Description générale

Analyse d'impact sur la vie privée	
Responsable de traitement	Valiuz
Responsable de la conduite de l'étude d'impact	Mélanie DEFOORT - DPO / Julie THOMAS - Juriste
Date de mise à jour	Mar-23
Statut de l'analyse	Finalisée

Vue d'ensemble

Traitement étudié	Responsabilités liées au traitement	Référentiels applicables		
Création d'un profil client cross-entreprise: Valiuz reçoit de la part de ses entreprises partenaires les données qu'elles ont collectées dans le cadre de leur relation client, et les agrège autour d'un identifiant unique propre à chaque client, en vue de réaliser les traitements de profilage et statistiques décrits ci-après. **Segmentation:** Améliorer la segmentation et le profilage des bases clients de chaque entreprise partenaire : **OCCULTATION** **Statistiques:** Permettre aux entreprises de mieux comprendre le profil et le comportement d'achat de leurs clients via des analyses statistiques anonymes ("insights"). **OCCULTATION**	Les entreprises partenaires de Valiuz apparaissent comme responsables de traitement. Il s'agit des entreprises détenues par la Famille Mulliez et signataires du contrat du service proposé par Valiuz. Au jour de la présente étude, 19 entreprises sont concernées : DECATHLON, LEROY MERLIN FRANCE, KIABI, AUCHAN, BOULANGER, NORAUTO, ALINEA, FLUNCH, 3BRASSEURS, SAINT MACLOU, TOP OFFICE, TAPE A L'OEIL, JULES, BIZZBEE, ROUGE GORGE, GRAIN DE MALICE, NHOOD, ELECTRO DEPÔT, CHRONODRIVE, ONEY BANK. **OCCULTATION** Valiuz n'agit que sur les instructions des entreprises et uniquement pour le compte de celles-ci. Elle apparaît donc comme sous-traitant au sens du RGPD. Valiuz est cependant considérée comme responsable conjoint du traitement s'agissant du tag (traceur) déposé sur le site internet des entreprises et qui permet de collecter la navigation des internautes sur le site concerné. **OCCULTATION** Les données clients concernées sont sur le périmètre France. **OCCULTATION**	Non		

