

# MICROSOFT

Livre blanc sur le cloud informatique  
et les autorités



## Clause de non-responsabilité

Le présent document contient une présentation générale des questions que nos clients posent souvent lorsqu'ils utilisent des solutions d'informatique en cloud. Il convient donc de leur donner les moyens de mieux comprendre le contexte technique et juridique en cas d'utilisation d'une solution d'informatique en cloud. Le présent document ne contient aucun examen au cas par cas de relations juridiques individuelles. Pour une évaluation juridique individuelle et définitive de la recevabilité de l'utilisation de solutions d'informatique en cloud Microsoft dans un cas d'application concret, vous devez par conséquent recourir à un conseil juridique séparé.

© (2022) Microsoft Corporation. Tous droits réservés. Microsoft, Windows et d'autres noms de produits sont ou peuvent être des marques commerciales déposées et/ou des marques commerciales aux Etats-Unis et/ou dans d'autres pays.

Les informations données figurent uniquement à titre informatif et à des fins de discussions et représentent le point de vue actuel de Microsoft Corporation ou de toute société affiliée au Groupe Microsoft à la date de cette présentation. Vu que Microsoft doit réagir aux conditions de marché en constante évolution, ces informations ne doivent pas être considérées comme une offre contraignante ou un engagement ou une acceptation de garanties, responsabilités, abus, etc. de la part de Microsoft, et Microsoft ne peut garantir l'exactitude des informations fournies après la date du présent document.

# Sommaire

<b>I. LE CLOUD INFORMATIQUE ET LES AUTORITÉS EN SUISSE.....</b>	<b>5</b>
A. INTRODUCTION .....	5
B. L'INFORMATIQUE EN CLOUD COMME OPPORTUNITÉ POUR LA NUMÉRISATION .....	6
a. Renforcement de la sécurité .....	6
b. Amélioration de la conformité .....	6
c. Renforcement de la fiabilité et de la résilience .....	6
C. DÉFIS À RELEVER .....	6
1. Le contrôle des données comme thème principal.....	7
2. Le modèle de responsabilité partagée.....	7
3. Exercice du contrôle dans le cloud.....	8
<b>II. DÉFIS JURIDIQUES.....</b>	<b>9</b>
A. VUE D'ENSEMBLE .....	9
1. Introduction .....	9
2. L'informatique en cloud comme état de fait de sous-traitance propre.....	9
3. Étranger .....	9
B. RÉGLEMENTATIONS EN MATIÈRE DE PROTECTION DES DONNÉES AUX NIVEAUX FÉDÉRAL ET CANTONAL .....	9
1. Généralités.....	9
2. Traitement de données par un tiers en sous-traitance .....	9
3. Les exigences les plus courantes de façon détaillée .....	10
a. Accord contractuel.....	10
b. Traitement selon des instructions et dans l'intérêt de l'organisme public .....	10
c. Recours à des sous-traitants ultérieurs.....	10
d. Sécurité des données .....	11
e. Traitements à l'étranger .....	12
4. Prescriptions concernant le maintien du secret.....	13
5. Données critiques.....	13

