Richtlinie zum Datenschutz und zur IT-Sicherheit

IT Sicherheit geht uns alle an!
Jeder Mitarbeiter verarbeitet täglich Daten elektronisch. Hierbei handelt es sich um Kundendaten, personenbezogene Daten, Finanzdaten bis hin zu besonders schützenswerten Daten. Manche dieser Daten dürfen keinesfalls in Hände Dritter fallen – sei es aus Gründen des Datenschutzes oder weil es sich um vertrauliche Unternehmensdaten handelt. Datensicherheit im Allgemeinen und speziell IT-Sicherheit sind daher unverzichtbar für unseren Erfolg. Unternehmensdaten müssen bestmöglich geschützt werden. Dies gilt sowohl für den Versuch, diese Daten auszuspionieren, als auch für die Gefahr des Datenverlustes durch technische Gebrechen.

1.
Der Mitarbeiter ist verpflichtet, an pluss-seitig angebotenen Security Awareness-Schulungen teilzunehmen.

2.
Die private Nutzung der bereitgestellten betrieblichen Geräte bzw. der Zugangsmöglichkeiten (insbesondere Computer und Internetzugang) ist untersagt. Insbesondere ist privates Streaming während der Arbeitszeit zur Vermeidung von Störungen im Betriebsablauf verboten.

3.
Die dienstliche Nutzung privater Geräte ist verboten. Insbesondere ist es verboten, dienstliche Daten, Selektionen, Auswertungen u.a.m. aus zvoove oder einer anderen Firmensoftware mit privaten Geräten zu verarbeiten; dazu gehört auch der Abruf des dienstlichen E-Mail-Accounts beispielsweise über Office 365 mit einem privaten Computer, Smartphone o. ä. Weiterhin ist es verboten, dienstliche Daten, Selektionen, Auswertungen u.a.m. aus zvoove oder einer anderen Firmensoftware auf privaten Speichermedien (Smartphones, USB-Sticks, SD Karten, externe Festplatten, CD's, DVD's etc.) abzuspeichern.

Ausgenommen hiervon ist die Verwendung der MS Authenticator App auf privaten Smartphones von Mitarbeitenden, die über kein dienstliches Smartphone verfügen.

4.
Hinsichtlich der E-Mail Nutzung gilt Folgendes:

- die Nutzung der pluss-seitig zur Verfügung gestellten E-Mail-Adresse ist nur für dienstliche Zwecke erlaubt;
- das Öffnen von E-Mails mit verdächtigen Absendern oder Betreffzeilen sowie das Öffnen von verdächtigen Dateianhängen ist nicht erlaubt;
- sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen auf keinen Fall weitergeben werden;
- wird der Mitarbeiter in einer E-Mail aufgefordert, einen Link anzuklicken, ist dieser mittels „Hyperlink kopieren" in den Browser zu übertragen und vor dem Aufrufen noch einmal zu überprüfen;
- das Beantworten von Spam-Mails (auch das Abbestellen von E-Mails) soll unterbleiben;
- der Mitarbeiter soll auch Kollegen über verdächtige Zusendungen informieren;
- bei Versenden von externen Massenmails ist die BCC Funktion zu verwenden;

pluss behält sich beim Austritt eines Mitarbeiters das Recht vor, dessen dienstliche E-Mail-Adresse vorläufig weiter zu verwenden, um den Unternehmensablauf nicht zu beeinträchtigen.

5.
Es ist auf eine verschlüsselte Kommunikation zu achten. Der Browser signalisiert dies mit einem Schloss. Alle übermittelten Daten und alle Daten, die in ein Formular auf dieser Webseite eingeben werden, sind demnach verschlüsselt.

Alle Zugangsdaten für dienstlich genutzte Web-Portale oder sonstige Dienste, die eine Autorisierung vorsehen, müssen in sicherer Form gespeichert werden. Die Ablage in einer E-Mail oder Datei ist nicht zulässig. Zu empfehlen ist ein digitaler Passwortsafe (ggf. Rücksprache mit der IT- Abt.). Dies gilt besonders dann, wenn mehrere Personen in einem Team dieselben Zugänge verwenden. Die Speicherung oder Verwendung von Zugangsdaten nach Austritt aus dem Unternehmen ist verboten.

6.
Aus Gründen der IT- Sicherheit ist es insbesondere verboten:

- eine pluss-seitig zur Verfügung gestellte PIN für die Informations- und Kommunikationselektronik an Dritte weiterzugeben oder zu verändern;
- aufgrund der Einheitlichkeit der Dateiablage im Netzwerk mit anderen als den zur Verfügung gestellten Speichermedien und Laufwerken zu arbeiten. Dateien dürfen nicht mit einem Kennwort versehen werden;
- Vorlagen, die aus dem ERP-System, dem plussnet (Intranet) oder sonst pluss-seitig zur Verfügung gestellt werden, zu verändern;
- jede Art von nicht durch die IT genehmigter Software herunterzuladen und/oder zu installieren. Als von der IT genehmigt gelten: Vorinstallationen und Softwaredateien gemäß Leitfaden „genehmigte Software“;
- betriebsrelevante E-Mails und Dateien zu löschen;
- Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten aufzurufen.

7.
Es ist untersagt, betriebliche Daten, Informationen oder Unterlagen – insbesondere personenbezogene und sonst vertrauliche Daten – an Dritte weiterzugeben, sie Dritten zur Kenntnis gelangen zu lassen (etwa durch Einsichtnahme am Bildschirm oder auf Ausdrucken), sie auf eigenen Speichermedien abzuspeichern, unbefugt zu kopieren oder zu anderen als betrieblichen Zwecken zu verwenden.

