Analyse d'impact cadre

Version du 04/09/2024

Pour le Groupe INSA

Table des matières

1. Contexte

La société Blockchain Certified Data (“BCD”) propose un service permettant l'édition d’un format sécurisé d’attestation en ligne, service proposé aux institutions d’enseignement supérieur, de formation, aux associations, administrations et entreprises (ci-après « Solution BCdiploma »).

A ce titre, et au regard de la réglementation relative à la protection des données à caractère personnel (notamment le RGPD), la société BCD intervient en tant que sous-traitant du ou des traitements mis en œuvre par lesdites entités.

Ce statut emporte différentes obligations, et en particulier l'obligation d'assistance à la réalisation des analyses d'impact relative à la protection des données à caractère personnel (ci-après « AIPD ») de son ou ses responsables du traitement (articles 28, 3, f) et 35 du RGPD).

Pour répondre à cette obligation, la société BCD a réalisé une « AIPD cadre » permettant d'effectuer la synthèse, notamment technique, de sa solution BCdiploma, qu'elle pourra transmettre aux responsables du traitement lorsque ceux-ci font une demande d’assistance à la réalisation ou la modification d’une AIPD, afin de faciliter leur travail en disposant de la synthèse des informations de la solution BCdiploma pertinentes à la réalisation d’une AIPD.

En particulier, la société BCD a opté pour un format « AIPD Cnil » (i.e., pouvant être mis en œuvre via l’outil PIA Cnil), qui est un modèle de plus en plus répandu, afin de faciliter l’incorporation de ces informations dans les AIPD des responsables du traitement.

2. Vue d'ensemble

2.1. Quel est le traitement qui fait l'objet de l'étude ?

Le traitement objet de la présente analyse est mis en œuvre par le responsable du traitement. Il relève donc de sa compétence de décrire ledit traitement au sein duquel la solution BCdiploma est mise en œuvre.

Cependant, ce traitement utilise, pour tout ou partie, la solution BCdiploma de la société BCD.

Pour rappel, la solution BCdiploma permet l'émission d'un format sécurisé d'attestation en ligne, et est proposé aux institutions d'enseignement supérieur, de formation, aux associations, administrations et entreprises. Plus précisément, [dénomination du responsable du traitement] entre les données des [typologie des personnes concernées ex. étudiants, diplômés, collaborateurs, salariés etc.] afin de pouvoir générer, administrer et transmettre aux personnes concernées ("titulaires") des attestations sécurisées, par exemple : des diplômes, attestations, micro-certifications ou tout autre document. En parallèle, ces dernières ont accès à une URL personnelle qu'ils peuvent diffuser selon leur bon vouloir (par exemple, en l'ajoutant sur leurs réseaux sociaux – notamment sur LinkedIn – ou en l'envoyant directement à un tiers, par exemple un recruteur).

BCdiploma est une application disponible en mode SaaS et accessible via un simple navigateur web, sans installation ni plugins supplémentaires. Tous les services applicatifs fournis par la société BCD sont hébergés dans un centre de données Azure (Microsoft).

Plus précisément, BCdiploma utilise un procédé breveté (US20200099511A1) utilisant des traitements cryptographiques et des environnements décentralisés de type Ethereum Virtual Machine compatibles (EVM).

La société BCD propose, en option de sa solution BCdiploma, des services optionnels complémentaires à savoir :

- un service d'emailing, via la société Brevo ;
- un service d'assistance intégré (outil de gestion des tickets d'assistance), via la société Hubspot.

2.2. Quelles sont les responsabilités liées au traitement ?

Le responsable du traitement est [dénomination du responsable du traitement], sis [domiciliation du responsable du traitement].

Les coordonnées du DPO du [dénomination du responsable du traitement] sont : [coordonnées du DPO du responsable du traitement].

Dans le cadre de la mise en œuvre de ce traitement, les sous-traitants sont :

NIVEAU DU SOUS-TRAITANT	DÉNOMINATION	DESCRIPTION
1	BCD	Prestataire d'un service en mode SaaS permettant l'édition d'un format d'attestation en ligne et sécurisé proposé aux institutions d'enseignement supérieur, de formation, aux administrations et entreprises
2	Microsoft	Hébergement cloud de la solution SaaS
2	Brevo	Service d'emailing
2	Hubspot	Service d'assistance intégré (outil de gestion des tickets d'assistance)

2.3. Quels sont les référentiels applicables ?

Les environnements techniques utilisés, de type EVM compatibles, ne sont pas assimilables à des sous-traitants (voir le paragraphe relatif à la sous-traitance infra).

Il relève de la compétence du responsable du traitement de définir le ou les référentiels applicables au traitement qu'il met en œuvre et au sein duquel la solution BCdiploma est mise en œuvre.

Évaluation de la vue d'ensemble : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]

---

3. Données, processus et supports

3.1. Quelles sont les données traitées ?

A titre liminaire, il est précisé au responsable du traitement qu'il est libre et seul décisionnaire du choix des données qu'il va faire figurer sur les attestations générées via la solution BCdiploma. Les données renseignées ci-dessous sont des exemples classiques de données traitées par BCD au sein de sa solution BCdiploma dans le cadre de documents académiques, tel une attestation de réussite au diplôme par exemple. Le responsable de traitement devra compléter cette liste selon les spécificités de son traitement, et ce paragraphe serait à amender en accordance. Seule l'utilisation des fonctionnalités de Micro-Certification et Accrochage RNCP nécessitent des données d'identification préétablies par BCdiploma, à savoir :

- Nom
- Prénom(s)
- Adresse de courriel

Les personnes concernées par le traitement, au sein de la solution BCdiploma, sont les personnes pour lesquelles le responsable de traitement souhaite générer une attestation (par exemple : attestation, diplôme et/ou micro-certification).

Les données traitées par [dénomination du responsable du traitement] sont :

- [Liste à établir par le responsable de traitement en fonction des variables paramétrées dans BCdiploma]
- ...

Destinataires externes :

- BCD ;
- toutes personnes à qui il a été communiqué le lien URL permettant d'accéder au diplôme/attestation/certificat ;
- Microsoft ;
- Brevo ;
- Hubspot ;
- [à compléter le cas échéant par le responsable du traitement]

3.2. Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

Il relève de la compétence du responsable du traitement de définir le cycle de vie des données mis en œuvre dans leur traitement.

En revanche, BCD peut décrire le cycle des données au sein de sa solution BCdiploma.

Ouverture du compte de l'institution :

L'ouverture du compte consiste en :

- l'ajout de l'institution au registre des émetteurs ;
- la génération d'une paire de clés cryptographiques secp256k unique associée au compte de l'émetteur et ne pouvant être utilisée que par l'institution elle-même à travers des interfaces de gestion et des APIs mises à disposition par la solution BCdiploma.

Plus précisément, à la demande d'une institution, BCD enregistre les preuves de l'existence légale de l'institution dans un annuaire public infalsifiable (registre des émetteurs) contenant : l'identité de l'institution, sa clé publique, ainsi qu'une empreinte des preuves liées aux vérifications effectuées. Le registre des émetteurs garantit la fiabilité de tous les participants et l'existence réelle des institutions, en collectant et en enregistrant l'empreinte d'éléments tels que l'adresse physique, le numéro de registre du commerce et des sociétés (RCS), le numéro DUNS, le numéro de TVA intracommunautaire, le KBis, les statuts etc.

Versement des données d'entrée :

Une fois son compte ouvert, l'institution a la possibilité de générer des attestations.

Pour cela, l'institution émettrice valide les données des attestations à émettre, par exemple dans son outil de gestion (SIS/CRM/LMS/ERP). Les données sont envoyées automatiquement à BCdiploma (via API) et/ou manuellement (via l'importation d'un fichier Excel).

Cette opération a pour but de certifier les données et de les rendre accessibles lors de la consultation d'une attestation, en :

- chiffrant les données en utilisant une combinaison de chiffrement SSS (Shamir's Secret Sharing) et AES256GCM ;
- signant une transaction contenant ce chiffré ;
- exécutant cette transaction dans un environnement EVM compatible.

