daten erfolgen, indem verhältnismäßige und nicht-invasive Maßnahmen zur Wahrung der Freiheit und Würde der Landesbediensteten ergriffen werden, wie zum Beispiel schrittweise und regelmäßige Überprüfungen, Zugang zu den Informationen nur für befugte Personen und mit persönlichen Berechtigungsnachweisen.

2. Le attività di cui al comma precedente si effettuano in forma anonima o pseudonima, tale da precludere l'immediata identificazione del dipendente mediante opportune aggregazioni su base collettiva o per gruppi sufficientemente ampi. Laddove le finalità non siano conseguibili con tali modalità, la rilevazione può avvenire anche su base individuale nel rispetto dei principi di trasparenza, limitazione della finalità e della conservazione, nonché di minimizzazione dei dati personali, adottando misure proporzionate e non invasive della libertà e dignità dei dipendenti, come ad esempio verifiche graduali e a cadenza periodica, accesso alle informazioni esclusivamente a persone all'uopo autorizzate e dotate di credenziali personali.

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.

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.

Anlage A: Datenschutzerklärung [Art. 13 der Datenschutz-Grundverordnung 2016/679 (in der Folge „DSGVO“)]

Mit Bezugnahme zur Organisationsrichtlinie zur Nutzung der informationstechnischen Dienste – einschließlich der persönlichen Softwareanwendungen zur Nutzung für die Arbeit, bezeichnend „b*ring your own device*“ beziehungsweise „BYOD“ und im Falle von Smart Working -, im Besonderen die Nutzung von Internet und der elektronischen Post, wird das Personal der Landesverwaltung darüber informiert, dass jede Verarbeitung seiner personenbezogenen Daten gemäß folgenden Vorschriften erfolgen wird:

Gegenstand der Verarbeitung: Erhebung von Informationen bezüglich der Nutzung von elektronischen Kommunikationsnetzen (Internet und der Dienste von Microsoft Office 365) sowie der elektronischen Post durch informationstechnische Geräte, die, zur Durchführung der Arbeitsleistung, auch im Smart Working Modus:

a) von der Landesverwaltung zur Verfügung gestellt werden
b) Privateigentum des Mitarbeiters (BYOD) sind.

Rechtliche Grundlage:
Art. 6, Abs 1, Buchstaben b), c) und e), Art. 88 der DSGVO, Art. 2086 und 2104 ZK, Art. 18-23 G. Nr. 81/2017, Art. 4 della L. 300/1970 (Arbeiterstatut).

Zweck der Datenverarbeitung:

a) Organisations- und Produktionszwecke wie zum Beispiel die strategische und optimale Verwaltung der IT-Tools und der damit verbundenen Ressourceninvestitionen, die Überprüfung des reibungslosen Funktionierens, um die Sicherheit, Integrität, Verfügbarkeit und die Robustheit der IT- Systeme und elektronischer Kommunikationsnetze der Landesverwaltung zu gewährleisten, sowie

Allegato A: Informativa relativa al trattamento dei dati personali [art. 13 Regolamento generale sulla protezione dei dati personali 2016/679 (d’ora in poi “RGPD”)]

Con riferimento al Disciplinare organizzativo per l’utilizzo dei servizi informatici - compresi gli applicativi di proprietà personale qualora adibiti ad uso lavorativo, segnatamente “b*ring your own device*” ovvero “BYOD” e in caso di smart working - in particolare di Internet (inclusi servizi di Microsoft Office 365) e della posta elettronica, si informano i dipendenti che ogni trattamento dei loro dati personali avverrà nel rispetto delle seguenti disposizioni:

Oggetto del trattamento: raccolta di informazioni relative all’utilizzo delle reti di comunicazione elettronica (Internet e servizi di Microsoft Office 365), nonché della posta elettronica, attraverso strumenti IT:

a) messi a disposizione dall’Amministrazione provinciale
b) di proprietà del dipendente (BYOD)

per svolgere la prestazione lavorativa, anche in modalità smart working.