<b>III. QUESTIONS ET RÉPONSES FRÉQUENTES.....</b>	<b>14</b>
1. Maîtrise des données; existe-t-il une définition claire et un accord concernant la maîtrise de ses données par le client? .....	14
2. Emplacement des données; le lieu où sont stockées les données des clients et où se trouvent les centres de données est-il clair à tout moment? .....	14
3. Comment les modifications de la documentation relative à la sécurité, à la protection des données et à la conformité, des listes de sous-traitants, des conditions générales, etc. sont-elles gérées?.....	18
4. Le client a-t-il la possibilité de réaliser lui-même des contrôles ou de les faire réaliser par un organe de contrôle indépendant, accrédité et choisi par le client? .....	18
5. Comment les journaux d'audit sont-ils sécurisés? – De quelle manière et à quelle fréquence sont-ils contrôlés pour la protection contre des événements non découverts en termes de sécurité?.....	18
6. Microsoft s'engage-t-elle explicitement à respecter les lois et règlements en matière de protection des données? .....	18
7. La convention sur le traitement des données respecte-t-elle les exigences minimales légales? .....	18
8. Microsoft peut-elle soutenir la «stratégie de sortie» d'un client? – Comment? .....	18
9. Existe-t-il de la documentation sur la méthode d'exploitation, de sécurisation et de maintenance des services en ligne? .....	19
10. Dans quelle mesure les normes internationales en matière de sécurité et de protection des données sont-elles prises en charge? .....	19
11. Comment est assurée la résilience géographique? .....	20
12. Comment est gérée la conservation des données? .....	20
13. Des tests de pénétration, aussi bien pour les réseaux que pour les applications, sont-ils réalisés? .....	20
14. Comment la récupération par le client de ses données en cas d'erreurs ou de pertes est-elle assurée? .....	21
15. Dans quelle mesure un chiffrement est-il utilisé pour des données «au repos» et pour des données «en transit»? .....	22
16. Le client a-t-il accès à des technologies de chiffrement supplémentaires, notamment BYOK, etc.? .....	23
a. Bring-Your-Own-Key/Hold-Your-Own-Key (BYOK/HYOK) .....	23
17. Quels contrôles en matière de sécurité et de protection des données effectue Microsoft en ce qui concerne ses propres collaborateurs et les collaborateurs des sous-traitants? .....	24
18. Comment Microsoft contrôle-t-elle la gestion des identités et des accès? .....	24
19. Comment Microsoft gère-t-elle la séparation des données des clients dans un environnement multi-tenant? .....	24
20. Comment sont traitées les demandes d'accès aux données ou de communication de données émises par les autorités? .....	24

21. Des sous-traitants sont-ils engagés? Et si oui, dans quelles conditions et pour quoi faire? .....	27
22. Dans quelle mesure des données sont-elles transférées dans des pays hors de l'UE/EEE? Quels contrôles juridiques, quelles mesures en matière de sécurité et de protection des données sont à la disposition du client pour réaliser une évaluation des risques et documenter des transferts?.....	28
23. Existe-t-il des aides pour l'obtention, la fourniture, la migration et la garantie de la conformité des services en ligne? .....	28
a. Cas d'utilisation par des clients existants.....	28
b. Analyse des coûts des services en cloud (TCO):.....	28
c. Tâches relatives à la conformité.....	28
d. Optimisation de la mise en œuvre des services en cloud .....	29
e. Surveillance et optimisation de la sécurité et de la conformité .....	29
f. Conformité réglementaire.....	29
g. Garantie d'une configuration et d'une implémentation optimales.....	30
h. Guide d'utilisation du cloud .....	30
i. Insider Risk Management .....	31
<b>IV. ANNEXE – RÉGLEMENTATIONS DANS LA CONFÉDÉRATION ET DANS LES CANTONS EN MATIÈRE DE PROTECTION DES DONNÉES .....</b>	<b>32</b>



# I. LE CLOUD INFORMATIQUE ET LES AUTORITÉS EN SUISSE

## A. INTRODUCTION

Le thème de l'utilisation de l'informatique en cloud par des autorités est **d'une grande actualité**: en décembre 2020, le Conseil fédéral (gouvernement) a d'une part adopté la stratégie d'informatique en cloud de l'administration fédérale et a d'autre part pris connaissance d'un rapport sur l'évaluation des besoins d'un cloud informatique suisse («Swiss Cloud»).

La **stratégie d'informatique en cloud de l'administration fédérale** prévoit, sous l'intitulé «Cloud vision» (vision de l'informatique en cloud), que l'administration fédérale dispose de la capacité complète de mettre à disposition des services informatiques pour l'administration fédérale à l'horizon 2025 en combinant des cloud privés de ses propres fournisseurs de prestations avec des cloud publics. Le cloud public est traité explicitement comme nouvelle option stratégique en matière d'approvisionnement informatique (Stratégie d'informatique en cloud 2020, page 7 et suiv.). La stratégie d'informatique en cloud est énoncée sous forme d'un principe (Principe D-1: Introduction progressive du traitement des données dans les cloud publics) selon lequel même si le cadre juridique offre une plus grande latitude, il convient dans un premier temps de traiter au maximum des informations classées internes dans un cloud public. Les informations d'une classe supérieure ou les données à caractère personnel particulièrement sensibles sont soumises à des exigences plus strictes (Stratégie d'informatique en cloud, page 13). Dans les dernières pages de la stratégie d'informatique en cloud de l'administration fédérale figure une **feuille de route avec des jalons**. Citons notamment le jalon «Contrats-cadres pour les cloud publics» prévu pour le troisième trimestre 2021 et la mise à jour de la stratégie d'informatique en cloud fin 2021. Au premier trimestre 2022, l'administration fédérale doit alors être en mesure d'utiliser de manière ordonnée, sûre et efficace les services informatiques provenant du cloud

public en respectant les principes en matière d'informatique en cloud. Même si la stratégie d'informatique en cloud se focalise sur l'administration fédérale, il faut partir du principe selon lequel de nombreux cantons observent l'évolution de la situation au niveau fédéral et prennent une direction similaire.