La solution BCdiploma génère alors l'attestation, c'est-à-dire :

- une URL sécurisée permettant le déchiffrement de l'attestation et pouvant dès lors être transmise au titulaire selon le mode opératoire choisi par l'institution (exemple : email) ;
- une clé cryptographique unique (clé de persistance) stockée dans un environnement sécurisé (Azure Key Vault) permettant de rendre l'attestation définitivement inaccessible en cas de suppression.

Certificat et lien URL :

Les certificats numériques sont publiés sous la forme d'une page web dont le contenu et les preuves d'enregistrement sont lus en temps réel à partir d'un environnement décentralisé EVM compatible.

Chaque titulaire de certificat recevra, selon le mode opératoire choisi par l'institution, l'URL permettant d'accéder à son certificat numérique. Cette URL est l'unique moyen de déchiffrer les données de l'attestation : il est impossible d'accéder aux données déchiffrées sans elle.

Le titulaire, ainsi que l'institution émettrice, sont les seuls gardiens de l'URL, et la responsabilité de la partager leur incombe. Le titulaire peut décider de la partager sur les médias sociaux ou de l'envoyer à un tiers.

Si l'institution souhaite supprimer une attestation, ou si le titulaire souhaite exercer son droit à l'oubli, l'institution a la possibilité, via l'interface de gestion de solution de la solution BCdiploma ou par API, de supprimer l'attestation.

Plus précisément, lorsqu'une attestation est supprimée, sa clé de persistance est définitivement supprimée et l'URL dirige vers une page « attestation révoquée ». Il n'y a plus aucun moyen d'accéder aux données de l'attestation.

3.3. Quels sont les supports des données ?

Il relève de la compétence du responsable du traitement de définir l'ensemble des supports (numériques ou papiers) intervenant dans la mise en œuvre du traitement. La solution BCdiploma ne pouvant être qu'un support parmi d'autres.

Concernant la solution BCdiploma, les données à caractère personnel sont traitées numériquement par cette dernière et sont hébergées dans un centre de données Azure (Microsoft).

Évaluation des données, processus et supports : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]

---

4. Principes fondamentaux

4.1. Proportionnalité et nécessité

4.1.1. Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

Les finalités du traitement dépendent de facto du traitement mis en œuvre. Dès lors, c'est au responsable du traitement de définir les finalités, voire les sous-finalités, de celui-ci.

Une fois définies, le responsable du traitement devra alors vérifier que ces finalités sont bien déterminées, explicites et légitimes.

Voici, à titre indicatif, un exemple de rédaction :

L'institution met en œuvre un traitement de données personnelles ayant pour finalités :

> *- l'établissement et la délivrance de certificats numériques valant attestations de réussite aux diplômes et certificats émis par l'institution (ci-après, les « Certificats numériques ») ;*
>
> *- leur mise à disposition au moyen d'un lien internet personnel ;*
>
> *- la gestion, l'authentification, l'enregistrement et la conservation d'une trace de ces Certificats numériques émis dans un environnement décentralisé.*

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

4.1.2. Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Les bases légales du traitement dépendent des finalités retenues pour le traitement. Dès lors, c'est au responsable du traitement de définir celles-ci en fonction des finalités retenues.

Voici, à titre indicatif, des fondements pouvant être retenus selon les documents concernés :

- l'obligation légale lorsqu'un texte autorise et encadre expressément le traitement ;
- les missions d'intérêt public assurées par [responsable du traitement] ;
- l'intérêt légitime du [responsable du traitement] (process soit traitement administratif), sous réserve d'avoir opéré une mise en balance de cet intérêt avec les droits et libertés des personnes concernées

---

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

4.1.3. Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

A titre liminaire, il est précisé au responsable du traitement que l'analyse ci-dessous ne porte que sur les données traitées par BCD au sein de sa solution BCdiploma (listées au paragraphe « Quelles sont les données traitées ? »). Si le traitement mis en œuvre par le responsable du traitement devait comporter des données supplémentaires, alors ce paragraphe devra être à amender en accordance par le responsable du traitement.

Comme précisé dans le paragraphe « Quelles sont les données traitées ? », c'est le responsable de traitement qui décide des données qu'il va transmettre à BCdiploma pour l'émission des attestations. Il s'agit donc, pour lui, de vérifier la bonne cohérence entre les données transmises et la finalité du traitement qu'il a retenu.

A titre d'exemple, voici une analyse concernant des données classiquement utilisée pour une attestation numérique de réussite au diplôme :

Données d'identification : Le traitement des données relatives au nom, prénom(s), date et lieu de naissance de la personne concernée [à compléter le cas échéant] par l'attestation numérique de réussite au diplôme/attestation/certificat est nécessaire à l'édition de ceux-ci pour répondre aux exigences de mentions obligatoires que ces documents nécessitent et/ou pour permettre à son titulaire de revendiquer la propriété de cette attestation auprès d'un tiers.

Données vie professionnelle de la personne concernée par le diplôme/attestation/certification : De même, la nature du diplôme/attestation/certificat obtenu est nécessaire à l'édition numérique de ceux-ci. L'identifiant de la personne concernée dans les bases du responsable du traitement (e.g., le numéro étudiant), quant à lui permet [à définir].

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

4.1.4. Les données sont-elles exactes et tenues à jour ?

Concernant les données à caractère personnel traitées par BCD, celles-ci sont issues uniquement, et sans aucune modification ou analyse par BCD, de leur transmission par le responsable du traitement.

C'est donc à ce dernier d'évaluer leur exactitude avant toute transmission.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

4.1.5. Quelle est la durée de conservation des données ?

Données traitées pour la mise en œuvre de la solution BCdiploma :

Pour les utilisateurs de l'interface de gestion de la solution BCdiploma, BCD met en œuvre des traitements de données à caractère personnel ayant, notamment, pour finalité l'accès des utilisateurs à l'ensemble des fonctionnalités de la plateforme BCdiploma SaaS, y compris le support utilisateur.

Ces données concernent les nom, prénom et adresse de courriel des utilisateurs habilités à se connecter à la solution ainsi que leurs logs de connexion et d'action sur la plateforme.

Ces données sont conservées 2 ans après la fin du contrat entre l'entité de l'utilisateur et BCD.

Données des attestations générées :

BCD héberge l'historique des données des attestations générées appartenant au responsable du traitement sur les serveurs qu'il déploie dans le cloud de son hébergeur (solution Azure de Microsoft). Cet historique peut être purgé à tout moment par le responsable de traitement, sans entraver le bon fonctionnement des attestations générées. Lors de cette purge, il prend néanmoins la responsabilité de conserver ces données et les liens URL des attestations. En effet, BCD ne sera plus en mesure de les restituer ultérieurement. Dans ce cas, la suppression d'une attestation reste possible à partir de son URL. En l'absence de purge par le responsable de traitement, ces données sont conservées 2 ans après la fin du contrat entre l'entité de l'utilisateur et BCD.

Par ailleurs, les chiffrés de données déposés dans un environnement EVM compatible sont stockés pour la durée de cet environnement. Le chiffré étant réalisé via une fonction AES 256 GCM, ce stockage n'entraîne pas de non-conformité particulière puisqu'il s'agit de l'un des trois procédés accepté par la Cnil[1] (voir le paragraphe relatif aux mesures de chiffrement dans la partie relative aux risques pour plus de détails techniques).

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

---

[1] Premiers éléments d'analyse de la Cnil, « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », 20 septembre 2018

5. Principes fondamentaux

5.1. Mesures protectrices des droits

5.1.1. Comment les personnes concernées sont-elles informées à propos du traitement ?

Il appartient au responsable du traitement de fournir l'information aux personnes concernées par les opérations sous-traitées au moment de la collecte de leurs données à caractère personnel.

A ce titre, BCD propose une mention d'information type pouvant éventuellement être utilisée comme modèle ou inspiration par ce dernier. Cette mention type est accessible à cette adresse : https://docs.bcdiploma.com/fr/legal/notice.html#information-des-personnes-physiques-dont-les-donnees-sont-traitees-rgpd

---

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

5.1.2. Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Pour la mise en œuvre de la solution BCdiploma, les données traitées par BCD sont transmises par le responsable du traitement. Ainsi, BCD ne recueille pas le consentement des personnes concernées qui, s'il était nécessaire, serait de la responsabilité du responsable du traitement.