Données processus et supports

Finalité	Base légale et justification	Données traitées	Durée de conservation	Destinataires
Reconnaître leurs clients (Uses cases de reconnaissance client) **OCCULTATION** **Profil Matching des Clients** **OCCULTATION**	UZ RC 1 : Intérêt légitime UZ RC 2 : consentement	Nom, prénom, genre Date de naissance Adresse email N° de téléphone fixe et mobile Modèle et type de terminal utilisé Adresse postale Ticket de caisse **(OCCULTATION)** Informations relatives à la fidélité **(OCCULTATION)** ID commun (ID Valiuz) **OCCULTATION**	**OCCULTATION** **OCCULTATION** la durée de conservation est déterminée par chaque entreprise, qui ne doit envoyer à Valiuz que les données des clients qui sont en base active. Mémo : la CNIL recommande maximum 3 ans après le dernier contact s'agissant de données relatives à des clients / prospects. S'agissant des données d'historique d'achats **OCCULTATION** liées aux clients envoyés par les entreprises les données sont conservées 3 ans par Valiuz (purge automatique). **OCCULTATION**	**1. Entreprises partenaires** : **OCCULTATION** **2. Valiuz** : **OCCULTATION** **3. Sous-traitants de Valiuz :** **OCCULTATION** **4. Sous-traitants des entreprises : OCCULTATION**
Améliorer le profilage que les entreprises font de leur base clients (Uses cases Connaissance Client) : **OCCULTATION**	**Intérêt légitime** Il s'agit de l'intérêt légitime de chaque entreprise de comprendre les attentes de ses clients, de mettre à jour leurs données, et d'améliorer la pertinence des communications qu'elle peut leur adresser. Le profilage qui peut ainsi être réalisé par Valiuz pour le compte de chaque entreprise partenaire est légitime dans le cadre d'une relation commerciale entre un commerçant et son client, y compris s'il est utilisé à des fins de prospection commerciale (cf. article 21, considérant 70 considérant 47 du RGPD). Ce profilage est utilisé exclusivement dans l'objectif d'améliorer l'expérience client des personnes concernées. Il n'implique pas de données sensibles et n'affecte pas les personnes concernées de manière significative. Chaque personne dispose en outre de la possibilité de s'opposer à tout moment à ces traitements de données, soit directement auprès de chaque entreprise partenaire, soit directement auprès de Valiuz (https://valiuz.com/mes-droits/). **Consentement pour la collecte et l'utilisation des données de navigation.**	Nom, prénom, genre Date de naissance Adresse email N° de téléphone fixe et mobile Modèle et type de terminal utilisé Adresse postale Ticket de caisse **(OCCULTATION)** Informations relatives à la fidélité **(OCCULTATION)** Si consentement cookie: ID cookie, **OCCULTATION** **OCCULTATION.**	Durée de vie du cookie: 12 mois Données de navigation issues du cookies : 12 mois **OCCULTATION**	
Effectuer des opérations techniques permettant d'améliorer la qualité des données traitées, et de les enrichir grâce à l'open data (Uses cases Opérations techniques / Qualité **OCCULTATION** La finalité de ces traitements est donc déterminée, explicite et légitime compte tenu de l'activité des entreprises partenaires, qui sont des commerçants et cherchent à satisfaire les attentes de leurs clients en leur proposant des offres susceptibles de les intéresser. **OCCULTATION**	**Intérêt légitime** Il s'agit de l'intérêt légitime de chaque entreprise de comprendre les attentes de ses clients, de mettre à jour leurs données, et d'améliorer la pertinence des communications qu'elle peut leur adresser. Le profilage qui peut ainsi être réalisé par Valiuz pour le compte de chaque entreprise partenaire est légitime dans le cadre d'une relation commerciale entre un commerçant et son client, y compris s'il est utilisé à des fins de prospection commerciale (cf. article 21, considérant 70 considérant 47 du RGPD). Ce profilage est utilisé exclusivement dans l'objectif d'améliorer l'expérience client des personnes concernées. Il n'implique pas de données sensibles et n'affecte pas les personnes concernées de manière significative. Chaque personne dispose en outre de la possibilité de s'opposer à tout moment à ces traitements de données, soit directement auprès de chaque entreprise partenaire, soit directement auprès de Valiuz (https://valiuz.com/mes-droits/). L'intérêt légitime est justifié et formalisé au sein d'une analyse juridique (document séparé), suivant les critères suivants: a) L'intérêt poursuivi est légitime (l'intérêt est manifestement licite au regard du droit, il est déterminé de façon suffisamment claire et précise, il est réel et présent pour l'organisme concerné, et non fictif) b) Le traitement est nécessaire au regard