

## Übersicht Informationssicherheitsrichtlinie Diction AG

Mai 2018

### Auszug aus der Informationssicherheitsrichtlinie Diction AG

Lieber Kunde

Lieber Interessent bzw. lieber Stellenbewerber

Liebe übrige Vertragspartner

Gerne informieren wir Sie als Verantwortliche mit dem vorliegenden Auszug aus unserer umfassenden und für die Diction AG geltenden Informationssicherheitsrichtlinie im Sinne einer kurzen Übersicht zu den Grundsätzen der Informationssicherheit und den etablierten und kontrollierten Prozessen.

Die Informationssicherheitsrichtlinie gilt auch für sämtliche Gesellschaften, die unter der Diction AG, insbesondere als Tochtergesellschaften in der Schweiz, in der Europäischen Union oder in einem übrigen Drittstaat, tätig sind sowie auch für andere vertraglich gebundene oder freie Mitarbeiter bzw. Dienstleister.

#### 1. Grundsätze zur Informationssicherheit bei der Diction AG

Die Grundsätze zur Informationssicherheit (Sicherheitspolitik) beschreiben die Strategie, die für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses bei der Diction AG erforderlich ist, die Ziele, die Verantwortlichkeiten und die Rollen. Konkrete Regelungen dazu werden in einer gesonderten Ordnung fixiert.

Potenzielle Sicherheitsvorfälle bei der Diction AG sind mit angemessenen Gegenmassnahmen auf allen Ebenen zu verhindern. Dies umfasst neben der Umsetzung von Schutzmassnahmen zur Sicherstellung des ordnungsgemässen Betriebs der Informationstechnik auch den Schutz von nicht elektronisch verarbeiteten Informationen durch entsprechende Sicherheitsprozesse. Die erfolgreiche Umsetzung der Sicherheitsprozesse ist nur mit der kooperativen Unterstützung aller Mitarbeitenden, Freelancer sowie anderer Dienstleister möglich.

#### 2. Ziele

Die grundlegenden Schutzziele der Informationssicherheit sind im Rahmen der beruflichen Notwendigkeiten die angemessene Verfügbarkeit, Vertraulichkeit und Integrität von Informationen.

Sie sind wie folgt definiert:

- Verfügbarkeit – Gewährleistung, dass Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit verfügbar sind.
- Vertraulichkeit – Gewährleistung, dass schützenswerte Informationen ausschliesslich berechtigten Nutzern zugänglich sind.
- Integrität – Gewährleistung, dass schützenswerte Informationen unversehrt und vollständig bleiben.

### 3. Leitgedanken

- Gesetzliche und vertragliche Anforderungen sowie Selbstverpflichtungen werden erfüllt.
- Die vorrangigen Kriterien für geeignete Sicherheitsmassnahmen sind deren Wirksamkeit im Hinblick auf das zu tragende Restrisiko und die wirtschaftliche Angemessenheit.
- Bei der Verarbeitung von Informationen werden die Grundanforderungen der Informationssicherheit eingehalten. Entsprechend ihres Schutzbedarfs werden Informationen angemessen und sicher verarbeitet und adäquat vor unberechtigten Zugriffen geschützt.
- IT-Systeme werden in einer angemessen sicheren Weise und Umgebung betrieben, sodass die Verfügbarkeitsanforderungen der IT-gestützten Prozesse erfüllt werden können.
- Alle Nutzer haben ein Grundverständnis für Belange der Informationssicherheit und sind zu einer zweckmässigen und verantwortungsvollen Nutzung der Informationstechnik angehalten.
- Die Wirksamkeit und Angemessenheit der Sicherheitsmassnahmen wird regelmässig überprüft und dokumentiert. Abweichungen werden mit dem Ziel analysiert, das Sicherheitsniveau kontinuierlich zu verbessern. Dies umfasst die Grundsätze zur Informationssicherheit und nachrangige Regelungen.

### 4. Verantwortlichkeiten

Die aus organisatorischer und strategischer Sicht tragenden Rollen für das Informationssicherheitsmanagement bei der Diction AG sind:

**Geschäftsführung** – Die Geschäftsführung trägt die Gesamtverantwortung für die Informationssicherheit bei der Diction AG.

**Informationssicherheitsbeauftragter (ISB)** – Der ISB ist federführend bei allen strategischen und taktischen Aspekten der Informationssicherheit bei der Diction AG. Er koordiniert diese Aufgabe sachbezogen und themenübergreifend in Kooperation mit den Ansprechpartnern der Abteilungen. Der ISB berichtet direkt an die Geschäftsführung.

Der ISB konsultiert den Datenschutzberater/-beauftragten (DPO) der Diction AG (siehe unter [Datenschutzklärung Diction](#) und [Data-Protection-Info-Sheet](#)) ohne Verzug bei festgestellten Mängeln im Bereich Datensicherheit und berichtet dem DPO regelmässig über die von ihm durchgeführten Prüfungen und Ausbildungen der Mitarbeiter bzw. übrigen Dienstleister.

Buchs, 11. Mai 2018

Patrick Fassbender, CEO Diction AG