Pour les éventuelles autres données à caractère personnel traitées par le responsable du traitement, ce dernier devra préciser les modalités du recueil du consentement des personnes concernées si celui-ci est nécessaire.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

5.1.3. Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

Pour les données à caractère personnel entrant dans le cadre de la sous-traitance par BCD et dans la mesure du possible, BCD aide le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès de BCD des demandes d'exercice de leurs droits, BCD adresse ces demandes dès réception par courrier électronique à [à compléter avec un contact au sein du responsable de traitement].

Pour les éventuelles autres données à caractère personnel traitées par le responsable du traitement, ce dernier devra préciser ses propres modalités prévues pour répondre aux demandes d'exercice des droits des personnes concernées. A toutes fins utiles, il est indiqué au responsable du traitement que l'ensemble des droits n'a pas vocation à être soulevé. En effet, les droits applicables dépendent de la base légale retenue pour l'une ou l'autre des finalités définies.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

5.1.4. Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit à l'effacement (droit à l'oubli) ?

Les demandes de droit à l'effacement et de droit de rectification s'effectuent selon les mêmes modalités que vu précédemment.

Droit à l'effacement :

La solution BCdiploma met à disposition une fonctionnalité de suppression des attestations. Dès lors, plus aucune donnée n'est stockée dans les environnements cloud (Azure) de BCD.
Le chiffré des données est rendu définitivement indéchiffrable par suppression de la clé de persistance correspondante. Lorsque la donnée inscrite sur la Blockchain est un engagement, une empreinte issue d'une fonction de hachage à clé ou un chiffré utilisant un algorithme et des clés conformes à l'état de l'art, alors la Cnil considère que le responsable de traitement (ou son sous-traitant) peut rendre la donnée quasi inaccessible, et se rapprocher ainsi des effets d'un effacement de la donnée.

Il est précisé que par "quasi inaccessible", il est entendu que la probabilité de "casser" le chiffrement des données est équivalente au niveau de force brute que nécessiterait le cassage de la fonction AES 256 (voir le paragraphe relatif au chiffrement dans la partie relative aux risques pour plus de détails techniques).

Ainsi, la suppression des clés de déchiffrement garantit qu'il ne sera plus possible de prouver ou de vérifier quelle information avait été engagée. La donnée chiffrée ne présente plus alors aucun risque en termes de confidentialité (puisqu'elle ne peut plus être déchiffrée). A noter cependant que cette information devra aussi être supprimée des autres systèmes où elle aura été stockée pour le traitement.

Droit à la rectification :

Le droit à la rectification se met en œuvre dans la solution BCdiploma par un effacement (voir paragraphe ci-dessus) suivi d'une réémission avec les données rectifiées.
Ainsi, les mêmes solutions qu'en cas de demande de suppression de la donnée à caractère personnel pourraient être appliquées à la donnée erronée si elle doit être supprimée.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

5.1.5. Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit d'opposition ?

Les demandes de droit de limitation et droit d'opposition s'effectuent selon les mêmes modalités que vu précédemment.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

5.1.6. Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Concernant le sous-traitant BCdiploma, les clauses relatives au règlement de la protection des données à caractère personnel sont conformes à l'article 28 du RGPD.

Les environnements techniques utilisés, de type EVM compatibles, ne sont pas assimilables à des sous-traitants. La Cnil précise à ce sujet que « *la blockchain est une technologie sur laquelle peut s'appuyer un traitement de données à caractère personnel, et non pas un traitement ayant une finalité à part entière* »[2]. Ainsi, la blockchain est un "outil" et non un traitement pouvant être sous-traité.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

---

[2] Premiers éléments d'analyse de la Cnil, « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », 20 septembre 2018

5.1.7. En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Flux transfrontières résultant de la blockchain :

L'utilisation de la technologie blockchain repose sur le fait que toute transaction sur la chaîne de blocs implique :

- un envoi à tous les mineurs de la blockchain d'une demande de validation d'une transaction ;
- une mise à jour de la blockchain par l'ajout du nouveau bloc dans la chaîne de bloc auprès de tous les participants.

Les données des attestations concernées sont stockées de manière pseudonymisée, puisque leur chiffrement est réversible par celui qui détient la clé de déchiffrement. Cependant, concernant les tiers au traitement et notamment les mineurs de la blockchain, ceux-ci ne disposent pas de cette clé (il est renvoyé au paragraphe relatif à l'anonymisation dans la partie relative aux risques pour plus de détails).

Ainsi, les tiers devraient procéder au "cassage" de la clé de chiffrement afin d'accéder aux données à caractère personnel contenues dans la blockchain ; étant entendu que la probabilité de "casser" le chiffrement des données est équivalente au niveau de force brute que nécessiterait le cassage de la fonction AES 256, c'est à dire quasi impossible (voir le paragraphe relatif au chiffrement dans la partie relative aux risques pour plus de détails techniques).

Par ailleurs, il est précisé que, en cas de violation de données, la perte de données protégées par un algorithme de chiffrement à l'état de l'art, si la clé de chiffrement n'est pas compromise et si une copie des données reste disponible, n'est pas à considérer comme une violation de données comportant un risque (et donc ne doit pas faire l'objet d'une notification à la Cnil et encore moins d'une communication aux personnes concernées)[3].

Ainsi, par analogie et par extension, si la perte de données protégées par un algorithme de chiffrement à l'état de l'art n'est pas une violation de données à caractère personnel, alors on peut légitimement en déduire que la "consultation" des données protégées par un algorithme de chiffrement à l'état de l'art ne constitue pas une opération de traitement effectuée par les mineurs.

Par conséquent, il n'y a pas lieu de considérer des flux transfrontières résultant de l'utilisation des blockchains puisque les mineurs n'ont accès qu'aux données pseudonymisées via une fonction AES 256 qui est un algorithme de chiffrement à l'état de l'art quasi impossible à casser

[3] Billet de la Cnil, "Violations de données personnelles : les règles à suivre", 19 juin 2018

(voir le paragraphe relatif au chiffrement dans la partie relative aux risques pour les détails techniques).

Hébergement de la base de données sur le Cloud Azure :

BCD a mis en place et exploite sa solution BCdiploma en mode SaaS dans les centres de données Azure West Europe et France Central.

Cependant, selon les Conditions de confidentialité et de sécurité de Microsoft (contenues dans les Conditions relatives aux Produits qui sont applicables aux services Azure), l'utilisation des services Azure peut entraîner des transferts limités de données à caractère personnel en dehors du territoire de l'UE. De tels transferts étant alors effectués conformément à l'addendum sur la protection des données de Microsoft (accessible à l'adresse : https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA).

Ainsi, selon l'article « Transferts des Données » de cet addendum, « *tous les transferts de* [...] *Données à Caractère Personnel hors de l'Union européenne, de l'Espace Économique Européen, du Royaume-Uni et de la Suisse pour fournir les Produits et les Services sont soumis aux conditions des Clauses Contractuelles Types 2021 mises en œuvre par Microsoft* ».

Dès lors, les flux transfrontières mis en œuvre par Microsoft sont encadrés selon les clauses contractuelles types comme exigé par l'article 46 du RGPD.

Accès au diplôme/attestation/certificat en clair par l'accédant :

Enfin, les personnes à qui le diplômé remet le lien hypertexte peuvent être situées dans le monde entier, y compris dans un « pays tiers ».
Cependant, la réglementation relative à la protection des données à caractère personnel ne s'applique pas au traitement effectué par l'accédant dans la mesure où ce traitement relève d'un traitement « *effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique* » (article 2, 2, c) du RGPD).

Service d'emailing par la société Brevo :

Les données à caractère personnel collectées sont destinées aux services commerciaux et comptables de Brevo. Elles peuvent être transmises aux filiales de Brevo, ou à des sous-traitants tiers auxquels Brevo est autorisée à faire appel dans le cadre de l'exécution de ses services.

Dans ce contexte, les données à caractère personnel peuvent être transférées vers un pays de l'UE ou un pays tiers.

Selon sa politique de confidentialité (accessible à l'adresse suivante : https://www.brevo.com/legal/privacypolicy/), Brevo met en œuvre « *des garanties assurant la protection et la sécurité de ces données, conformément aux règles et réglementations applicables* ».