A la différence de la stratégie d'informatique en cloud de l'administration fédérale, le **rapport sur l'évaluation des besoins d'un cloud informatique en Suisse («Swiss Cloud»)**, basé sur un sondage, intègre explicitement les cantons (voir Résumé de gestion à la page 4 du [rapport](#)). La conclusion principale du rapport indique qu'un «Swiss Cloud» sous forme d'infrastructure de droit public n'est pas nécessaire (Rapport sur l'évaluation des besoins d'un cloud informatique suisse, page 28). En revanche, cela exige un «Swiss Cloud» en tant que label sous forme de conditions-cadres et de lignes directrices appropriées pour une utilisation compétente et sécurisée des services en cloud existe. Le rapport présente ensuite une vue d'ensemble des **obstacles à l'utilisation de l'informatique en cloud** (Rapport sur l'évaluation des besoins d'un cloud informatique suisse, page 19). Dans des entretiens, les thèmes qui limitent les organisations dans leur utilisation de l'informatique en cloud sont cités: les bases légales d'une utilisation de services en cloud ne sont pas clairement comprises; de nombreuses fonctions distinctes doivent être impliquées au sein de l'organisation; la protection des données et les organes qui en sont chargés empêchent parfois l'innovation. Globalement, les obstacles seraient vraisemblablement dus à deux domaines: d'une part à l'insuffisance des conditions-cadres et des connaissances au sein de l'organisation pour pouvoir utiliser des services en cloud et d'autre part au manque de clarté pour utiliser des services en cloud en toute sécurité et de manière juridiquement appropriée.

Alors que les incertitudes diffuses pour de nombreuses autorités cantonales et communales semblaient conduire à une certaine réserve et à une position attentiste, certaines autorités, après un examen détaillé des conditions juridiques, des possibilités techniques et des dispositifs de sécurité, ont déjà franchi le **pas dans l'informatique en cloud**. Par exemple, le canton de Bâle-Ville<sup>1</sup>, l'Assurance immobilière Berne<sup>2</sup> ainsi que la ville de Zoug<sup>3</sup>, l'hôpital cantonal de Baden<sup>4</sup> ou les communes de Mumpf dans le canton d'Argovie et de Bülach dans le canton de Zurich utilisent déjà les services en cloud de Microsoft (voir à ce sujet l'article «[Joyeux anniversaire: un an Microsoft Cloud en Suisse, pour la Suisse](#)» et «[La stratégie numérique/TIC pour la ville de Bülach](#)»). Et ce, bien que les lois sur la protection des données dans les cantons respectifs ne soient pas moins strictes que dans les autres (voir à ce sujet l'aperçu des actes législatifs sur la protection des données de la Confédération et des cantons en annexe).

Le présent livre blanc a pour objectif de contribuer à pallier aux connaissances lacunaires et aux ambiguïtés juridiques, l'accent étant mis sur l'utilisation de l'informatique en cloud par les autorités des cantons et des communes.

1 <https://news.microsoft.com/de-ch/2020/06/10/additional-azure-services-and-power-bi-available-from-swiss-data-centers/>

2 <https://news.microsoft.com/de-ch/2021/05/25/assurance-immobiliere-berne-et-ses-filiales-misent-sur-le-microsoft-cloud-en-suisse/>

3 <https://customers.microsoft.com/en-us/story/1363955807430340962-stadtzug-novacpta-teams>

4 <https://news.microsoft.com/de-ch/2021/05/18/le-kantonsspital-baden-et-heypatient-sa-developpent-conjointement-un-assistant-de-sante-base-sur-le-cloud/>

## B. L'INFORMATIQUE EN CLOUD COMME OPPORTUNITÉ POUR LA NUMÉRISATION

Les avantages pour les autorités sont évidents: Les solutions d'informatique en cloud peuvent contribuer à la mise en œuvre d'initiatives en matière de numérisation aux niveaux communal, cantonal et national et la puissance d'innovation peut ainsi être renforcée.