de l'objectif poursuivi. c) Les personnes concernées peuvent raisonnablement s'attendre au traitement de données qui est envisagé: elles ne doivent pas être surprises. d) Les conséquences du traitement envisagé sur les personnes concernées (notamment sur leur vie privée) sont limitées (ex: pas plus de pub). c) Le degré d'intrusion dans la sphère individuelle du traitement envisagé est faible compte tenu de ses incidences sur la vie privée des personnes (traitement de données sensibles, traitement portant sur des personnes vulnérables, profilage, etc.), de ses incidences sur leurs autres droits fondamentaux (liberté d'expression, liberté d'information, liberté de conscience, etc.), des autres impacts concrets du traitement sur leur situation (suivi ou surveillance de leurs activités ou déplacements, exclusion de l'accès à des services, etc.).	Nom, prénom, genre Date de naissance Adresse email N° de téléphone fixe et mobile Modèle et type de terminal utilisé Adresse postale Ticket de caisse **(OCCULTATION)** Informations relatives à la fidélité **(OCCULTATION)** **OCCULTATION**		
Statistiques **OCCULTATION** Ces traitements de données ont pour finalité de permettre aux entreprises de comprendre qui sont leurs clients (profil type / tendances de consommation) et ainsi d'en tirer certaines conséquences (adaptation de leur offre, de leur implantation, etc.). Cette finalité est explicite et légitime compte tenu de l'activité des membres de l'alliance, qui sont des commerçants et cherchent à prendre des décisions stratégiques éclairées notamment par le profil type de leurs clients et les tendances de consommation de leurs clients.	**Intérêt légitime** Il s'agit de l'intérêt légitime de chaque entreprise de comprendre les attentes de ses clients, de mettre à jour leurs données, et d'améliorer la pertinence des communications qu'elle peut leur adresser. Le profilage qui peut ainsi être réalisé par Valiuz pour le compte de chaque entreprise partenaire est légitime dans le cadre d'une relation commerciale entre un commerçant et son client, y compris s'il est utilisé à des fins de prospection commerciale (cf. article 21, considérant 70 considérant 47 du RGPD). Ce profilage est utilisé exclusivement dans l'objectif d'améliorer l'expérience client des personnes concernées. Il n'implique pas de données sensibles et n'affecte pas les personnes concernées de manière significative. Chaque personne dispose en outre de la possibilité de s'opposer à tout moment à ces traitements de données, soit directement auprès de chaque entreprise partenaire, soit directement auprès de Valiuz (https://valiuz.com/mes-droits/). L'intérêt légitime est justifié et formalisé au sein d'une analyse juridique (document séparé), suivant les critères suivants: a) L'intérêt poursuivi est légitime (l'intérêt est manifestement licite au regard du droit, il est déterminé de façon suffisamment claire et précise, il est réel et présent pour l'organisme concerné, et non fictif) b) Le traitement est nécessaire au regard de l'objectif poursuivi. c) Les personnes concernées peuvent raisonnablement s'attendre au traitement de données qui est envisagé: elles ne doivent pas être surprises. d) Les conséquences du traitement envisagé sur les personnes concernées (notamment sur leur vie privée) sont limitées (ex: pas plus de pub). c) Le degré d'intrusion dans la sphère individuelle du traitement envisagé est faible compte tenu de ses incidences sur la vie privée des personnes (traitement de données sensibles, traitement portant sur des personnes vulnérables, profilage, etc.), de ses incidences sur leurs autres droits fondamentaux (liberté d'expression, liberté d'information, liberté de conscience, etc.), des autres impacts concrets du traitement sur leur situation (suivi ou surveillance de leurs activités ou déplacements, exclusion de l'accès à des services, etc.).	Nom, prénom, genre Date de naissance Adresse email N° de téléphone fixe et mobile Modèle et type de terminal utilisé Adresse postale Ticket de caisse **(OCCULTATION)** Informations relatives à la fidélité **(OCCULTATION)**		
OCCULTATION	Consentement	identifiant multi-site ("cross-site")	12 mois	**OCCULTATION**
OCCULTATION. Constitution d'une base de données réconciliant les identifiants cookie de différents partenaires pour un même navigateur **OCCULTATION**	Consentement	identifiant multi-site ("cross-site")	12 mois	**OCCULTATION**
Fourniture aux entreprises bénéficiaires du service d'un accès à la plateforme Valiuz leur permettant d'utiliser le service	Contrat conclu entre Valiuz et chaque entreprise partenaire	Adresse IP / Logs de connexion	12 mois	**OCCULTATION**

