# IT-Richtlinien für Mitarbeitende in Verbindung mit der DSGVO

## Einleitung

IT Sicherheit geht uns alle an!

Blossin verarbeitet schützenswerte Daten, vorwiegend elektronisch.

Datensicherheit im Allgemeinen und speziell IT-Sicherheit sind daher unverzichtbar. Dies gilt sowohl für den Versuch, diese Daten auszuspionieren, als auch für die Gefahr des Datenverlustes.

Die nachfolgenden Punkte sind sowohl für Blossin und deren Mitarbeitende von großer Bedeutung.

Dabei sind generell folgende Punkte zu beachten:

## Sicherer Umgang mit personenbezogenen Daten

Personenbezogene Daten sind all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben.

Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit sind besonders schützenswert (siehe Art. 9 DSGVO).

Das Speichern und Verarbeiten von personenbezogenen Daten ist nur unter Zustimmung des Betroffenen zulässig (Art. 6 DSGVO).

Bitte berücksichtigen Sie folgende Punkte:

- Personenbezogene Daten müssen geheim gehalten werden. Nur bei schriftlicher Zustimmung dürfen diese Daten an Dritte weitergegeben werden.
- Bei Weitergabe der Daten muss auf einen sicheren Kommunikationsweg geachtet werden.
- Nach dem Ausscheiden aus dem Betrieb dürfen Sie personenbezogene Daten, die Ihnen beruflich zugänglich gemacht wurden, nicht weitergeben oder für andere Zwecke nutzen.

## Social Media

Soziale Medien können ein Sicherheitsproblem verursachen. Generell sollte man sich vor Augen führen, dass JEDE Information, für irgendjemanden wichtig sein kann. Ein Foto von Ihrem Arbeitsplatz kann z.B. Ordner zeigen, wo Kundennamen ersichtlich sind. Die Information, dass das gesamte Unternehmen auf Skiwochenende fährt, könnte einem Hacker das nötige Zeitfenster aufzeigen, um sich digital Zutritt zu verschaffen. Daher gehen Sie mit Informationen, die Sie preisgeben, besonders sorgsam um. Siehe auch „Umgang mit Social-Media“[1].

Bitte berücksichtigen Sie folgende Punkte:

- Posten Sie keine Fotos von ihrem Arbeitsplatz, wenn sensible Daten oder identifizierbare Personen ohne Fotofreigabe zu sehen sind.

[1] ..\..\..\..\Marketing\Projekte\Social Media\Umgang mit Social Media.docx

- Geben Sie in keinen Foren oder sozialen Medien sensible Informationen über Blossin preis. Bei Unsicherheiten ist die Geschäftsleitung vorab zu kontaktieren.
- Posten Sie keine personenbezogenen Daten, deren Veröffentlichung nicht nachweislich zugestimmt wurde. Bei vorliegenden Einverständniserklärungen von Kooperationspartnern ist die Vereinbarung der gemeinsamen Verantwortlichkeit ausreichend oder muss abgeschlossen werden.

Werden im Rahmen von Veranstaltungen Fotos in sozialen Medien verbreitet, stellen Sie sicher, dass Personen nicht zu erkennen sind oder aber diese der Veröffentlichung aktiv zugestimmt haben.

Folgenden Konstellationen für die Veröffentlichung von Fotos nach § 23 KUG ohne schriftliches Einverständnis der abgebildeten Personen sind erlaubt:

1. Bildnisse aus dem Bereich der **Zeitgeschichte**;
2. Bilder, auf denen die Personen nur als **Beiwerk** neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von **Versammlungen**, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;
4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

Die Informationspflichten des Art. 13 DSGVO sollten gleichwohl beachtet werden, z.B. durch Hinweise an den Eingängen, dass Fotos angefertigt und ggf. veröffentlicht werden.[2]

## Clean Desk Policy

Die **Clean Desk Policy** legt fest, wie Mitarbeitern ihren Arbeitsplatz zurücklassen sollen, wenn sie das Büro verlassen.

Bitte beachten Sie folgende Punkte:

- Sperren Sie Ihren Computer, wenn Sie Ihren Arbeitsplatz verlassen (z. B. unter Windows mit „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.
- Schließen Sie das Büro ab.
- Lassen Sie keine Ausdrucke im Drucker/Kopierer liegen.
- Lassen Sie Passwortnotizen nicht offen an Ihrem Arbeitsplatz liegen.
- Unterlagen und Notizen, auf denen sich sensible Daten befinden, sollen nicht offen auf dem Schreibtisch liegen bleiben.

