

## **Aperçu de la directive sur la sécurité des informations de Diction SA**

Mai 2018

### **Extrait de la directive sur la sécurité des informations de Diction SA**

Cher client,

Chère personne intéressée, cher candidat,

Chers partenaires contractuels,

En tant que responsables de la sécurité des informations, c'est avec plaisir que nous vous informons, par la présente, concernant les principes applicables dans notre entreprise en matière de sécurité des informations ainsi que les processus mis en place et contrôlés dans ce domaine. Vous trouverez ces informations ci-dessous sous forme de bref extrait de notre directive complète en matière de sécurité des informations en vigueur au sein de Diction SA.

Cette directive s'applique également à l'ensemble des sociétés exerçant leur activité sous l'égide de Diction SA, en particulier à ses filiales situées en Suisse, dans l'Union européenne ou dans d'autres Etats tiers ainsi qu'aux autres collaborateurs ou prestataires, contractuels ou indépendants, de Diction SA.

#### **1. Principes applicables à la sécurité des informations chez Diction SA**

Les principes applicables à la sécurité des informations (politique de sécurité) décrivent la stratégie nécessaire afin d'initier et de mettre en place un processus global en matière de sécurité des informations auprès de Diction SA, ainsi que les objectifs, responsabilités et fonctions y afférents. Les règles concrètes sont fixées dans un règlement séparé.

Il s'agit de prévenir les incidents de sécurité potentiels pouvant survenir à tous les niveaux de l'entreprise au moyen de contremesures appropriées. Celles-ci comprennent, outre la mise en œuvre de mesures de protection visant à assurer le bon fonctionnement des technologies informatiques, également la protection des informations qui ne sont pas traitées sous forme électronique grâce à des procédures de sécurité appropriées. Le succès de la mise en œuvre des procédures de sécurité ne peut être assuré qu'avec la coopération de l'ensemble des collaborateurs, des free-lances et des autres prestataires de l'entreprise.

#### **2. Objectifs**

Dans le cadre des différents impératifs professionnels, les objectifs fondamentaux de protection en matière de sécurité des informations visent principalement à garantir la disponibilité suffisante, la confidentialité et l'intégrité des informations.

# diction

Plus précisément, ces principes peuvent être définis de la manière suivante:

- **Disponibilité:** garantie que les informations, les applications et les systèmes informatiques soient disponibles dans l'étendue prévue et en temps utile pour les ayant droits.
- **Confidentialité:** garantie que les informations sensibles soient accessibles exclusivement aux utilisateurs autorisés.
- **Intégrité:** garantie que les informations sensibles demeurent intactes et complètes.

### **3. Idées clé**

- Les exigences légales et contractuelles sont respectées, de même que les engagements volontaires de l'entreprise.
- Les principaux critères permettant d'apprécier le caractère adéquat des mesures de sécurité sont leur efficacité sous l'angle du risque résiduel à assumer ainsi que leur bien-fondé économique.
- Lors du traitement des informations, nous respectons les exigences fondamentales de la sécurité des informations. En fonction de leur besoin de protection, les informations sont traitées de manière sûre et appropriée et protégées de manière adéquate contre les accès non autorisés.
- Sécurité et adéquation caractérisent non seulement la manière, mais également l'environnement d'utilisation des systèmes informatiques, afin que les exigences relatives à la disponibilité des processus informatiques puissent être remplies.
- L'ensemble des utilisateurs disposent de connaissances de base sur les questions de sécurité des informations et s'engagent à utiliser les technologies informatiques de manière pertinente et responsable.
- L'efficacité et la pertinence des mesures de sécurité sont régulièrement contrôlées et documentées. Les différences sont analysées dans le but d'améliorer en permanence le niveau de sécurité. Ceci comprend les principes applicables à la sécurité des informations et les réglementations secondaires.

### **4. Responsabilités**

Chez Diction SA, les rôles principaux en matière de gestion de la sécurité des informations sont exercés, d'un point de vue organisationnel et stratégique, par les entités suivantes:

**La direction:** la direction assume la responsabilité globale de la sécurité des informations au sein de Diction SA.

**Le délégué à la sécurité des informations (DSI):** le DSI est responsable de l'ensemble des aspects stratégiques et tactiques de la sécurité des informations chez Diction SA. Il coordonne cette mission de manière professionnelle et transversale, en coopération avec les différents interlocuteurs des départements. Le DSI rend compte directement à la direction. Lorsqu'il constate des failles dans le domaine de la sécurité des données, le DSI consulte sans délai le conseiller/délégué à la

# diction

protection des données (DPO) de Diction SA (cf. Politique de protection des données de Diction et Fiche d'information sur la protection des données) et établit des rapports réguliers à l'intention du DPO concernant les contrôles effectués ainsi que les formations des collaborateurs et des autres prestataires.

Buchs, le 11 mai 2018

Patrick Fassbender, CEO de Diction SA