Brevo précise aussi qu'elle « *ne transfère les données à caractère personnel à des tiers à des fins de marketing sans le consentement exprès des Utilisateurs de Brevo.*

En outre, les données à caractère personnel ne peuvent être communiquées à des tiers à des fins autres que le marketing que dans les cas suivants :

- *avec leur autorisation ;*
- *à la demande des autorités légales compétentes, sur requête judiciaire ou dans le cadre d'un litige.* »

Service d'assistance intégré (outil de gestion des tickets d'assistance) par la société Hubspot :

La politique de confidentialité de Hubspot (accessible à l'adresse suivante : https://legal.hubspot.com/fr/privacy-policy) renvoie notamment à leur Data Protection Addendum qui précise, dans son article 8, f, A, que « *HubSpot ne transférera pas les données européennes vers un pays ou un destinataire qui n'est pas reconnu comme offrant un niveau adéquat de protection des données personnelles (au sens des Lois européennes sur la protection des données applicables), à moins qu'il ne prenne d'abord toutes les mesures nécessaires pour garantir que le transfert est conforme aux Lois européennes sur la protection des données applicables. Ces mesures peuvent inclure (sans limitation) :*

(i) *le transfert de ces données à un destinataire couvert par un cadre approprié ou un autre mécanisme de transfert juridiquement adéquat reconnu par les autorités ou tribunaux compétents comme assurant un niveau de protection adéquat des données à caractère personnel, y compris le cadre de protection des données ;*

(ii) *à un destinataire qui a obtenu une autorisation de règles d'entreprise contraignantes conformément aux Lois européennes sur la protection des données ; ou,*

(iii) *à un destinataire qui a exécuté les Clauses contractuelles types, dans chaque cas telles qu'adoptées ou approuvées conformément aux Lois européennes sur la protection des données applicables.* »

Ainsi pour les flux transfrontières étant, ou pouvant être, mis en œuvre lors de l'utilisation des services de BCD, notamment dans sa solution BCdiploma, ceux-ci sont encadrés par des garanties suffisantes, tel que recommandé par les articles 44 et suivants du RGPD.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

---

6. Risques

A titre liminaire, il est rappelé que, lors de la mise en œuvre de sa solution BCdiploma, la société BCD fait appel à plusieurs sous-traitant ultérieurs :

- la société Microsoft, pour son produit Azure ;
- la société Brevo, pour son service d'emailing ;
- la société Hubspot, pour son service d'assistance intégré (outil de gestion des tickets d'assistance).

Il est précisé au responsable du traitement qu'il ne relève pas de l'obligation de la société BCD de décrire les mesures de sécurité mises en œuvre par ses propres sous-traitants (qui correspondent à la qualification de sous-traitants ultérieurs pour le responsable du traitement). En effet, la société BCD reste la seule responsable de la sous-traitance confiée initialement vis-à-vis du responsable du traitement.

Cependant, il est précisé que :

- la société Microsoft dispose de la double certification SOC 2 et ISO 27001 ;
- la société Brevo dispose de la certification ISO 27001 ;
- la société Hubspot dispose de la certification SOC 2.

Ainsi, bien que ces deux certifications n'assurent pas une complète conformité aux exigences du RGPD, elles apportent la preuve des intentions et des efforts de mise en conformité avec le RGPD, notamment au regard des mesures de sécurité.

6.1. Mesures existantes ou prévues

6.1.1. Organisation et politiques de protection de la vie privée

Organisation :

La société BCD fournit la solution BCdiploma en mode SaaS au responsable du traitement. Elle agit donc comme sous-traitant de niveau 1.

Au sein de la société BCD, il y a une identification claire des personnes responsables (CEO, CTO, etc.), notamment dans la politique « Information Security Management Organisation Structure », et en particulier une identification claire de leur délégué à la protection des données à caractère personnel (désignation n° DPO-135854).

La société BCD dispose d'un registre des traitements en sa qualité de sous-traitant.

La société Microsoft, via sa solution Azure, assure l'hébergement de cette solution en mode SaaS. Elle agit donc comme sous-traitant de niveau 2.

Les sociétés Hubspot et Brevo fournissent des services optionnels à la solution BCdiploma (respectivement un service d'assistance intégré ainsi qu'un service d'emailing). Elles agissent donc en qualité de sous-traitants de niveau 2, lorsque ces services annexes sont fournis.

Pour les sous-traitants de niveau 2 Microsoft et Brevo, un DPO a été désigné (informations et données de contact accessibles sur les sites web de ces sous-traitants).

Politiques :

Des mesures organisationnelles sont prises pour garantir la sécurisation de l'exploitation :

- mise en place d'une notice concernant les traitements des données à caractère personnel des utilisateurs ;
- mise en place d'une politique de confidentialité ;
- mise en place d'un certain nombre de politiques relatives à la sécurité (notamment des SI, des technologies, des flux et des données).

La société BCD, dans sa politique « Pratiques en matière de confidentialité et de sécurité informatique », liste l'ensemble de sa documentation relative à la sécurité ainsi qu'à la confidentialité.

Enfin, la société BCD procède à la revue périodique ou à des tests périodiques de ces différentes politiques et procédures.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.2. Intégrer la protection de la vie privée dans les projets

Privacy by design :

Le "Privacy by Design" est un concept central dans le cadre de la protection des données, particulièrement en ce qui concerne la conformité avec le Règlement Général sur la Protection des Données (RGPD). L'adoption de ce principe dans le développement et le déploiement de solutions technologiques garantit que la protection des données personnelles est intégrée dès la conception et tout au long du cycle de vie des systèmes.

La mise en œuvre de "Privacy by Design" repose sur plusieurs modalités clés :

- Proactivité et prévention : Dès le début du développement, des mesures préventives sont mises en place pour anticiper et éviter les risques de violation de données. Cela implique l'identification et l'atténuation des risques potentiels avant même que le système ne soit opérationnel.

- Paramètres par défaut respectueux de la vie privée : par défaut, les paramètres des systèmes et applications sont configurés pour offrir le plus haut niveau de protection des données. Cela signifie que les utilisateurs n'ont pas besoin de modifier les paramètres pour protéger leur vie privée.

- Conception intégrée : la protection des données est intégrée dans l'architecture du système. Cela inclut l'utilisation de techniques de pseudonymisation et de chiffrement pour protéger les données personnelles, ainsi que la segmentation et la minimisation des données pour réduire l'exposition aux risques.

- Sécurité et intégrité des données : des mesures de sécurité sont mises en place pour protéger les données contre les accès non autorisés, les pertes et les altérations. Cela comprend des contrôles d'accès stricts et des audits réguliers de sécurité.

Tests :

Tous les tests de préproduction ont lieu dans un environnement de test. L'environnement de test reflète autant que possible l'environnement de production.

Des tests qui sont effectués reprennent, au minimum, le top 10 de l'OWASP (Open Web Application Security Project).

Des tests de pénétration externes sont effectués avant la publication initiale, puis périodiquement ou après une modification importante (voir paragraphe « Contrôle d'intégrité » infra).

Toutes les applications web accessibles au public sont testées à l'aide d'outils ou de méthodes de sécurité manuels ou automatisés au moins une fois par an ou après une modification importante.

Toutes les vulnérabilités identifiées dans le cadre de la phase de test, y compris les tests d'intrusion, sont corrigées avant la mise en production ou gérées par le biais du processus de gestion des risques.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.3. Gestion des risques

La société BCD a connaissance des risques que peuvent représenter les données au regard des objectifs du RGPD, à savoir :

- perte temporaire ou définitive des données ;
- indisponibilité du service et donc de l'accès aux données ;
- divulgation non autorisée de données à caractère personnel, transmises et conservées.

C'est la raison pour laquelle la société BCD accompagne le responsable du traitement dans la réalisation de son AIPD.

La société BCD procède à des audits externes, et dispose à ce titre d'une politique de gestion des audits.

La société BCD a déjà procédé à des tests de sécurité (notamment de pénétration) de sa solution BCdiploma. Le dernier en date est un audit réalisé par la société Synacktiv qui a le statut CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) selon l'accréditation donnée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Cet audit a révélé plusieurs vulnérabilités (1 de gravité élevée, 1 de gravité moyenne et 3 de gravité faible). Ces vulnérabilités ont été corrigées par BCD, et une attestation pourra être fournie au responsable du traitement sur demande.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.4. Gérer les incidents de sécurité et les violations de données

Gestion des incidents de sécurité :

La société BCD dispose d'une procédure de gestion des incidents (« Security and Incident management process ») qui précise la procédure à appliquer en cas d'incidents de sécurité ainsi que les rôles et responsabilités de chacun.

