UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Mandats attribués à des entreprises externes (infrastructures cloud)

Directive DIT-17b Champ d'application : Université

1 Buts

Le but de cette directive est de rendre les entreprises externes attentives à la législation à laquelle l'Université de Fribourg est soumise et aux règles qui doivent être respectées en matière d'infrastructures informatiques dans le cloud. Le but principal est de sensibiliser aux éventuels problèmes et non de gêner le travail des deux parties.

Cette directive constitue une convention entre l'Université de Fribourg et une entreprise externe dans le cadre de travaux impliquant l'infrastructure informatique dans le cloud. Celle-ci doit figurer en annexe à toutes commandes de travaux à des firmes externes.

2 Abréviation

DIT Direction des services IT de l'Université de Fribourg

3 Bases légales

Vu:

- l'article 3 de la Loi du 19 novembre 1997 (état au 10 septembre 2015) sur l'Université,
- l'article 18 al. 2 de la loi cantonale du 25 novembre 1994 sur la protection des données (LPrD),
- le règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD),

l'université de Fribourg (ci-après, « l'Université »), par l'intermédiaire de l'unité organisationnelle (UO) concernée, doit établir une convention (présente directive) avec toute entreprise extérieure à l'Université (ci-après, « l'entreprise ») effectuant dans le cloud des travaux permettant un accès direct ou indirect à des données de l'Université (fichiers, bases de données, etc.). Les mandats concernant des travaux sur l'infrastructure informatique physique de l'Université (non-cloud) sont réglés par la directive DIT-17.

Version	Date	Remplace	Auteur(s)	Commentaires
1.0	24.6.2003	-	B. Vuillemin/ J.-F. Descloux	
2.0	26.2.2014	1.0	B. Vuillemin/ A. Gachet	Actualisation et validation par comité de direction IT ; intégration commentaires GSI ; validation GSI
2.1	5.3.2015	2.0	B. Vuillemin/ A. Gachet	Ajout de la version allemande de la directive
2.2	11.11.2016	2.1	B. Vuillemin/ A. Gachet	Ajout de la signature DIT à l'annexe 1.
2.3	23.9.2019	2.2	A. Gachet	Etablissement de la version DIT-17b, spécifique aux travaux dans le cloud

4 Règles de conduite

Selon l'activité de l'entreprise, certaines règles de la présente directive ne sont pas applicables. Dans ce cas, elles seront biffées d'un commun accord. Néanmoins, les éléments figurant aux points 4.1, 4.2, 4.3 et 4.7 s'appliquent dans tous les cas et ne sauraient faire l'objet d'amendements.

4.1 Généralités

Les collaborateurs de l'entreprise s'engagent à respecter les règles d'utilisation de l'informatique applicables à tous les utilisateurs de l'Université.

Les collaborateurs de l'entreprise seront annoncés nominativement à la DIT[1]. L'Université se réserve le droit de supprimer les droits d'accès de tout collaborateur de l'entreprise, à tout moment.

L'Université doit permettre aux collaborateurs de l'entreprise de travailler dans des conditions adéquates pour réaliser leurs tâches, durant l'intégralité de la période d'autorisation.

Si le collaborateur de l'entreprise fait une fausse manipulation quelle qu'elle soit (par exemple, destruction d'un fichier), il doit la signaler à un collaborateur de la DIT sans délai.

Si le collaborateur de l'entreprise remarque quelque chose qu'il juge anormal, il doit prévenir un collaborateur de la DIT sans délai.

4.2 Sécurité informatique

Le travail de l'entreprise doit respecter en tout temps la sécurité informatique mise en place par l'Université.

Il est du ressort de l'entreprise de s'en assurer, notamment en se renseignant auprès de la DIT.

4.3 Protection des données

Dans le cadre de son travail, le collaborateur de l'entreprise pourra être amené à accéder à des données de types *personnelles* ou *sensibles* de *degré de confidentialité* 1 (accessible au public), 2 (à usage interne) ou 3 (confidentiel ou secret) au sens de la réglementation fribourgeoise sur la protection des données.

Au-delà des dispositions cantonales en matière de protection des données, le Rectorat a émis ses propres règles de fonctionnement en limitant l'extraction de listes de personnes à un résultat de 10 noms au maximum.

De plus, le simple fait de rechercher un nom d'étudiant est soumis à une autorisation écrite. En ce sens, le fichier des étudiants n'est pas accessible, sauf autorisation écrite du Rectorat sur la base d'une demande motivée.

Il est de la responsabilité de l'entreprise de sensibiliser ses collaborateurs. La DIT peut fournir de la documentation à ce sujet.

[1] Dans les cas où l'entreprise peut justifier que la livraison à la DIT d'une liste nominative *ex ante* relève d'une procédure inutilement lourde et complexe, elle doit au minimum s'engager à pouvoir livrer, si la DIT en fait la requête, une liste *ex post*. *In fine*, la DIT est seule habilitée à décider si une livraison *ex ante* est requise ou non.

4.4 Accès logique aux infrastructures dans le cloud

Les collaborateurs de l'entreprise, qu'ils soient dans les locaux de l'Université ou à distance, ne pourront se connecter sur les infrastructures cloud que sous leurs propres noms d'utilisateur.

Toute communication à un tiers d'un nom d'utilisateur ou d'un mot de passe est interdite et engage la responsabilité du possesseur du compte. Pour les cas exceptionnels, une autorisation de la DIT est indispensable.

En outre, en cas de changement de prestataire cloud, l'entreprise s'engage à obtenir l'accord préalable de l'Université.