Les solutions d'informatique en cloud peuvent permettre aux autorités d'augmenter leur efficacité et de mettre à la disposition du public des offres de services modernes. Le passage à une solution d'informatique en cloud offre également aux autorités et aux collectivités de plus petite taille aux niveaux cantonal et communal des possibilités d'améliorer la sécurité et la conformité:

### a. Renforcement de la sécurité

Les économies d'échelle importantes avec lesquelles Microsoft travaille offrent la possibilité d'intégrer rapidement des mesures de sécurité de premier ordre dans les solutions d'informatique en cloud. Il n'est pas étonnant que de nombreux gros clients de l'administration au niveau international trouvent des possibilités, en utilisant des solutions de sécurité Microsoft, de réduire le risque global pour leurs processus et services, en particulier lorsqu'ils procèdent à une comparaison 1:1 avec leur environnement informatique local existant (dont la sécurité n'est pas toujours optimale). On constate de plus en plus que la sécurité devient un argument puissant pour une analyse de rentabilisation de l'informatique en cloud et non le problème.

### b. Amélioration de la conformité

Les coûts des collectivités pour respecter les prescriptions ont nettement augmenté ces dernières années en raison de la publication de plusieurs nouvelles prescriptions aux niveaux national et cantonal. Ces prescriptions définissent des exigences strictes qu'il n'est pas toujours facile de respecter et de nombreuses autorités luttent pour combler les lacunes que présentent leurs environnements informatiques locaux. Les services en cloud de Microsoft offrent une vaste palette de fonctions de conformité intégrées, qui permettent aux autorités, en passant au cloud informatique, d'augmenter de manière structurelle leur niveau global de conformité tout en économisant aussi les coûts sans cesse croissants des investissements dans des mesures de conformité sur site.

### c. Renforcement de la fiabilité et de la résilience

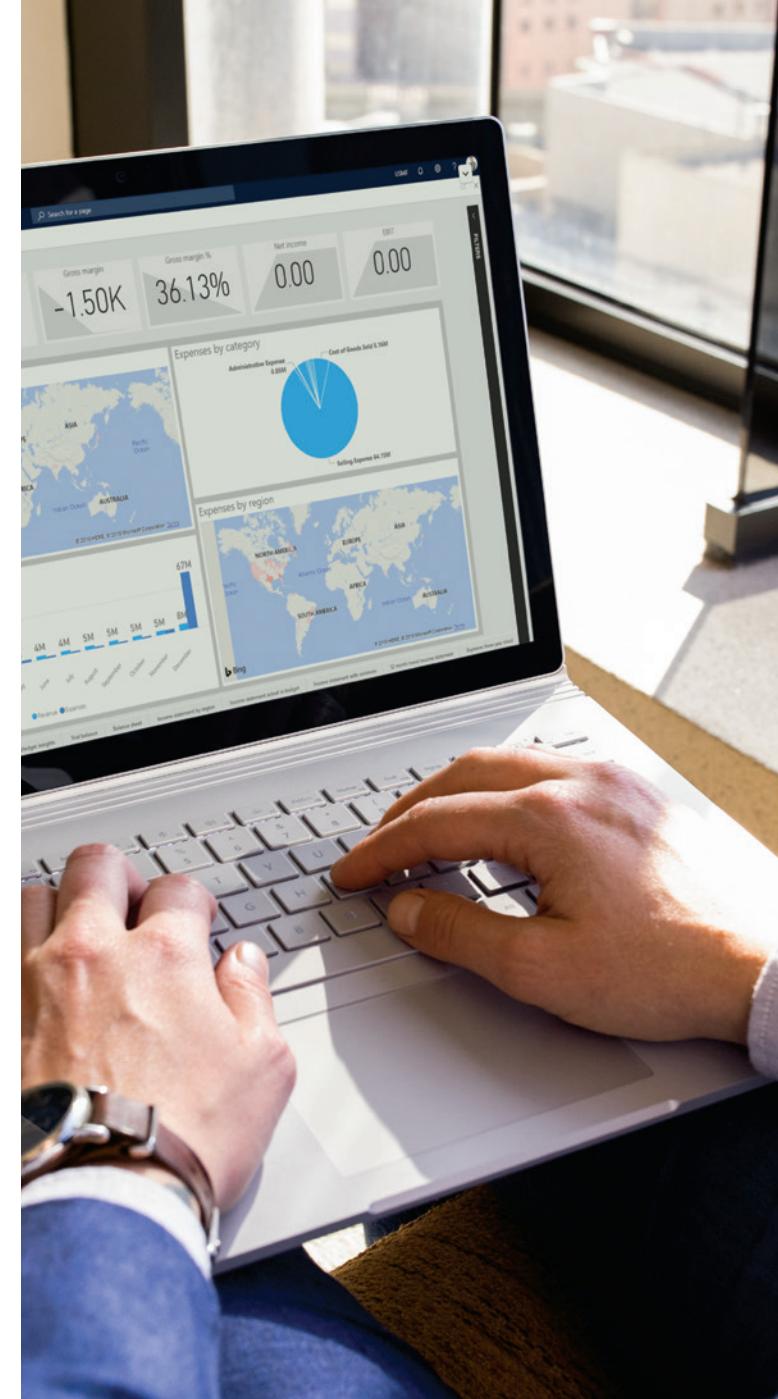
Les solutions d'informatique en cloud sont souvent basées sur la technologie la plus récente combinée avec un degré élevé d'automatisation de service. Il en résulte que des prestataires de services en cloud proposent typiquement un très haut niveau de disponibilité de service dans plusieurs zones de disponibilité à l'échelle mondiale. Le fait d'utiliser ces technologies d'informatique en cloud permet de rendre les services plus tolérants aux pannes et plus résistants aux défaillances.