Résumé des résultats de l'analyse

Risques majeurs identifiés	Mesures et garanties	Niveau de risque résiduel
Risque d'atteinte à la vie privée des personnes concernées	**OCCULTATION**	**OCCULTATION**
Risque que l'information fournie aux personnes concernées soit insuffisante	La mise en place des mentions d'informations appartient à chaque entreprise partenaire. **OCCULTATION**	**OCCULTATION**

Risque d'une mauvaise remontée des préférences des personnes concernées	OCCULTATION	OCCULTATION	[redacted]
Accès illégitime aux données relatives aux personnes concernées	OCCULTATION	OCCULTATION	[redacted]

Analyse de l'impact sur la vie privée au regard des catégories de données personnelles traitées

Catégories de données personnelles	Impact initial	Justification de l'évaluation de l'impact initial
Données d'identification	OCCULTATION	Données pseudonymisées
Données transactionnelles	OCCULTATION	Données non sensibles susceptibles de révéler les centres d'intérêts, habitudes de consommation…
Données socio-démographiques	OCCULTATION	Données non sensibles mais révèlent des informations sur la vie familiale, situation financière etc.
Données de navigation	OCCULTATION	Données non sensibles mais susceptibles de révéler de nombreuses informations sur les intérêts, habitudes, typologie d'acheteurs etc.
Données issues de l'open data	OCCULTATION	Donnes pseudonymisées
RÉSULTAT DE L'IMPACT INITIAL TOTAL	OCCULTATION	Données non sensibles mais leur combinaison peut révéler des informations sur vie personnelle des personnes concernées

Echelle d'estimation de l'impact sur la vie privée lié à la nature des données :

1 - Mineur : Données non sensibles et limitées à des informations d'état civil et coordonnées.

2 - Limité : Données non sensibles, susceptibles de révéler des informations sur la vie personnelle ou professionnelle.

3 - Important : Données hautement personnelles (NIR, géolocalisation, coordonnées bancaires, etc.).

4 - Maximal : Données sensibles (catégories particulières) au sens du RGPD (révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, données génétiques, données biométriques aux fins d'identifier une personne physique de manière unique, données de santé ou concernant la vie sexuelle ou l'orientation sexuelle, données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes).

Analyse de l'impact sur la vie privée au regard des niveaux de risques juridiques

	Risques juridiques	Probabilité	Gravité	Niveau de risque	Description du risque et justification de l'évaluation du niveau de risque
RJ1	Risque d'atteinte à la vie privée des personnes concernées	OCCULTATION	OCCULTATION	OCCULTATION	Description du risque: Les traitements de données mis en oeuvre dans le cadre de l'alliance (UZ RC, UZ CC, UZ OT et UZ SA) reposent sur l'intérêt légitime de chaque entreprise partenaire. Cet intérêt légitime est documenté et justifié. OCCULTATION
RJ2	Risque de traitement de données hautement personnelles	OCCULTATION	OCCULTATION	OCCULTATION	Description du risque: Bien que cela ne soit pas l'objet des traitements de données mis en oeuvre dans le cadre du service proposé par Valiuz, il est possible que des données pouvant être considérées comme "hautement personnelles" OCCULTATION
RJ3	Risque de détournement de finalité	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RJ4	Risque que l'information fournie aux personnes concernées soit insuffisante	OCCULTATION	OCCULTATION	OCCULTATION	Description du risque: Il existe un risque que les personnes n'aient pas conscience que leur données sont partagées à Valiuz car : OCCULTATION
RJ5	Risque de non-conformité de certaines procédures d'obtention du consentement au dépôt du cookie	OCCULTATION	OCCULTATION	OCCULTATION	Description du risque: Les entreprises se resposent sur la base légale du consentement pour le dépôt du tag commun. Il s'agit d'un tag soumis à consentement dans la mesure où il permet de collecter des données personnelles (données de navigation, panier…) à des fins de personnalisation de la communication réalisée par les entreprises. OCCULTATION OCCULTATION
RJ6	Risque d'une mauvaise remontée des préférences du client consommateur	OCCULTATION	OCCULTATION	OCCULTATION	Description du risque: La remontée des choix des clients (consentement cookie, opt-out Valiuz), dépend principalement des entreprises partenaires. OCCULTATION

Echelle d'estimation de la probabilité de réalisation du risque :

1. Mineur : il ne semble pas possible que la menace puisse être réalisée au regard des caractéristiques du traitement.

2. Limité : il semble difficile que la menace puisse être réalisée au regard des caractéristiques du traitement.

3. Important : il semble possible que la menace puisse être réalisée au regard des caractéristiques du traitement.

4. Maximal : il semble extrêmement facile que la menace puisse être réalisée au regard des caractéristiques du traitement.