Gestion des violations de données :

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par courrier électronique à [adresse DPO du responsable du traitement].

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.5. Gestion des personnels

Information et formation des personnels :

BCD dispose d'une politique de sécurité des systèmes d'information, documentée et actualisée, communiquée à l'ensemble de son personnel.

Par ailleurs, BCD s'engage, de manière régulière, à sensibiliser et former les utilisateurs de sa solution BCdiploma (en particulier son propre personnel) à la sécurité des actifs informationnels, aux conséquences d'une faille de sécurité, ainsi qu'à leur rôle et obligations en la matière.

Confidentialité :

Tous les employés et les tiers qui ont accès à des informations confidentielles doivent signer un accord de confidentialité ou de non-divulgation avant d'avoir accès aux installations de traitement de l'information.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.6. Gestion des tiers accédant aux données

La société BCD s'est dotée d'une politique de gestion des fournisseurs.

Au titre de cette politique, tous les tiers sont enregistrés et inscrits dans le registre des fournisseurs tiers. Les tiers sont classés en fonction des données traitées, stockées ou transmises. Chaque tiers fait l'objet d'un audit et d'un examen de la sécurité des données conformément au processus d'audit et d'examen des tiers.

En particulier, un contrat, un accord et/ou un accord de traitement des données approprié doit être mis en place et applicable avant d'engager un fournisseur tiers pour traiter, stocker ou transmettre des informations confidentielles ou personnelles. Ces contrats et accords conclus avec des fournisseurs tiers prévoient le droit d'audit susmentionné.

Ainsi, les relations avec les sous-traitants de la société BCD (Microsoft, Brevo, Hubspot) sont gérés contractuellement et comprennent des clauses de confidentialité.

Ces sous-traitants sont soumis aux mêmes obligations que la société BCD.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.7. Maintenance

Au sein des CGU de la solution BCdiploma de BCD, il est spécifié que cette dernière est en charge de réaliser les opérations de maintenance corrective des anomalies et à faire ses meilleurs efforts pour corriger l'anomalie dans les meilleurs délais.

De plus, un service en ligne de tickets d'anomalies et d'incidents est mis à la disposition optionnelle du client (via la société Hubspot). Une notification de réception du ticket sera adressée dans l'heure au client. Le ticket sera traité sur la plage horaire 9 :00/18 :00 CET, les jours ouvrés en France.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.8. Chiffrement

Dans le cadre de l'utilisation de l'application BCdiploma SaaS, les données des attestations sont inscrites chiffrées sur la blockchain.

Cette inscription sur la blockchain repose sur un protocole de chiffrement par bloc en cryptographie symétrique AES 256 GCM dont le but vise à assurer la confidentialité en cryptant les données de manière à ce que les parties non autorisées ne puissent pas les lire sans la clé correcte. Le chiffrement AES étant un algorithme de cryptographie symétrique, cela signifie que le processus de chiffrement et de déchiffrement utilise la même clé pour les deux processus. Cela signifie que l'expéditeur et le destinataire des données en question ont besoin d'une copie de la clé secrète.

Cette fonction fait partie des exemples cités par la Cnil comme étant un algorithme sûr et reconnu[4]. Cette fonction est reconnue par le NIST et le U.S. DHS comme un système non vulnérable aux attaques quantiques[5].

Par ailleurs, les clés AES 256 GCM ne sont jamais stockées mais construites dynamiquement à la demande au moment de leur utilisation. Elles sont ainsi protégées par un procédé cryptographique de type SSS décrit dans le brevet US20200099511A1.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

---

[4] Billet Cnil, « Sécurité : Chiffrement, hachage, signature », 14 mars 2024

[5] U.S Department of Homeland Security POST-QUANTUM CRYPTOGRAPHY FREQUENTLY ASKED QUESTIONS

6.1.9. Anonymisation

La fonction AES-256 GCM, dans la mesure où elle n'entraine pas une anonymisation définitive des données, consiste, en principe, en des mesures de pseudonymisation.

Dans son considérant 26, le RGPD précise que les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable.

Cependant, pour déterminer si une personne physique est identifiable, le RGPD précise aussi (même considérant) qu'il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage.

Or, pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci.

Ainsi, pour identifier la personne physique, les tiers qui ne disposent pas des clés de déchiffrage vont devoir "casser" le chiffrement.

A ce titre, et comme il a été déjà évoqué supra, la probabilité de "casser" le chiffrement des données est équivalente au niveau de force brute que nécessiterait le cassage de la fonction AES 256, soit quasiment impossible. En revanche, le responsable du traitement dispose des clés de déchiffrage.

En conséquence, les données à caractère personnelle qui font l'objet d'un chiffrement par BCD sont bien à considérer comme des données pseudonymisées.

Cependant, bien que ne consistant pas en une anonymisation parfaite, la pseudonymisation constitue une des mesures recommandées par le RGPD pour limiter les risques liés au traitement de données personnelles (selon la Cnil[6]).

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

---

[6] Billet Cnil, « L'anonymisation de données personnelles », 19 mai 2020

6.1.10. Contrôle des accès logiques

Accès :

La société BCD dispose d'une politique d'habilitation.
En application de cette politique, les habilitations sont accordées selon le principe du moindre privilège ; c'est-à-dire que les utilisateurs n'ont accès qu'aux informations dont ils ont besoin pour accomplir leurs tâches et remplir leur rôle.

Les accès sont accordés par le CTO de la société BCD, le propriétaire du système d'information ou le « propriétaire des données » (data owner) qui a été formellement approuvé en amont.

L'accès n'est accordé à des tiers que dans le cadre d'un contrat en cours et d'un accord de confidentialité ou de non-divulgation applicable. L'accès est accordé pour une durée déterminée, à un système spécifique, à une personne spécifique et est fourni sur réception d'une demande d'accès formelle, valide et autorisée.

Revue des accès :

L'accès des utilisateurs aux systèmes est examiné au moins une fois par an pour s'assurer qu'il est toujours approprié et pertinent.
Les comptes inactifs et dormants font l'objet d'une enquête et des mesures appropriées sont prises, y compris la mise à jour de la documentation requise.

Le système d'accès principal des utilisateurs est examiné tous les 90 jours afin de s'assurer qu'il est toujours approprié et pertinent.

Mots de passe :

L'accès aux systèmes et aux informations est authentifié par des mots de passe.
Les mots de passe initiaux fournis aux utilisateurs doivent être modifiés lors de la première utilisation. De même, les mots de passe fournis par le fournisseur et les mots de passe par défaut sont modifiés dès l'installation.

La gestion des mots de passe est encadrée par une politique de gestion des mots de passe.

L'utilisation de l'authentification multi-facteur (MFA) est systématique pour l'accès aux informations sensibles et données personnelles.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.11. Cloisonnement

Réseau :

Les points de réseau situés dans les zones publiques ne permettent pas d'accéder au réseau interne de l'entreprise.

Environnements :

Les environnements de développement, de test et de production sont séparés et ne partagent pas de composants communs. Les environnements de développement, de test et de production se trouvent sur des groupes de ressources distincts.

Les tâches administratives sont séparées entre les environnements de développement, de test et de production.

Données :

Les données de production ne sont jamais utilisées à des fins de test ou de développement.

Les données relatives au titulaire de la carte ne sont jamais utilisées à des fins de test ou de développement.

Les données personnelles ne sont jamais utilisées à des fins de test ou de développement.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.12. Journalisation

Mesures de journalisation physique :

Les registres d'accès aux zones où des informations confidentielles sont traitées ou stockées sont conservés pendant au moins trois mois.

De même, les visiteurs sont enregistrés dans le registre des visiteurs et les informations sont conservées pendant au moins trois mois.

Mesures de journalisation numérique :

L'accès aux systèmes est contrôlé et signalé, et les actions qui affectent ou pourraient affecter directement ou indirectement la confidentialité, l'intégrité ou la disponibilité des données sont gérées via le processus de gestion des incidents (il est renvoyé au paragraphe supra à ce titre).