### C. Défis à relever

L'utilisation de solutions d'informatique en cloud est maintenant très répandue et, avec le nombre croissant d'offres facilement accessibles, elle est de plus en plus approuvée également par les autorités. Les avantages sont évidents, mais les autorités doivent aussi tenir compte des défis à relever: les données sont détenues par le prestataire de services en cloud, éventuellement à l'étranger, mais restent sous le contrôle des autorités. On parle alors de traitement des données «sous-traité» au prestataire de services en cloud. Afin d'assurer le contrôle sur le traitement sous-traité des données, l'autorité doit se pencher sur les conditions en place chez le prestataire de services en cloud, notamment eu égard à la sécurité des informations.

Le point de départ du présent livre blanc est donc en particulier la question de savoir comment Microsoft, en tant que prestataire de services en cloud, gère les défis qui se posent lorsque des clients de l'administration aux niveaux cantonal et communal décident d'utiliser des services en ligne Microsoft.

Le contenu est basé sur des expériences qui ont été recueillies lors de nombreux entretiens avec des autorités cantonales et communales en Suisse. Par ailleurs, les informations sont en grande partie pertinentes pour des organisations privées, mais elles ont été spécialement adaptées aux besoins du secteur public.



## 1. Le contrôle des données comme thème principal

Les solutions d'informatique en cloud visent à ce que les données, au lieu d'être traitées dans des ordinateurs ou des serveurs locaux propres le soient dans les infrastructures correspondantes de prestataires tiers spécialisés comme, par exemple, Microsoft. En général, un tel traitement des données par un tiers est juridiquement autorisé à condition qu'en plus du respect des exigences en matière de conformité au cas par cas il soit notamment garanti que le responsable des données «garde le contrôle».

Dans ce contexte, le contrôle signifie d'une part que la prise de mesures techniques, organisationnelles et contractuelles permet de garantir que seules des personnes habilitées ont accès aux données et que les obligations substantielles en matière de protection des données (mesures de sécurité, obligations de déclaration, respect des principes de traitement, etc.) sont respectées. D'autre part, il convient de garantir que les tiers ayant des droits d'accès n'exploitent pas les données sans y être autorisés et qu'ils les suppriment de manière définitive sur demande du responsable des données. En cas de solutions d'informatique en cloud, l'exigence de contrôle comprend notamment l'exigence que la sous-traitance correspondante puisse être, si nécessaire, restituée ou transférée avec des efforts matériels et dans un temps raisonnables vers l'infrastructure initiale ou vers une autre infrastructure.

Les exigences à remplir dépendent des circonstances et de la nature des données. Par exemple, les exigences sont élevées si les données sont transmises non cryptées au prestataire tiers ou si leur exploitation par un tiers non autorisé pourrait affecter sensiblement les personnes concernées (p. ex. données relevant du secret professionnel).