Echelle d'estimation de la gravité / impact du risque :

1. Mineur : Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficultés.

2. Limité : Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés.

3. Important : Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives.

4. Maximal : Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter.

Echelle de calcul du niveau de risque juridique

Impact / Gravité				
4 - Maximal	4	4	4	4
3 - Important	3	3	4	4
2 - Limité	2	2	3	3
1 - Mineur	1	2	2	3
Probabilité	1 - Mineur	2 - Limité	3 - Important	4 - Maximal

Analyse de l'effectivité des mesures correctives / garanties permettant d'assurer la conformité aux principes de protection de la vie privée et de réduire les risques identifiés

	Mesures / Garanties juridiques	Effectivité	Justification
MJ1	Finalités déterminées et respectées / Pas de partage des données entre les entreprises partenaires / Limitation des données collectées à ce qui est strictement nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation)	OCCULTATION	Les données sont nécessaires pour répondre aux finalités visées et ne sont utilisées que pour réaliser ces finalités. OCCULTATION
MJ2	Qualité : préservation de la qualité des données à caractère personnel (exactes et tenues à jour)	OCCULTATION	L'entreprise est responsable de fournir des données exactes et à jour. OCCULTATION
MJ3	Durée de conservation limitée	OCCULTATION	OCCULTATION En tout état de cause, les durées suivantes sont appliquées par Valiuz: - Données de navigation (page consultées, produits consultés): 13 mois - Historique d'achat du client: 3 ans, cette durée se justifiant par la nécessité de pouvoir définir des tendances et des évolutions des habitudes d'achat.
MJ4	Recueil d'un consentement conforme au RGPD et à la doctrine de la CNIL	OCCULTATION	Le consentement est exigé pour le dépôt d'un cookie/traceur permettant de suivre la naviguation d'une personne sur un site internet et de lui adresser des publicités ciblées. Tel est le cas du tag commun utilisé par les entreprises partenaires. Les entreprises doivent respecter la réglementation e-privacy et se conformer aux recommandations de la CNIL : - Mise en place d'un outil simple de gestion des consentement (CMP), - Mise en place d'une information décrivant le tag au sein de la CMP et de la politique "cookies" figurant sur le site internet des entreprises, - Le cookie ne doit pas se déposer tant que l'internaute n'a pas donné son consentement (en cliquant sur "J'accepte"). - Mention des partenaires utilisant des cookies sur le site et liste de ces partenaires accessible via un lien cliquable.
MJ5	Fourniture d'une information complète et compréhensible aux personnes concernées	OCCULTATION	Les personnes concernées doivent être informées des conditions du traitement de leurs données via l'ensemble des moyens d'information utilisés par l'entreprise, notamment sur le site internet des entreprises (au sein d'une charte d'utilisation et d'une politique de confidentialité présentes en page d'accueil), et en magasin (collecte offline) via un affichage (art. 12, cons. 58, 60 et 61 RGPD). OCCULTATION **Il appartient aux entreprises, lorsqu'elles rejoignent Valiuz, de s'assurer d'informer les personnes dont les données sont déjà en base, avant de les transmettre à Valiuz pour la fourniture du Service, en respectant un délai suffisant pour permettre aux clients de s'opposer au traitement. L'entreprise détermine les conditions dans lesquelles elle va communiquer à l'égard de ses clients.** La mise en place des mentions d'informations appartient à chaque entreprise participante. OCCULTATION
MJ6	Garanties contractuelles obtenues des entreprises participantes et des autres fournisseurs de données, afin d'assurer que ceux-ci imposent le même niveau de protection des personnes, de consentement et d'information, lorsqu'ils collectent de l'information et/ou des consentements	OCCULTATION	Clauses contractuelles insérées systématiquement dans les contrats afin de s'assurer que les entreprises participantes et fournisseurs de données garantissent fournir des données collectées de façon loyale et respecter les recommandations de la CNIL en matière de collecte du consentement, notamment cookie, lorsque nécessaire. En particulier: OCCULTATION
MJ7	Recommandation d'un bouton d'opposition au partage des données à intégrer sur les formulaires de collecte des données (création de compte, paramétrage du compte)	OCCULTATION	OCCULTATION
MJ8	Mise en place d'une procédure d'audit afin de valider la conformité des entreprises partenaires et autres fournisseurs de données (bandeau cookie, politique de confidentialité…)	OCCULTATION	Une clause d'audit est intégrée de manière systématique dans les contrats avec les fournisseurs exterieurs à l'alliance. OCCULTATION
MJ9	Mise en place de procédures pour assurer l'effectivité de l'exercice des droits des personnes concernées	OCCULTATION	Un processus d'opposition automatique est accessible à partir du site Valiuz. Les personnes peuvent également formuler toute autre demande (accés, etc), en écrivant à Valiuz (mesdroits@Valiuz.com). Les entreprises ont également mis en place un processus d'opposition avec remontée de l'information à Valiuz. OCCULTATION