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.13. Contrôle d'intégrité

La société BCD a déjà procédé à des tests de sécurité (notamment de pénétration) de sa solution BCdiploma. Le dernier en date est un audit réalisé par la société Synacktiv qui a le statut CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) selon l'accréditation donnée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Cet audit a révélé plusieurs vulnérabilités (1 de gravité élevée, 1 de gravité moyenne et 3 de gravité faible). Ces vulnérabilités ont été corrigées par BCD, et une attestation pourra être fournie au responsable du traitement sur demande.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.14. Archivage

Données traitées au sein de la solution BCdiploma :

BCD héberge les données des certificats d'authenticité appartenant au responsable du traitement sur les serveurs qu'il déploie dans le cloud de son hébergeur (solution Azure de Microsoft). Ces données sont "chiffrées au repos", protégeant les données stockées en les chiffrant sur le disque, empêchant l'accès non autorisé en cas de compromission matérielle. Cette mesure garantit la confidentialité des données et la conformité aux exigences réglementaires.

En complément, voir paragraphe "Durée de conservation des données".

Données traitées pour la mise en œuvre de la solution BCdiploma :

BCD met en œuvre des traitements de données à caractère personnel ayant, notamment, pour finalité l'accès des utilisateurs à l'ensemble des fonctionnalités de la plateforme BCdiploma SaaS, y compris le support utilisateur.

Ces données concernent les nom, prénom et adresse de courriel des utilisateurs habilités à se connecter à la solution ainsi que leurs logs de connexion et d'action sur la plateforme.

Ces données sont conservées 2 ans après la fin du contrat entre l'entité de l'utilisateur et BCD.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.15. Sécurisation de l'exploitation

La société BCD a mis en place une politique de continuité d'activité (« Business Continuity Policy »). Cette politique renvoie notamment vers un ensemble de documentation permettant de répondre aux problématiques suivantes :

- les rôles et les responsabilités des personnes et des équipes ayant autorité pendant et après un incident,
- un processus de mise en œuvre d'une solution,
- des détails pour gérer les conséquences immédiates d'un incident perturbateur en tenant compte des éléments suivants
    - le bien-être des personnes
    - les options stratégiques, tactiques et opérationnelles pour répondre à la perturbation, et
    - la prévention de pertes supplémentaires ou de l'indisponibilité d'activités prioritaires
- des précisions sur la manière dont l'organisation communiquera avec les employés et leurs proches, les principales parties intéressées et les personnes à contacter en cas d'urgence, et dans quelles circonstances,
- la manière dont l'organisation poursuivra ou reprendra ses activités prioritaires dans des délais prédéterminés,
- les détails de la réponse médiatique de l'organisation à la suite d'un incident, y compris
    - une stratégie de communication
    - l'interface privilégiée avec les médias
    - des lignes directrices ou un modèle pour la rédaction d'une déclaration à l'intention des médias, et
    - les porte-parole appropriés.
- un processus de retrait une fois l'incident terminé.

De même, la société dispose de procédures documentées pour rétablir et reprendre ses activités à partir des mesures temporaires adoptées pour répondre aux besoins normaux de l'entreprise après un incident.

Enfin, des plans techniques de reprise après sinistre sont en place et testés.

Les plans de continuité des activités sont testés au moins une fois par an et/ou en cas de changement important. En cas d'incidents liés à la continuité des activités, ceux-ci sont enregistrés et suivis dans un registre. Les incidents liés à la continuité des activités sont également signalés à l'équipe Management Review Team.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.16. Sécurisation des canaux informatiques

La sécurisation des données échangées en mode SaaS :

La solution BCdiploma est en mode SaaS. Ainsi, tous les services d'application fournis par BCdiploma sont hébergés dans des centres de données Azure (SOC 1-2, ISO 27001-2) et s'appuient sur des services gérés, disponibles 24 heures sur 24 et 7 jours sur 7.

L'accès à ces services est sécurisé par plusieurs mesures, notamment :

- Les services sont uniquement accessibles via des protocoles sécurisés (https + TLS 1.2) sur des ports standard. Ainsi :
    - Tous les échanges vers/depuis/entre les services BCdiploma sont cryptés et sécurisés via https et TLS 1.2, sur la base de certificats SSL valides et non auto-signés, garantissant le cryptage de bout en bout des données en transit.
    - Au repos, les données sont cryptées à l'aide de l'algorithme de cryptage AES-256 (voir supra).
- L'accès aux services se fait par des points d'extrémité publics, avec des noms de domaine sécurisés par DNSSEC
- Les demandes entrantes sont systématiquement suivies et filtrées par un CDN (Azure Frontdoor) combiné à un Web Application Firewall (WAF), offrant une résistance aux attaques et aux DDoS
- Les communications entre services se font exclusivement via des protocoles sécurisés. Chaque service d'application de BCdiploma est déployé en tant qu'application gérée dans Azure (Appservice), garantissant :
    - une disponibilité et une évolutivité maximales, y compris des mécanismes d'équilibrage de charge et d'extension automatique.
    - une prise en compte optimale des CVE et des dernières versions des logiciels.

La sécurisation des liens URL des attestations :

Les liens des certificats sont protégés contre les attaques courantes (CSRF, spam, empoisonnement d'URL, etc.) :

- Au niveau du nom de domaine, protégé par DNSSec ;
- Au niveau de la qualité et de la surveillance active des certificats SSL utilisés pour authentifier nos serveurs ;
- Au niveau de l'infrastructure, via la porte d'entrée d'Azure et le pare-feu d'application Web garantissant une protection contre les attaques dos/ddos et les 10 principaux risques d'OWASP ;
- Au niveau logiciel, notamment avec une gestion rigoureuse des en-têtes de sécurité.

La sécurisation des clés de chiffrement (pour la fonction AES 256 GCM) :

Toutes les clés cryptographiques utilisées par la solution sont sécurisées dans l'environnement « Azure KeyVault ». En particulier, les « secp256k1 elliptic curve keys » nécessaires pour interagir avec les blockchains EVM sont sécurisées dans des Azure Keyvault HSM conformes à la norme FIPS 140-2 niveau 3.

La sécurisation des postes de travail :

La société BCD dispose d'une politique de sécurisation des postes de travail, documentée et actualisée au sein d'un ensemble de documents (« Mobile and Teleworking Policy et Protection Against Malware Policy » et "Clear Desk and Clear Screen Policy").

La sécurisation des canaux publics (ouverts aux tiers) :

La société BCD a mis en place un ensemble de mesures pour garantir la sécurité des canaux publics qu'elle met à disposition des utilisateurs. Ces mesures sont décrites exhaustivement dans un document ("Technical Documentation"), sécurisant les canaux publics grâce, en substance :

- à l'utilisation systématique du protocole sécurisé HTTPS pour les échanges ;
- à la sécurisation des domaines via DNSSEC ;
- au traitement et au filtrage des requêtes entrante par Web Application Firewall (WAF).

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.17. Sécurisation des matériels

Le personnel de la société BCD travaille principalement à distance, mais dispose de locaux physiques. Ces locaux physiques font l'objet d'une politique de sécurité des environnements physique documentée ("Physical and Environmental Security Policy"). Ces locaux physiques ne contiennent pas de matériel dédié.

Le matériel est fourni par la société. Ce matériel mobile est attribué individuellement et doit être enregistré dans la liste des appareils. Les appareils mobiles sont dotés d'un cryptage, d'un antivirus et d'un contrôle d'accès appropriés, le cas échéant. De même, il est précisé qu'un cryptage systématique des disques et des supports de stockage a lieu.

Un pare-feu personnel doit être installé et configuré sur tout appareil mobile se connectant à l'environnement des données relatives aux titulaires de cartes de paiement. Le logiciel de pare-feu personnel doit être configuré selon des paramètres de configuration spécifiques documentés, fonctionner activement et ne pas pouvoir être modifié par les utilisateurs d'appareils mobiles et/ou appartenant à des employés.

Les appareils mobiles peuvent être effacés à distance en cas de perte ou de vol. Cette fonction est activée avant que l'utilisateur n'ait accès à l'appareil mobile et le verrouillage automatique des appareils mobiles est activé.