## Persönliche Passwörter

Passwörter schützen vor unbefugten Zugriff.

Bitte beachten Sie folgende Punkte:

- Verwenden Sie möglichst nie das gleiche Passwort für unterschiedliche Zugänge.
- Verwenden Sie zur Unterstützung ggf. eine Passwortdatenbank.

[2] https://www.datenschutz-guru.de/fotos-von-sportveranstaltungen-in-vereinszeitung/

- Verwenden Sie Kennwörter, die mindestens 10 Zeichen haben. Ein Passwort muss aus Großbuchstaben, Kleinbuchstaben, Ziffer und Sonderzeichen bestehen, um sicher zu sein.
- Niemals Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen, etc. verwenden. Diese werden bei Angriffen zuerst ausprobiert.
- Verwenden Sie keine Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden. Auch Eigennamen, geografische Begriffe etc. dürfen nicht verwendet werden.
- Trivial-Passwörter (hallohallo, abcdefgh, 08/15, 1234 etc.) sind ebenfalls ungeeignet. Sie können von Anderen leicht beim Beobachten der Passworteingabe erkannt werden.
- Geben Sie ihr Passwort niemandem weiter! Auch Kolleg_innen oder IT-Administratoren benötigen ihr Kennwort nicht. Ausnahmen (Notfälle, Urlaub) sind mit der Geschäftsleitung abzusprechen. Nach genehmigter Ausnahme muss das Passwort geändert werden.
- Ändern Sie Ihr Kennwort in regelmäßigen Abständen (mind. alle 180 Tage).
- Überlegen Sie sich einen Satz und verwenden Sie nur die Anfangsbuchstaben für Ihr Passwort. Beispiel:
    - Am Samstag arbeite ich von 9 bis 13 Uhr - ASaiv9-13U
- Sie sind für Ihr Kennwort verantwortlich! Sollten Sie den Verdacht haben, dass ein Dritter Ihr Kennwort kennt, ändern Sie dieses sofort (für den PC mit Strg Alt Entf) oder kontaktieren Sie die IT-Administratoren.

Das gleiche gilt für Web-Portale oder sonstige Dienste, die eine Autorisierung vorsehen.

Zugangsaccounts sind als Betriebseigentum zu sehen und nach Austritt aus dem Betrieb zu übergeben.

## Verschlüsselte Kommunikation

Bitte achten Sie auf eine verschlüsselte Kommunikation. Ihr Browser beispielsweise signalisiert dies mit einem Schloss. Alle übermittelten Daten und alle Daten, die Sie zum Beispiel in ein Formular auf dieser Webseite eingeben, sind demnach verschlüsselt.


Bitte beachten Sie, dass eine normale E-Mail KEINE sichere Kommunikation darstellt. Nur sensiblen Daten, wie zum Beispiel Gesundheitsdaten, Konfession, rassische und ethnische Herkunft, müssen verschlüsselt werden. Dazu ist der Arbeitshinweis „Personenbezogene Daten sicher verschicken“[3].

## Dokumente und Datenträger richtig entsorgen

Weggeworfene Dokumente stellen ein Sicherheitsproblem dar, wenn diese Daten in falsche Hände geraten. Aus diesem Grund müssen Datenträger (USB Stick, Festplatte, SD Karte, CD/DVD…) sicher entsorgt werden. Für die sichere Entsorgung übergeben Sie die Datenträger den IT-Administratoren.

[3] Personenbezogene Listen sicher verschicken.docx

Bitte beachten Sie folgende Punkte:

- Werfen Sie Datenträger oder wichtige Dokumente (z.B. personenbezogene Daten, Verträge, Finanzunterlagen, strategische Unterlagen) auf keinen Fall in den Papierkorb! Diese Vorgehensweise gilt auch für Archivmaterial. Datenträger sind an die IT-Administratoren zu übergeben. Schriftliches Material ist über den Aktenvernichter (Tonne oder Schredder) zu entsorgen.

## Speicherung von Daten

Bitte sorgen Sie dafür, dass Daten nur in den X-Ordnern gespeichert werden. Verwenden Sie Ihren privaten Cloud-Speicher nicht für Betriebsdaten. Eine Speicherung auf lokalen Datenträgern wie die interne Festplatte/Laufwerk C: ist kurzfristig übergangsweise bis zum nächsten Arbeitstag möglich. Eine externe betriebliche Festplatte steht für Grafik-/Marketingmaterialien zur Verfügung. USB Sticks dürfen nicht verwendet werden. Ausnahmen sind durch die Geschäftsleitung zu genehmigen.