Base giuridica:
Art. 6, par. 1, lett. b) e c), und e); art. 88 del RGPD, artt. 2086 e 2104 c.c., artt. 18-23 L. 81/2017, art. 4 della L. 300/1970 (Statuto dei lavoratori).

Finalità del trattamento:

a) organizzative e produttive, quali la gestione strategica e ottimale degli strumenti informatici e dei relativi investimenti di risorse, la verifica sulle funzionalità, la sicurezza, l’integrità, la disponibilità e la robustezza dei sistemi IT e delle reti di comunicazione elettronica, l’individuazione delle anomalie e l’identificazione di incidenti di sicurezza;
b) di sicurezza sul lavoro e

die Identifizierung von Sicherheits- und Datenschutzverletzungen,
b) Arbeitssicherheit und
c) Schutz des Vermögens des Landes (Schutz der Landeswerte und Kontrolle zur Feststellung von unrechtmäßigem Handeln der Mitarbeiter bei Verletzung der Policy oder betrügerischen Aktivitäten).

c) di tutela del patrimonio provinciale (protezione dei beni provinciali ed accertamento di condotte illecite per violazioni delle policy o attività fraudolente).

Art der Datenverarbeitung: Automatisch und manuell, die Verarbeitung wird von beauftragen Personen, denen die geltenden gesetzlichen Bestimmungen bekannt gemacht worden sind, mittels geeigneter Maßnahmen zur Gewährleistung des Datenschutzes und zur Vorbeugung vor unbefugtem Zugriff durch Dritte, durchgeführt. Die Erhebung der Daten erfolgt in *anonymisierter* oder *pseudonymisierter Form* durch geeignete Aggregationen auf kollektiver Basis oder für ausreichend große Gruppen, um die sofortige Identifizierung der Mitarbeiter auszuschließen. Können die Zwecke auf diese Weise nicht erreicht werden, so kann die Erhebung auch auf individueller Basis unter Einhaltung der Grundsätze zur Verarbeitung personenbezogener Daten erfolgen, indem Maßnahmen ergriffen werden, die angemessen sind und die Freiheit und Würde der Landesbediensteten nicht beeinträchtigen, wie zum Beispiel schrittweise und regelmäßige Überprüfungen, Zugang zu den Informationen nur für befugte Personen und mit persönlichen Berechtigungsnachweisen. In jedem Fall werden nur Daten erhoben, die dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind (Datenminimierung).

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 non consentire l'accesso ai dati stessi da parte di soggetti terzi non autorizzati. La rilevazione dei dati si effettua in forma anonima o pseudonima, tale da precludere l'immediata identificazione dei dipendenti mediante opportune aggregazioni su base collettiva o per gruppi sufficientemente ampi. Laddove le finalità non siano conseguibili con tali modalità, la rilevazione può avvenire anche su base individuale nel rispetto dei principi di trattamento dei dati personali adottando misure proporzionate e non invasive della libertà e dignità dei dipendenti, come, ad esempio, verifiche graduali ed a cadenza periodica, accesso alle informazioni a esclusivamente a persone all'uopo autorizzate e dotate di credenziali personali. In ogni caso sono rilevati solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle singole finalità perseguite (principio di minimizzazione dei dati).

Dauer der Verarbeitung: Auf der Intranetseite unter folgendem Pfad angegeben: „IT Sicherheit / Unterlagen / Regelung Nutzung IT Dienste / Gestione dati utenti2".

Durata del trattamento: indicato nella pagina Intranet seguendo il seguente percorso: "Sicurezza IT / Materiale / Disciplinare uso servizi IT / Gestione dati utenti2".

Verpflichtende Datenübermittlung: die Übermittlung der Daten ist unerlässlich, um die oben genannten Verpflichtungen zu erfüllen; ein Widerspruch gegen die Verarbeitung könnte zur Aufhebung des Vertragsverhältnisses führen.