Insbesondere

- ist es verboten, Dritten Passwörter oder sonstige Zugangsmöglichkeiten zur dienstlichen EDV (z. B. Chipkarten) mitzuteilen oder zugänglich zu machen, z. B. durch Notieren von Passwörtern oder Lagerung der Chipkarte am Lesegerät;
- ist es verboten, betriebsfremden Personen Zugriff auf die betriebliche EDV und/oder betriebliche Unterlagen zu gewähren;
- ist es verboten, Sicherheitsmaßnahmen zu deaktivieren oder zu umgehen oder sonstige technische Veränderungen an den durch pluss zur Verfügung gestellten Geräten vorzunehmen.

Stellt der Mitarbeiter fest, dass personenbezogene Daten verlorengegangen sind, ist dies unverzüglich an die Rechtsabteilung zu melden.

8.
Die Entsorgung von Dokumenten hat in der Betriebsstätte über den dort zur Verfügung gestellten Dokumenten-Schredder oder durch das von der Niederlassung beauftragte, auf die Entsorgung spezialisierte Dienstleistungsunternehmen zu erfolgen. Über die fachgerechte Entsorgung ist ein Zertifikat auszustellen. Es ist untersagt, Dokumente durch den Papierkorb zu entsorgen.

Nicht mehr benötigte Datenträger (USB Stick, Festplatte, SD Karte, CD/DVD etc.) sind an die IT-Abteilung zu übergeben.

9.
Die Tätigkeit außerhalb der ersten Tätigkeitsstätte darf ausschließlich über eine angemessen abgesicherte Verbindung, z. B. sogenanntes Virtual Private Network (VPN) über alle Kommunikationswege einschließlich des genutzten heimischen WLAN/WiFi-Netzes sowie der Internetanbindung über Festnetz erfolgen. WiFi-Zugänge müssen mit einem sicheren Passwort abgesichert sein.

10.
Die Tätigkeit am Arbeitsplatz ist so zu gestalten, dass Dritte keine personenbezogenen Daten auf dem Bildschirm einsehen können.

11.
Sobald der Mitarbeiter seinen Arbeitsplatz verlässt (und sei es nur kurz, etwa zur Toilette), muss sichergestellt sein, dass kein Dritter auf betriebliche Daten oder Akten zugreifen kann. Dies bedeutet insbesondere, dass

- der verwendete Computer gesperrt werden muss, sodass bei Rückkehr zumindest die Eingabe des Passwortes erforderlich ist;

- Fenster verschlossen sein müssen, außer bei kurzzeitiger Abwesenheit, während der ein Eindringen realistischerweise ausgeschlossen werden kann (z. B. 10. Stock und keine Möglichkeit, aus der Nachbarwohnung herüberzuklettern);
- bei Nutzung von ausgedruckten Dokumenten (insbesondere Personalunterlagen), diese in einem Schrank einzuschließen sind oder der Büroraum abzuschließen ist.

12.
Telefonate und Videokonferenzen mit vertraulichem Inhalt sind so zu führen, dass nicht befugte Kollegen, Haushaltsmitglieder, Besucher, Nachbarn oder andere unbefugte Personen den Inhalt des Gesprächs nicht wahrnehmen können. Hierbei sind auch geöffnete Fenster zu berücksichtigen. Öffentliche Räume, Balkone, Terrassen oder Gärten eignen sich grundsätzlich nicht für solche Gespräche.

13.
Alle betrieblichen Daten, Informationen und Unterlagen, auf die der Mitarbeiter von seinem Arbeitsplatz aus Zugriff hat, verbleiben ausschließlich im Verfügungsbereich von pluss. pluss ist jederzeit berechtigt, die Herausgabe sämtlicher betrieblicher Daten, Unterlagen und Akten einschließlich sämtlicher Kopien zu verlangen; sind zum Zugriff auf betriebliche Daten Passwörter oder sonstige Schlüssel erforderlich, sind diese mit herauszugeben. Der Mitarbeiter kann hiergegen kein Zurückbehaltungsrecht geltend machen.

14.
Alle Störungen oder Auffälligkeiten bei der EDV-Nutzung (beispielsweise Warnungen oder Fehlermeldungen, die nicht selbst verursacht wurden) sind unverzüglich der IT-Abteilung zu melden. Dies betrifft auch den Verlust eines Arbeitsgeräts.

15.
Sämtliche Kommunikations- und Dokumentationsabläufe werden grundsätzlich gespeichert. Im berechtigten Interesse können diese zu jeder Zeit überprüft und analysiert werden.

16.
Die Richtlinie zur IT-Sicherheit und zum Datenschutz ist in ihrer jeweils gültigen Fassung Bestandteil aller Anstellungsverträge. Die Richtlinie zur IT-Sicherheit und zum Datenschutz gilt auf unbestimmte Dauer. pluss ist berechtigt, diese Richtlinie jederzeit mit Wirkung für die Zukunft ganz oder teilweise zu ändern oder aufzuheben. Die aktuelle Fassung der Richtlinie kann unter „https://www.pluss.de/Vertragsbestandteile/“ oder mittels des rechts abgebildeten QR-Codes eingesehen werden.

17.
Verstöße gegen diese Richtlinie können nicht nur arbeitsrechtliche Folgen (Ermahnung, Abmahnung, fristgerechte oder fristlose Kündigung) haben, sondern auch mit Geldbuße bedroht und/oder strafbar sein (z. B. im Fall des Kopierens von Daten nach Art. 83 DSGVO, § 42 BDSG, § 23 GeschGehG). Darüber hinaus können Verstöße gegen diese Richtlinie Unterlassungs- und Schadensersatzansprüche nach sich ziehen.