## Umgang mit mobilen IT-Geräten

Mobile IT Geräte (Notebooks, Smartphones...) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar.

Bitte beachten Sie folgende Punkte:

- Lassen Sie das Gerät nicht unbeaufsichtigt.
- Überlassen Sie das Gerät nicht anderen Personen.
- Melden Sie einen Diebstahl oder Verlust sofort der IT-Abteilung.
- Achten Sie bei Passworteingabe am Gerät auf ihren Sichtschutz – ähnlich wie bei einem Bankautomaten.
- Installieren Sie nur Anwendungen, die Ihnen als vertrauenswürdig und sicher bekannt sind und von Ihrer IT-Abteilung frei gegeben wurden.
- Dienstgeräte dürfen nur für den betrieblichen Gebrauch genutzt werden. Für Mobiltelefone gilt eine Übergangsregelung bis zum 31.07.2022.

## Internetnutzung

Es gilt ein sensibler Umgang bei der Nutzung des Internetzes.

Bitte beachten Sie folgende Punkte:

- Bei Webseiten ist besondere Sorgfalt geboten.
- Wenn möglich, lehnen Sie Cookies auf fremden Webseiten ab oder verwenden Sie nur die notwendigen.
- Übermitteln Sie keine persönlichen Daten, vor allem nicht, wenn die Verbindung nicht als sicher (Verschlüsselungssymbol) markiert wird.
- Webseiten, die mit dem Download z.B. kostenloser Zusatzsoftware oder unseriösen Gewinnspielen locken, sind grundsätzlich zu misstrauen. Downloads sind generell untersagt. Update-Hinweise sind dem IT-Administratoren zu melden und werden generell von IT-Administratoren vorgenommen. Heruntergeladen werden können PDFs im dienstlichen Sinne (z.B. Anträge, Verwendungsnachweise). Weitere benötigte Downloads sind mit der Geschäftsleitung abzusprechen.

- Das Herunterladen von Dateien kann – abgesehen von der Gefahr des Einschleppens von Schadsoftware – auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde und nur auf dem Endgerät gespeichert ist.
- Der Download von Musik- und Videodateien ist prinzipiell untersagt. Ausnahmen sind Downloads von themenbezogenen Videos im dienstlichen Interesse. Bei Bedarf kann eine Ausnahmegenehmigung durch die die Geschäftsleitung erfolgen.
- Rufen Sie keine Webseiten mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten auf. Das kann gravierende rechtliche Probleme – auch für den Betrieb – nach sich ziehen.
- Fragen Sie lieber einmal zu viel bei Ihren IT-Administratoren nach.

## E-Mail Nutzung

Die E-Mail-Nutzung ist nur für den betrieblichen Gebrauch genehmigt. Die Geschäftsleitung kann auf betriebliche E-Mail-Accounts zugreifen, da es sich um betriebliche Daten handelt (Ausnahme Betriebsrat@blossin.de).

Bitte beachten Sie folgende Punkte:

- Öffnen Sie keine E-Mails, wenn Ihnen Absender oder Betreffzeile verdächtig erscheinen.
- Öffnen Sie keine Dateianhänge ohne sicher zu sein, dass Ihnen der Absender bekannt ist oder real erscheint. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)? Erwarten Sie die beigelegten Dateien und passen sie zum Absender, oder kommen sie völlig unerwartet?
- Öffnen Sie keine E-Mails mit Spaßprogrammen, da diese Schadsoftware enthalten können.
- 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 Sie auf keinen Fall weitergeben.
- Oftmals kann in einer E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien Sie dabei vorsichtig: In betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als in der Mail zu sehen ist. Beim Anklicken wird dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Öffnen Sie Links nur, wenn Ihnen der Absender bekannt ist und real erscheint oder Sie diese E-Mail erwarten.
- Beantworten Sie keine Spam-Mails! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch Ihr Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
- Benachrichtigen Sie Ihre IT-Administratoren über verdächtige Zusendungen, die nicht im Spam-Ordner sind. Besprechen Sie die aktuellen E-Mails, die Sie als Phishing-Versuche oder Virus-Mails erkannt haben, um gemeinsam die typischen Kennzeichen kennenzulernen. Sie können auf diese Weise sehr rasch Ihre Erkennungsfähigkeit trainieren und verbessern.
- Fragen Sie Ihre IT-Administratoren, falls Sie sich unsicher sind.
- Denken Sie bei ihrem Urlaubsantritt oder bei Abwesenheit an den Abwesenheitsassistenten, um die Absender über ihre Abwesenheit zu informieren.