4.5 Transferts de données

L'entreprise n'est pas autorisée à exporter des données de l'Université vers sa propre infrastructure.

Demeure réservée, sur la base d'une convention additionnelle et en fonction de certains besoins spécifiques, la possibilité d'obtenir une autorisation du responsable de la sécurité informatique[2] pour une telle exportation, pour une durée limitée et prédéfinie. Dans ce cas, les dispositions de cryptage imposées seront indiquées. Le transfert sans cryptage est interdit. A la fin de la période autorisée, l'entreprise fournira la déclaration de destruction des données selon les modalités de l'annexe 2. Cela s'applique aux transferts entre l'Université et l'entreprise, mais aussi entre l'entreprise et ses éventuels sous-traitants (voir aussi chapitre 4.6).

De plus, il est de la responsabilité de l'entreprise de s'assurer que tout transfert de données ne sera pas utilisé par un de ses collaborateurs pour exporter des données en contradiction avec la protection des données telle qu'édictée par l'Université.

4.6 Sous-traitance

Si l'entreprise sous-traite ou collabore avec une organisation tierce (entreprise, organisme public, etc.) qui sera amenée à traiter des données de l'Université, l'entreprise organisant la sous-traitance transmettra la présente directive aux organisations liées, collectera leurs déclarations et les adjoindra à la sienne.

4.7 Non-respect des règles, interruption du contrat

Le non-respect d'une ou plusieurs de ces règles sera étudié avec attention par l'Université et toutes les suites appropriées seront envisagées, y compris des prétentions en dommages et intérêts. Le contrat pourra être interrompu par l'Université, notamment en cas de faute grave. Dans tous les cas, l'entreprise devra fournir toute la documentation sur le travail déjà effectué. Cette documentation devra être à jour et de qualité jugée acceptable par la DIT.

5 Application

Cette directive a été approuvée par le Groupe de Sécurité Informatique en date du 23 septembre 2019 et entre en vigueur immédiatement.

[2] En cas d'absence de ce dernier, les règles de suppléance en vigueur s'appliquent.

Annexe 1. Formulaire d'acceptation de la directive DIT-17b de l'université de Fribourg

Principe

L'entreprise soussignée[3] déclare avoir lu la directive DIT-17b de l'université de Fribourg et s'engage à en respecter le contenu. Elle devra, sur demande de l'université de Fribourg, fournir les informations suivantes :

- date, heure, durée des accès logiques (depuis la date de signature du contrat ou, pour les contrats de longue durée, au maximum durant les 6 mois précédents la demande) ;
- motifs des accès ;
- noms des collaborateurs et collaboratrices concerné-e-s ;
- infrastructures cloud accédées ;
- données personnelles accédées (fichiers, bases de données).

Validité

Ce document, signé par le représentant légal de l'entreprise externe, est à retourner au responsable du mandat au sein de l'université de Fribourg, qui le contresignera puis en transmettra l'original au secrétariat de la DIT, à l'adresse suivante : Université de Fribourg, Direction des services IT, Bd de Pérolles 90, 1700 Fribourg.

Pour l'université de Fribourg	Pour l'entreprise externe
	Nom de l'entreprise :_____
Responsable du mandat	Représentant légal
Nom :_____	Nom :_____
Fonction :_____	Fonction :_____
Date :_____	Date :_____
Signature :_____	Signature :_____

Le formulaire d'acceptation de la directive DIT-17b ne sera considéré comme valide que s'il comporte la signature du directeur des services IT ou la personne désignée par lui :

Direction des services IT	
Nom :_____	Date :_____
Fonction :_____	Signature :_____

Muni des trois signatures ci-dessus, ce document est valable pour la durée du mandat, à partir de la date de signature par le responsable des services IT.

La DIT se charge d'établir trois exemplaires de la présente convention, un pour la firme mandatée, un pour le responsable du mandat, et un pour la DIT (Direction des services IT de l'Université de Fribourg).

[3] Dans les cas exceptionnels où une autorisation doit être délivrée rapidement et où le présent formulaire ne peut pas être signé dans l'immédiat par un représentant légal de l'entreprise, le formulaire peut être rempli par le signataire à titre personnel. La durée de validité d'une autorisation personnelle est d'un mois. L'établissement d'une autorisation temporaire à titre personnel ne décharge pas l'entreprise de remplir le formulaire au nom de la société.

Annexe 2. Annonce de destruction des données

L'entreprise enverra une lettre (voir modèle ci-dessous) au responsable du mandat au sein de l'université de Fribourg, qui en fera une copie pour ses dossiers (et la fournira au maître des données sur demande) et transmettra l'original au secrétariat de la DIT.

Modèle de base de l'annonce de destruction des données. La lettre doit être signée par un représentant légal.

Concerne : Annonce de destruction de données appartenant à l'université de Fribourg

Madame, Monsieur,

Dans le cadre du mandat …… nous vous informons par la présente que nous avons détruit les données appartenant à l'université de Fribourg, utilisées du …… au ……..

Ces données ont été effacées de tous nos serveurs, ainsi que de toutes nos installations de tests.

Les sauvegardes de ces données ont également été détruites.

Les supports de transfert, tels que bandes, CD, DVD, ont été détruits.

[selon cas] Nous n'avons pas transmis ces données à des entreprises tierces (collaboration ou sous-traitance).

[selon cas] L'entreprise ……., à qui nous avons sous-traité du travail, a elle aussi détruit toutes les données de l'université de Fribourg, comme l'atteste sa déclaration en annexe [l'entreprise sous-traitante utilisera le même modèle de lettre].

<Signature par un représentant légal de l'entreprise>