Les appareils mobiles ne sont pas sauvegardés par défaut dans les solutions de sauvegarde de l'entreprise et relèvent de la responsabilité de l'utilisateur désigné.

Enfin, le BOYD est strictement encadré (sur autorisation spécifique).

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.18. Sécurité physique

Le contrôle des accès aux locaux :

L'accès au bâtiment se fait par l'intermédiaire d'une zone de réception surveillée.

L'accès aux sites et aux bâtiments est réservé au personnel autorisé. En particulier, les droits d'accès aux zones sécurisées sont régulièrement réexaminés et mis à jour, et révoqués si nécessaire. L'accès aux zones sécurisées est refusé par défaut. L'accès aux zones où des informations confidentielles sont traitées ou stockées est limité aux seules personnes autorisées par la mise en place de contrôles d'accès appropriés.

Les portes extérieures d'une zone de livraison et de chargement doivent être sécurisées lorsque les portes intérieures sont ouvertes,

L'accès des employés est basé sur le principe d'habilitations en fonction du poste. Les badges de contrôle d'accès sont attribués pour identifier l'employé et doivent être portés en permanence. Les badges de contrôle d'accès ne doivent être ni partagés, ni transférés, ni prêtés. L'accès est révoqué immédiatement en cas de résiliation et tous les badges d'accès physique sont désactivés et doivent être restitués.

Le cas échéant, le personnel externe ne se voit accorder qu'un accès restreint aux zones sécurisées ou aux installations de traitement d'informations confidentielles qu'en cas de besoin et est toujours accompagné ; cet accès est autorisé et surveillé. En particulier, l'accès à une zone de livraison et de chargement depuis l'extérieur du bâtiment doit être limité au personnel identifié et autorisé. L'aire de livraison et de chargement doit être conçue de manière à ce que les fournitures puissent être chargées et déchargées sans que le personnel de livraison n'ait accès à d'autres parties du bâtiment.

Les visiteurs peuvent accéder librement aux zones publiques. Les visiteurs reçoivent des instructions sur les exigences de sécurité et sur les procédures d'urgence. Les visiteurs reçoivent un laissez-passer qui indique clairement leur statut, leur interdit l'accès aux zones sécurisées et expire à la fin du jour ouvrable au cours duquel il a été délivré. L'accès des visiteurs aux zones sécurisées nécessite la vérification de leur identité et la présentation d'une pièce d'identité. Les visiteurs sont toujours accompagnés, sauf dans les zones publiques et les toilettes.

La sécurité physique des accès aux locaux :

Le toit, les murs et le sol extérieurs du site sont de construction solide.

Les portes et les fenêtres sont verrouillées lorsqu'elles ne sont pas surveillées. Toutes les portes extérieures sont convenablement protégées contre les accès non autorisés par des serrures et des mécanismes de contrôle des badges d'entrée.

Toutes les portes coupe-feu situées dans un périmètre de sécurité sont munies d'une alarme, surveillées et testées en même temps que les murs afin de déterminer le niveau de résistance requis.

Des systèmes de détection d'intrusion sont installés.

L'accès physique aux équipements de réseau :

L'accès physique aux équipements de réseau est limité. Notamment :

- aux points d'accès sans fil,
- aux routeurs,
- aux appareils portables,
- au matériel de réseau/communication,
- et aux lignes de télécommunication.

Les points de réseau situés dans les zones publiques ne permettent pas d'accéder au réseau interne de l'entreprise.

Les prises et points d'accès au réseau interne de l'entreprise sont sécurisés par un contrôle d'accès physique à l'entrée et à la sortie.

Il est interdit aux visiteurs de connecter des appareils aux prises / points de réseau permettant l'accès au réseau interne de l'entreprise, sauf autorisation explicite, et ils sont toujours accompagnés dans les zones où des prises / points de réseau sont actifs.

La sécurité face aux équipements d'enregistrement :

Les équipements photographiques, vidéo, audio ou tout autre équipement d'enregistrement, tels que les caméras des appareils mobiles, ne sont pas autorisés dans les zones sécurisées, sauf autorisation.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.19. Gestion des postes de travail

Concernant la solution BCdiploma :

La solution BCdiploma est fournie en mode SaaS. Elle n'est pas gérée via un poste de travail dédié au sein de la société BCD.

Concernant les postes du personnel :

La société BCD dispose d'une politique de sécurisation des postes de travail, documentée et actualisée au sein d'un document « Clear Desk and Clear Screen Policy »), indiquant en substance :

- Les ordinateurs sont déconnectés ou verrouillés lorsqu'ils sont laissés sans surveillance.
- L'utilisation non autorisée des photocopieurs et des technologies de reproduction est empêchée.
- Les dispositifs de paiement sont sécurisés lorsqu'ils ne sont pas utilisés.
- Les supports de données confidentiels sont détruits de manière sécurisée.
- Les bureaux sont rangés à la fin de chaque journée de travail.
- Les notifications et pop-ups sont désactivés lors des présentations et dans les espaces publics.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.20. Lutte contre les logiciels malveillants

Concernant la solution BCdiploma :

Les demandes entrantes sont systématiquement suivies et filtrées par un CDN (Azure Frontdoor) combiné à un Web Application Firewall (WAF), offrant une résistance aux attaques et aux DDoS.

Concernant les matériels du personnel :

La société BCD dispose d'une politique de sécurisation des postes de travail, documentée et actualisée au sein d'un ensemble de documents (« Mobile and Teleworking Policy » et « Protection Against Malware Policy »).

Du fait du cloisonnement et de la technique utilisée (la blockchain et Microsoft Azure), les données, notamment personnelles, traitées dans le cadre de la solution BCdiploma ne sont pas impactées par l'éventuelle compromission d'un matériel du personnel.

Cependant, il est précisé qu'un pare-feu personnel doit être installé et configuré sur tout appareil mobile se connectant à l'environnement des données relatives aux titulaires de cartes de paiement. Le logiciel de pare-feu personnel doit être configuré selon des paramètres de configuration spécifiques documentés, fonctionner activement et ne pas pouvoir être modifié par les utilisateurs d'appareils mobiles et/ou appartenant à des employés.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.21. Sauvegarde des données

Concernant la solution BCdiploma :

Pour rappel, les données des attestations générées via la solution BCdiploma sont téléversées par le responsable du traitement dans l'application BCdiploma SaaS et inscrites dans la blockchain après chiffrement, puis rendues accessibles via le lien URL de l'attestation.
L'historique des données des attestations émises est mis à disposition du responsable du traitement dans l'application BCdiploma SaaS. Le responsable du traitement est informé que BCD héberge les données des attestations appartenant au responsable du traitement sur les serveurs qu'il déploie dans le cloud de son hébergeur (solution Azure de Microsoft).

Le responsable du traitement peut, à tout moment, supprimer tout ou partie de l'historique des données de attestations via l'application BCdiploma SaaS, sans altérer le bon fonctionnement des certificats d'authenticité déjà générés. En cas de suppression des données par le responsable du traitement, BCD n'est pas en mesure, par la suite, de restituer ces données, et le responsable du traitement sera seul responsable de la conservation des données qu'il estime nécessaire à la bonne administration des attestations émises.

Dans ce cas, BCD précise ne réaliser aucune sauvegarde des données des attestations supprimées par le responsable du traitement. Le responsable du traitement doit ainsi, dans ce cas, réaliser ses propres sauvegardes et archivages électroniques.

Le code de développement de la solution BCdiploma est stocké dans un dépôt de code sécurisé qui applique et respecte les exigences de la politique de contrôle d'accès et de séparation des tâches.

Concernant la sauvegarde réalisée par la société BCD, celle-ci dispose d'une politique et d'un plan de gestion des sauvegardes formels, documentés et à jour.

Ainsi, BCD revoit et teste régulièrement son plan et ses procédures de gestion des sauvegardes pour la solution. De même, elle vérifie et tient à jour un inventaire de toutes les sauvegardes disponibles. La solution BCdiploma fait notamment l'objet de sauvegardes quotidiennes, hebdomadaires et mensuelles, décrites au sein d'une procédure écrite et maintenues dans un document « Data management procedure ».

Toutes les sauvegardes de la solution sont vérifiées et cryptées à l'aide d'un cryptage fort (AES-256).