## Social Engineering

Unter Social Engineering versteht man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Vorwiegend wird dieser Angriff per Telefon oder E-Mail durchgeführt.

Social Engineers geben sich gerne als Mitarbeiter_innen aus. Vielleicht behaupten sie auch, eine Behörde oder ein wichtiges Kundenunternehmen zu vertreten oder zu Ihrer IT-Abteilung zu gehören. Ihre Opfer werden durch firmeninternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann als „gestresster Kollege“ an Ihre Hilfsbereitschaft oder drohen als „Kunde“ mit dem Verlust eines Auftrages. Kommt ein Social Engineer bei einer Mitarbeiterin oder einem Mitarbeiter nicht ans Ziel, wird der Angriff bei der nächsten Ansprechperson wiederholt – bis er erfolgreich ist.

Bitte beachten Sie folgende Punkte:

- Seien Sie bei Telefonanrufen oder E-Mails skeptisch, speziell wenn der Wunsch oder der Auftrag der Person außergewöhnlich ist.
- Falls möglich, besprechen Sie die Angelegenheit mit Ihrem Kollegen oder mit Ihrer Kollegin persönlich.
- Bedenken Sie, dass Social Engineering sehr oft angewandt wird, aber meistens lange Zeit unentdeckt bleibt.
- Geben Sie keine vertraulichen Informationen (z.B. personenbezogene Daten, Interna) per Telefon oder E-Mail weiter.

### Private Nutzung der IT

Die Nutzung der IT für private Zwecke ist untersagt. Dies betrifft sowohl die Nutzung der Geräte an sich (PC, Laptop, Smartphone – Ausnahmeregelung bis 31.07.2022) als auch Ihr Firmenpostfach (E-Mail) und den Firmen internen Internetanschluss. Ausnahme ist das Gäste- WLAN.

Die Geschäftsleitung kann auf alle genutzten Dateiverzeichnisse – Ausnahme Betriebsrat – zugreifen, da es sich um betriebliche Daten und Betriebseigentum handelt.

### Warnungen und Fehlermeldungen

Warnungen oder Fehlermeldungen, die Sie nicht lösen können, müssen unverzüglich den IT Administratoren gemeldet werden. Siehe auch „Verfahrensweise bei technischen Störungen“[4].

### Installation von Applikationen

Die Installation von Applikationen ist untersagt. Dies gilt sowohl für IT-Geräte (PC’s, Notebooks, Server), aber auch für Firmeneigene Mobilgeräte wie Smartphone und Tablets. Falls Sie eine Applikation benötigen, senden Sie eine Mail-Anfrage an die Geschäftsleitung.

### Austritt aus dem Unternehmen

Bei Austritt aus dem Betrieb behält sich Blossin das Recht vor, auf E-Mail-Adressen des/der ausscheidenden Mitarbeiter_in weiter zuzugreifen, um den Betriebsablauf nicht zu beeinträchtigen. Darüber

[4] ..\Notfallpläne\Verfahrensweise bei technischen Störungen des Hausnetzes und des Serversystems.doc

hinaus verpflichtet sich der/die Mitarbeiter_in, sämtliche Dokumente, IT-Equipment und Unterlagen bei Austritt unaufgefordert dem Betrieb zu übergeben. In einem Beschäftigungsverhältnis ist in der Regel der Arbeitgeber der Inhaber des generierten Geistigen Eigentums. Speziell im Hinblick auf Dokumente, Berechnungen oder dergleichen ist dies ein wesentlicher Punkt.

Eine willkürliche Löschung von Dokumenten, E-Mails, oder sonstigen firmenrelevanten Daten ist untersagt.

## Arbeitsrechtliche Konsequenzen

Ein Verstoß gegen die Richtlinien kann eine arbeitsrechtliche Pflichtverletzung darstellen, hierbei muss mit einer arbeitsrechtlichen Konsequenz gerechnet werden.

Mit Ihrer Unterschrift bestätigen Sie, dass Sie diese Richtlinien beachten und umsetzen werden.

……..
Ort, Datum

…….. ……..
Vorname Name Unterschrift Mitarbeiter_in