L'exigence de «contrôle» n'est pas explicitement stipulée dans une loi ou une disposition légale de niveau supérieur. De façon implicite, tous les actes législatifs pertinents aux niveau fédral et cantonal en matière de droit de l'information visent à organiser les exigences de contrôle de l'information. Le contrôle comme obligation est donc en quelque sorte le «distillat» abstrait qui reste lorsqu'on réduit les normes juridiques pertinentes à l'essentiel.

Par ailleurs, les instruments permettant d'exercer et de garantir le contrôle des données sont généralement identiques pour les solutions d'informatique en cloud et les infrastructures informatiques locales, à savoir **des mesures techniques, organisationnelles et contractuelles**.

## 2. Le modèle de responsabilité partagée

La manifestation et l'organisation du contrôle ou le «mix» et l'interaction des différents instruments pour l'exercice du contrôle varient en fonction du niveau d'intégration des solutions d'informatique en cloud impliquées. Cela se reflète également dans la répartition de la responsabilité et des coûts pour l'établissement d'une protection appropriée contre certains risques (notamment la protection et la sécurité des données).

Dans un environnement informatique en cloud, contrairement à une infrastructure informatique locale, la responsabilité de la mise en œuvre et de la gestion des contrôles de sécurité pour les applications informatiques est partagée entre le client et le prestataire de services en cloud. Cela ressemble à un scénario de sous-traitance classique. Cependant, la responsabilité ultime des données traitées incombe toujours au client.

En principe, les solutions d'informatique en cloud suivent un modèle de responsabilité partagée («shared responsibility model»). Cela répartit la responsabilité entre le client et le prestataire de services en cloud le long des limites de la virtualisation; de sorte qu'une seule partie est responsable d'un aspect particulier.



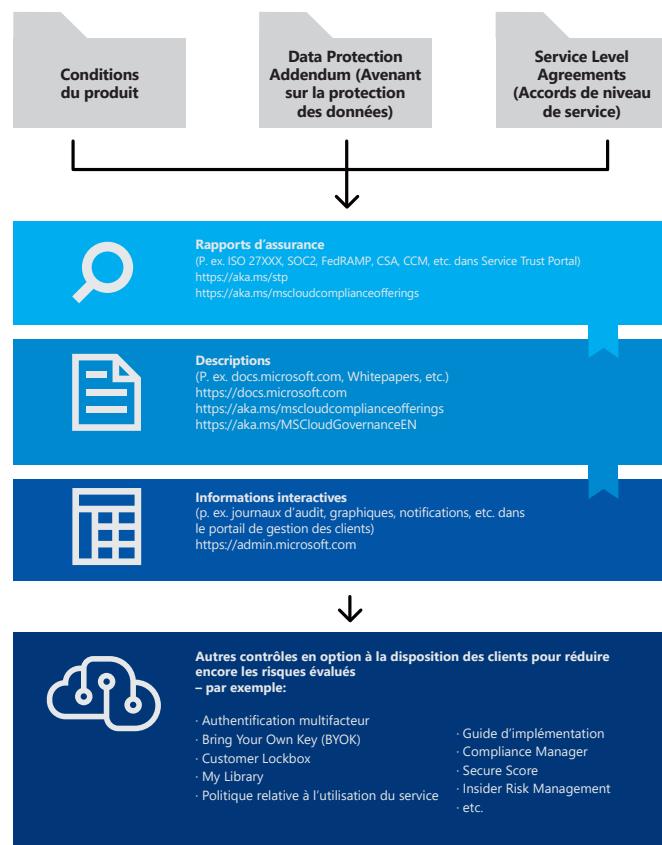
A risk assessment is not limited to the Cloud Provider, but focuses on the end-to-end process or service.



Et corrélativement, avec les solutions d'informatique en cloud, un certain déplacement de la fonction de contrôle a lieu, de sorte que les aspects organisationnels ou opérationnels du contrôle prennent plus d'importance. Si, par exemple, une autorité dans un environnement informatique en cloud n'a elle-même que de manière limitée la possibilité de mettre en œuvre des mesures techniques contre l'accès non autorisé aux données (parce que le prestataire de services en cloud fournit la technique correspondante), l'autorité doit assumer sa responsabilité en prenant d'autres mesures adaptées. Outre une évaluation minutieuse du prestataire de services en cloud, un suivi régulier de l'efficacité de la protection des données fournie par le prestataire pourrait être, par exemple, une mesure appropriée pour garantir le contrôle (p. ex. surveillance permanente des accès et tentatives d'accès par l'analyse correspondante des journaux d'événements).