Echelle d'estimation de l'effectivité de la mesure corrective / garantie :

1. Négligeable : la mesure n'est pas mise en oeuvre ou ne réduit pas le niveau de risque.

2. Limitée : la mesure n'est pas systématiquement mise en oeuvre ou ne réduit que très peu le niveau de risque.

3. Importante : la mesure est systématiquement mise en oeuvre mais ne réduit pas complètement le niveau de risque ou ne correspond pas aux recommandations du secteur / à l'état de l'art.

4. Maximale : la mesure est systématiquement mise en oeuvre et supprime totalement ou quasi-totalement le risque.

MJ10	Mise en place de procédures internes permettant d'assurer un haut niveau de protection des données	**OCCULTATION**	**OCCULTATION**
MJ11	Les obligations des sous-traitants sont clairement définies et contractualisées / Pas de réutilisation des données pour d'autres finalités que celles fixées par chaque entreprise partenaire	**OCCULTATION**	**OCCULTATION**
MJ12	En cas de transfert de données en dehors de l'Union européenne, les données sont protégées de manière équivalente	**OCCULTATION**	Valiuz s'efforce de limiter les possiblités de transferts de données hors UE en exigeant systématiquement la localisation des données en UE. Des transferts de données hors UE restent cependant possibles **OCCULTATION**. Les CCT de la Commission Européenne sont systématiquement annexées au contrat conclu avec les prestataires.
MJ13	Pas de données sensibles / Contrôle des segments proposés suivant notre démarche éthique	**OCCULTATION**	**OCCULTATION**
MJ14	Respect des attentes raisonnables des personnes / Sondage client / Focus group	**OCCULTATION**	**OCCULTATION**
MJ15	Sensibilisation des collaborateurs	**OCCULTATION**	**OCCULTATION**

Analyse de l'impact sur la vie privée au regard des niveaux de risques techniques

	Catégories de risques	Sources du risque	Principales menaces de réalisation du risque	Impacts potentiels sur la vie privée	Probabilité	Gravité	Niveau de risque	Justification de l'évaluation du niveau de risque
RT1	Accès illégitime aux données	Sources humaines internes ou externes agissant délibérément (salariés, utilisateurs, tiers…) / Sources non-humaines externes de façon limitée	OCCULTATION	Dérangement / harcèlement des clients. Utilisation des données pour ternir la réputation des personnes. Retraitement des données visant à établir des segments sensibles (ex: faisant apparaître une appartenance religieuse)	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RT2			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RT3			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RT4			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RT5	Modification non désirée des données	Sources humaines internes ou externes agissant accidentellement ou intentionnellement	OCCULTATION	Mauvaise identification de la personne pouvant entrainer une communication inadaptée à son profil	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RT6			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RT7			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RT8			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION
RT9	Disparition des données	Sources humaines agissant accidentellement ou intentionnellement. Sources non humaine limitées	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION.
RT10			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	
RT11			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	
RT12			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	
RT13			OCCULTATION		OCCULTATION	OCCULTATION	OCCULTATION	

Principales sources des risques techniques :

Sources humaines internes, par ex. : Erreurs humaines ou manque de diligence des salariés, stagiaires, intérimaires ou mandataires sociaux, défaut ou insuffisance des mesures de sécurité mises en place (ex : dispositif d'identification ou d'authentification, gestion des accès, suivi des sessions administrateurs…), défaut ou insuffisance des mesures de confidentialité mises en place (anonymisation, pseudonymisation, chiffrement…), défaut ou insuffisance des procédures de gestion et/ou de notification des violations de données personnelles ou des incidents de sécurité.

Sources humaines externes, par ex. : Actes accidentels ou délibérés des destinataires de données personnelles, tiers autorisés, clients, prestataires ou visiteurs, attaques ciblées de concurrents, pirates informatiques ou d'organisations criminelles.