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.

Rechte der Landesbediensteten: Der Landesbedienstete hat das Recht auf Zugang zu den eigenen Daten, auch durch Dritte, die

Diritto del dipendente: Il dipendente ha diritto di ottenere, con richiesta, anche mediante terzi cui abbia conferito delega o procura specifica,

dazu ermächtigt sind oder denen er eine eigene Vollmacht erteilt hat, es steht ihm zudem das Recht auf Berichtigung oder Vervollständigung unrichtiger bzw. unvollständiger Daten zu; sofern die gesetzlichen Voraussetzungen gegeben sind, kann er 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/transparenteverwaltung/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, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Verantwortlichen, zum Schutz der Rechte Dritter oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden. Erhält der Mitarbeiter auf seinen 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 Beschwerde bei der Datenschutzbehörde oder Rekurs bei Gericht einlegen.

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 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 dipendente può proporre reclamo all'Autorità Garante per la protezione dei dati o inoltrare ricorso all'autorità giurisdizionale.

Verantwortlich für die Datenverarbeitung: Die Autonome Provinz Bozen – Südtirol
E-Mail: generaldirektion@provinz.bz.it
PEC: generaldirektion.direzionegenerale@pec.prov.bz.it

Titolare del trattamento: La Provincia autonoma di Bolzano - Alto Adige
E-mail: direzionegenerale@provincia.bz.it
PEC: generaldirektion.direzionegenerale@pec.prov.bz.it

Datenschutzbeauftragte (DSB): Die Kontaktdaten der DSB der Autonomen Provinz Bozen sind folgende:
E-Mail: dsb@provinz.bz.it
PEC: rpd_dsb@pec.prov.bz.it

Responsabile della protezione dei dati: I dati di contatto del RPD sono i seguenti:
E-mail: rpd@provincia.bz.it
PEC: rpd_dsb@pec.prov.bz.it

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:
a) die Abteilungsdirektoren,
b) die Amtsdirektoren,

Preposti al trattamento di dati personali relativi alle materie di rispettiva competenza e alle funzioni di gestione amministrativa, finanziaria e tecnica sono:
a) i direttori di ripartizione;
b) i direttori d'ufficio;
c) i soggetti titolari di incarichi speciali di cui all'articolo 17-bis della legge provinciale 23 aprile 1992, n. 10 e successive modifiche,

c) die Personen, welchen Sonderaufträge im Sinne von Artikel 17-bis des Landesgesetzes Nr. 10 vom 23. April 1992 in geltender Fassung erteilt werden,
d) die Führungskräfte, einschließlich jener der Hilfskörperschaften.

d) i dirigenti, ivi compresi i dirigenti degli enti strumentali.

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, Liechtenstein) ohne die geeigneten Garantien gemäß Abschnitt V der DSGVO 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.

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 Microsoft Office 365, che si è impegnata in base al contratto in essere a non trasferire dati personali al di fuori dell’Unione Europea e dei Paesi dell’Area Economica Europea (Norvegia, Islanda e Liechtenstein), senza le adeguate garanzie di cui al capo V del RGPD;
c) l’autorità o la 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.

Ermächtigte Landesbedienstete: Alle Landesbediensteten werden vom Verantwortlichen und von den Auftragsverarbeitern zur Verarbeitung der personenbezogenen Daten ermächtigt. Sie müssen sich an die ihnen erteilten schriftlichen Anweisungen halten.

Dipendenti autorizzati: Tutti i dipendenti sono autorizzati dal titolare e dai responsabili del trattamento a compiere le operazioni di trattamento di dati personali, attenendosi alle istruzioni scritte loro impartite.

Automatisierte Entscheidungsfindung: Die Verarbeitung der Daten stützt sich nicht auf eine automatisierte Entscheidungsfindung.

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