Concernant les matériels du personnel :

Le personnel de BCD n'a pas à stocker sur ces appareils mobiles de données relatives au traitement mis en œuvre par le responsable du traitement dans le cadre de la solution BCdiploma.

A toutes fins utiles, il est cependant précisé que les appareils mobiles peuvent être effacés à distance en cas de perte ou de vol. Cette fonction est activée avant que l'utilisateur n'ait accès à l'appareil mobile et le verrouillage automatique des appareils mobiles est activé.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.22. Surveillance du SI

Les accès sont contrôlés conformément à la politique de contrôle des accès mis en place (voir supra).

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

6.1.23. Eloignement des sources de risques

De par l'utilisation en mode SaaS de sa solution BCdiploma sur le cloud Azure, la société BCD bénéficie des datacenters de Microsoft.

Ces data centers répondent aux meilleures exigences en matière de sécurité.

Ce plus, ceux-ci sont nombreux et interconnectés ; permettant ainsi le rapatriement des données d'un data center à l'autre le cas échéant (dégâts environnementaux, etc.).

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

7. Risques

La société BCD a précisé les analyses des risques concernant les traitements de données à caractère personnel ayant lieu au sein de sa solution BCdiploma.

Cependant, ces analyses de risques doivent porter sur le traitement dans son entier. Dès lors, c'est au responsable du traitement de définir celles-ci en fonction du traitement qu'il met en œuvre.

7.1. Accès illégitime à des données

7.1.1. Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

L'accès illégitime aux données à caractère personnel traitées dans la solution BCdiploma permet l'accès aux données que le responsable de traitement a décidé de faire figurer sur les attestations (voir paragraphe "quelles sont les données traitées ?").

Ainsi, le titulaire d'une attestation peut potentiellement subir des atteintes à sa vie privée (divulgation des données, chantage, jalousie professionnelle, etc.) ainsi qu'une atteinte à sa réputation (absence de mention sur son diplôme, etc.).

De plus, il y a un risque de perte de confiance sur la fiabilité du dispositif et de ses intervenants (le responsable du traitement – en tant qu'institution émettrice – et la société BCD).

7.1.2. Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Un accès illégitime aux données à caractère personnel traitées dans la solution BCdiploma pourrait être causé via :

- la perte ou vol des identifiants,
- non-respect des obligations de discrétion,
- piratage d'un des outils ou une attaque informatique,
- non verrouillage d'un poste de travail,
- erreur d'adressage d'un courriel/courrier.

7.1.3. Quelles sources de risques pourraient-elles en être à l'origine ?

Source humaine accidentelle : le personnel de l'institution émettrice, le personnel de la société BCD, le personnel d'un autre sous-traitant.

Source humaine malveillante : pirate informatique.

7.1.4. Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

L'ensemble des catégories listées précédemment, à savoir :

- Chiffrement,
- Pseudonymisation,
- Cloisonnement,
- Contrôle des accès logiques,
- Journalisation,
- Contrôle d'intégrité,
- Archivage,
- Sécurisation des documents papier,
- Sécurisation de l'exploitation,
- Lutte contre les logiciels malveillants,
- Gestion des postes de travail,
- Maintenance,
- Sécurisation des canaux informatiques,
- Surveillance du SI,
- Sécurité physique,
- Sécurisation des matériels,
- Eloignement des sources de risques,
- Organisation de la politique de protection de la vie privée,
- Gestion des personnels,
- Gestion des risques,
- Gérer les incidents de sécurité et les violations de données,
- Intégrer la protection de la vie privée dans les projets,
- Superviser la protection de la vie privée,
- Gestion des tiers accédant aux données.

7.1.5. Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limité. En effet, les personnes concernées, notamment les titulaires des attestations, pourraient connaître des conséquences négatives qu'elles devraient pouvoir surmonter.

7.1.6. Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Limitée. Au vu des sources de risques retenues, la réalisation de la menace semble limitée, en s'appuyant sur les caractéristiques détaillées précédemment de la solution BCdiploma.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

7.2. Modifications non désirées de données

7.2.1. Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

La modification des données traitées au sein de la solution BCdiploma pourrait entraîner la corruption du diplôme, attestation ou certificat édité.

Ainsi, l'intégrité du document ne serait plus garantie et ce dernier ne pourra alors plus remplir sa fonction initiale : être la version numérique authentifiée d'un document papier certifié.

En conséquence les impacts sont nombreux : toutes opérations nécessitant de prouver son niveau de connaissance via la présentation numérique d'un diplôme, d'attestation ou de certification est compromise. Ce qui peut être particulièrement impactant dans le milieu professionnel notamment.

Cependant, il est précisé que le diplôme, attestation ou certificat pourra toujours être édité au format papier par l'institution émettrice.

7.2.2. Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Une modification non désirée des données à caractère personnel traitées dans la solution BCdiploma pourrait être causée via :

- un piratage d'un des outils ou une attaque informatique.

7.2.3. Quelles sources de risques pourraient-elles en être à l'origine ?

Source humaine malveillante : pirate informatique.

7.2.4. Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Bien que l'ensemble des mesures de sécurité existantes décrites précédemment servent de manière plus ou moins directe à empêcher la modification non désirée des données, les opérations de chiffrement et de pseudonymisation contribuent largement (et plus largement, le recours à la technologie blockchain).

7.2.5. Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limitée. En effet, les personnes concernées, notamment les titulaires du diplôme, vont obtenir un certificat numérique qui ne sera pas authentique. Cependant, le diplôme, attestation ou certificat pourra toujours être édité au format papier par l'institution émettrice.

7.2.6. Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable. Il ne semble pas possible que les sources actuelles de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques techniques de la blockchain, la fonction AES 256 étant notamment reconnue par le NIST et le U.S. DHS comme un système non vulnérable aux attaques quantiques[7].

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

---

[7] U.S Department of Homeland Security POST-QUANTUM CRYPTOGRAPHY FREQUENTLY ASKED QUESTIONS

7.3. Disparition de données

7.3.1. Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

La disparition des données au sein de la solution BCdiploma entraînerait soit l'incapacité d'éditer le document demandé, soit l'incapacité d'y accéder. De manière plus concrète, le titulaire ne pourra pas obtenir son diplôme, attestation ou certification en version numérique authentifiée.

En conséquence les impacts sont les mêmes que pour la modification non désirée vue précédemment, à savoir : toutes opérations nécessitant de prouver son niveau de connaissance via la présentation numérique d'un diplôme, d'attestation ou de certification est compromise. Ce qui peut être particulièrement impactant dans le milieu professionnel notamment.

Cependant, il est précisé que le diplôme, attestation ou certificat pourra toujours être édité au format papier par l'institution émettrice.

7.3.2. Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les principales menaces qui pourraient entraîner la perte des données sont :

- une erreur par suppression manuelle ;
- un problème entraînant la perte des données ou l'inaccessibilité aux data centers de Microsoft ;
- un piratage d'un des outils ou une attaque informatique.

7.3.3. Quelles sources de risques pourraient-elles en être à l'origine ?

Source non-humaine : tous accidents entraînant la perte des données dans les data centers de Microsoft (cas exceptionnel ou relevant de la force majeure).

Source humaine accidentelle : le personnel de l'institution émettrice, le personnel de la société BCD, le personnel d'un autre sous-traitant.

Source humaine malveillante : pirate informatique.

7.3.4. Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Bien que l'ensemble des mesures de sécurité existantes décrites précédemment servent de manière plus ou moins directe à empêcher la modification non désirée des données, les opérations liées à la prévention de ces risques (comme le chiffrement ou les procédures de gestion des incidents pour les attaques informatiques, la gestion du personnel pour les erreurs du personnel de la société BCD, etc.) mais aussi les opérations liées au rétablissement des données perdues (notamment la sauvegarde et l'archivage des données).

7.3.5. Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limitée. En effet, bien que les personnes concernées (notamment les titulaires du diplôme) ne puissent obtenir un certificat numérique, le diplôme, attestation ou certificat pourra toujours être édité au format papier par l'institution émettrice.

7.3.6. Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Limitée, Il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports.

Évaluation : [à évaluer par le responsable du traitement]
Commentaire d'évaluation : [à préciser par le responsable du traitement]
Plan d'action / mesures correctives : [à définir par le responsable du traitement]

7.4. Vue d'ensemble des risques

[à compléter par le responsable du traitement]