Sources non humaines, par ex. : Virus informatique non ciblé, campagnes de *phishing* massive, codes malveillants d'origine inconnue, pannes techniques, matériaux défectueux, catastrophes naturelles.

les caractéristiques des supports.

2. Limité : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports.

3. Important : il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports.

Echelle d'estimation de la gravité / impact du risque :

1. Mineur : Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficultés.

2. Limité : Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés.

3. Important : Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives.

4. Maximal : Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter.

Echelle de calcul du niveau de risque technique				
Impact / Gravité				
4 - Maximal	3	4	4	4
3 - Important	3	3	4	4
2 - Limité	2	2	3	3
1 - Mineur	1	1	2	3
Probabilité	1 - Mineur	2 - Limité	3 - Important	4 - Maximal

Analyse de l'effectivité des mesures correctives / garanties permettant de réduire les risques identifiés

	Mesures / Garanties sécurité organisationnelle et technique	Effectivité	Justification
Mesures portant spécifiquement sur les données du traitement			
MT1	Pseudonymisation	**OCCULTATION**	**OCCULTATION**
MT2	Chiffrement	**OCCULTATION**	**OCCULTATION**
MT3	Cloisonnement des données (par rapport au reste du système d'information)	**OCCULTATION**	**OCCULTATION**

Echelle d'estimation de l'effectivité de la mesure corrective / garantie :

1. Négligeable : la mesure n'est pas mise en oeuvre ou ne réduit pas le niveau de risque.

2. Limitée : la mesure n'est pas systématiquement mise en oeuvre ou ne réduit que très peu le niveau de risque.

3. Importante : la mesure est systématiquement mise en oeuvre mais ne réduit pas complètement le niveau de risque ou ne correspond pas aux recommandations du secteur / à l'état de l'art.

4. Maximale : la mesure est systématiquement mise en oeuvre et supprime totalement ou quasi-totalement le risque.

MT4	Contrôle des accès logiques des utilisateurs	**OCCULTATION**	**OCCULTATION**
MT5	Traçabilité (journalisation)	**OCCULTATION**	**OCCULTATION**
MT6	Contrôle d’intégrité	**OCCULTATION**	**OCCULTATION**
MT7	Archivage	**OCCULTATION**	**OCCULTATION**
MT8	Sécurité des documents papier	**OCCULTATION**	**OCCULTATION**
MT9	Minimisation	**OCCULTATION**	**OCCULTATION.**
Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre			
MT10	Sécurité de l’exploitation	**OCCULTATION**	**OCCULTATION**
MT11	Lutte contre les logiciels malveillants	**OCCULTATION**	**OCCULTATION**
MT12	Gestion des postes de travail	**OCCULTATION**	**OCCULTATION**

MT13	Sécurité du site internet et de la plateforme	**OCCULTATION**	**OCCULTATION**
MT14	Sauvegardes	**OCCULTATION**	**OCCULTATION**
MT15	Maintenance	**OCCULTATION**	**OCCULTATION**
MT16	Sécurité des canaux informatiques (réseaux)	**OCCULTATION**	**OCCULTATION**
MT17	Surveillance	**OCCULTATION**	**OCCULTATION**
MT18	Contrôle d'accès physique	**OCCULTATION**	**OCCULTATION**
MT19	Sécurité des matériels	**OCCULTATION**	**OCCULTATION**
MT20	Éloignement des sources de risques	**OCCULTATION**	**OCCULTATION**
MT21	Protection contre les sources de risques non humaines	**OCCULTATION**	**OCCULTATION**
Mesures organisationnelles (gouvernance)			

MT22	Organisation	**OCCULTATION**	**OCCULTATION**
MT23	Politique (gestion des règles)	**OCCULTATION**	**OCCULTATION**
MT24	Gestion des risques	**OCCULTATION**	**OCCULTATION**
MT25	Gestion des projets (démarche Privacy by design)	**OCCULTATION**	**OCCULTATION**
MT26	Gestion des incidents et des violations de données	**OCCULTATION**	**OCCULTATION**

MT27	Gestion des personnels (mesures de sensibilisation, procédure pour limiter les accès illégitimes aux données)	**OCCULTATION**	**OCCULTATION**
MT28	Relations avec les tiers	**OCCULTATION**	**OCCULTATION**
MT29	Intégrer la protection de la vie privée dans les projets	**OCCULTATION**	OCCULTATION

Risque résiduel - acceptation du risque résiduel - validation

Risques	Niveau de risque initial	Mesures correctives / garanties	Effectivité de la mesure / garantie	Evaluation du risque résiduel		Evaluation de l'acceptabilité des risques résiduels *(à compléter par le client)*			
				Niveau de risque résiduel	Justification	Acceptable ?	Justification	***Vérification*** *(si possible: DPO, chef de projet, IT, direction…)*	**Validation** *(par le responsable de traitement, le responsable projet…)*
Risque d'atteinte à la vie privée des personnes concernées	OCCULTATION	* Fourniture d'une information complète et compréhensible aux personnes concernées au sein de la politique de confidentialité de chaque entreprise et sur les formulaires de collecte des données. * Mise en place de procédures pour assurer l'effectivité de l'exercice des droits des personnes concernées, de l'information des personnes et du receuil de leur consentement (mentions communes, contrôle de la mise en place des mentions) * Possibilité pour les personnes de s'opposer aux traitements Valiuz directement sur le site Valiuz * Possibilité pour les personnes de s'opposer aux partage de leurs données à Valiuz lors de la création de leur compte client en ligne OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	Oui	OCCULTATION	OCCULTATION.	Validé
Risque de traitement de données hautement personnelles	OCCULTATION	* Contrôle de la taxonomie pour s'assurer de la conformité des critères * Mise en place de procédures internes permettant d'assurer un haut niveau de protection des données OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	Oui	Le risque est très peu probable compte tenu de l'offre de service proposée par Valiuz.	Acceptable	Validé
Risque de détournement de finalité	OCCULTATION	Le mandat confié à Valiuz par les entreprises est fixé au contrat: aucune autre utilisation des données que celles autorisées au contrat n'est donc possible. OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	Oui	Le risque de détournement de finalité est minime : Valiuz n'agit que sur instructions des entreprises.	Acceptable	Validé
Risque que l'information fournie aux personnes concernées soit insuffisante	OCCULTATION	La mise en place des mentions d'informations appartient à chaque entreprise participante. Afin d'éviter que les entreprises participantes prennent du retard dans la mise en place des mentions, ou n'utilisent pas les mentions adéquates, les mesures suivantes sont prévues: OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	Oui	OCCULTATION	OCCULTATION.	Validé
Risque de non-conformité de certaines procédures d'obtention du consentement	OCCULTATION	Le consentement est exigé pour le dépôt d'un cookie/traceur permettant de suivre la personne en vue de la profiler et de lui adresser des publicités ciblées. Tel est le cas du tag commun utilisé par l'alliance. Les entreprises doivent respecter la réglementation e-privacy et se conformer aux recommandations de la CNIL : - Mise en place d'un outil simple de gestion des consentement (CMP), - Mise en place d'une information décrivant le tag au sein de la CMP et de la politique "cookies" figurant sur le site internet des entreprises, - Le cookie ne doit pas se déposer tant que l'internaute n'a pas donné son consentement (en cliquant sur "J'accepte"). - Mention des partenaires utilisant des cookies sur le site et liste de ces partenaires accessible via un lien cliquable.	OCCULTATION	OCCULTATION	OCCULTATION	Oui	OCCULTATION	OCCULTATION	Validé

Risque d'une mauvaise remontée des préférences du client consommateur	OCCULTATION	OCCULTATION * Possibilité pour la personne de s'opposer aux traitements Valiuz sur le site Valiuz	OCCULTATION	OCCULTATION	OCCULTATION	Oui	OCCULTATION	OCCULTATION	Validé	
Accès illégitime	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	Validé	
Modification non désirée	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	Validé	
Disparition de données	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	OCCULTATION	Validé	

Plan d'action		
Risques	**Plan d’actions 2023**	**Staut 2023**
OCCULTATION	**OCCULTATION**	En cours
OCCULTATION	**OCCULTATION**	En cours

Cycle de vie des données

OCCULTATION