### 3. Exercice du contrôle dans le cloud

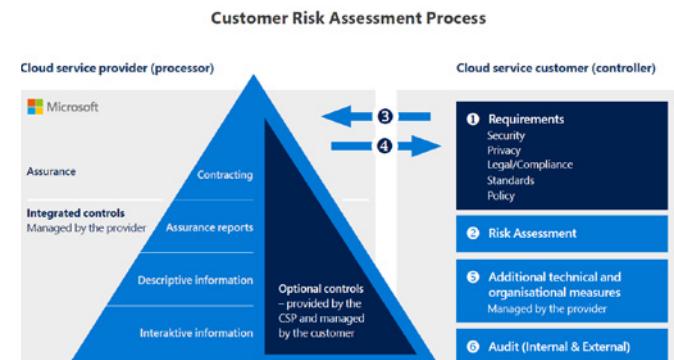
Pour avoir la compréhension nécessaire et le discernement qui constituent le point de départ de la preuve du contrôle, il est indispensable de connaître la structure d'ensemble des accords portant sur les services en cloud Microsoft, de la documentation, des instructions et en particulier des certifications et des rapports d'audit. Le «Microsoft Assurance Framework» donne à cet égard la vue d'ensemble nécessaire et un guide sur le processus de contrôle à suivre:



1. le niveau le plus haut est le **dispositif contractuel à conclure avec Microsoft**. Cela comprend entre autres les **Universal Licence Terms (conditions universelles de licence)**, dans lesquels se trouve l'accord sur le traitement des données (désigné pour l'informatique en cloud Microsoft **Data Protection Addendum**) (l'avenant sur la protection des données).
2. Les obligations contractuelles définies dans le dispositif contractuel de Microsoft peuvent être contrôlées à l'aide des documents du deuxième niveau, appelés les «Assurance Reports» (rapports d'assurance). Les clients ont accès à l'ensemble des **rapports d'audit de prestataires tiers, des certificats sur le respect des normes, SOA** etc.
3. Le troisième niveau comprend des documentations descriptives complémentaires, dans lesquelles Microsoft met à disposition des **instructions et descriptions** de certaines fonctions, caractéristiques, processus, etc. On y trouve également une série de **livres blancs** spécifiques à des thèmes ou à des secteurs, comme le présent document.
4. Enfin, les clients ont accès à des informations et des documentations en continu, notamment sur l'utilisation des services en cloud de Microsoft, qui sont à disposition via un **portail de gestion des services en cloud** individuel.

Pour ces quatre niveaux de rapports d'assurance «Assurance Reports», des fonctions, des services et des processus complémentaires peuvent être mis en œuvre pour les clients individuels. Ils peuvent être utilisés sur la base de l'évaluation générale des risques de la solution et des flux de données et peuvent par conséquent être intégrés dans un plan d'atténuation en rapport avec les risques identifiés que le client souhaite réduire. Dans l'illustration ci-dessus, quelques-unes des mesures les plus fréquentes sont représentées dans l'encadré à droite et seront décrites plus loin dans le présent document.

Le «Assurance Framework» Microsoft joue par conséquent un rôle décisif dans le cadre de la réalisation du contrôle chez le client. Le contexte est présenté dans le modèle de processus ci-après:



## II. DÉFIS JURIDIQUES

### A. VUE D'ENSEMBLE

#### 1. Introduction

Bien que le principe du «Cloud first» se trouve déjà dans une «Stratégie d'informatique en cloud des autorités suisses» adoptée il y a bientôt dix ans, on sent aujourd'hui encore du côté des autorités une certaine réserve, due en particulier aux incertitudes qui existent quant à la gestion de solutions d'informatique en cloud. Dans la Stratégie d'informatique en cloud 2020, huit ans après la décision en faveur du principe «Cloud first», il est tout de même encore (ou déjà) question d'un **changement de paradigme vers le «Cloud first»** (Stratégie d'informatique en cloud 2020, page 28).

Les **incertitudes** sont observées chez les autorités à tous les niveaux fédéraux, à savoir les autorités fédérales, cantonales et communales. Alors que pour les autorités fédérales, la loi sur la protection des données et d'autres actes législatifs au niveau fédéral sont au premier plan, des autorités cantonales et communales doivent s'en tenir à la loi sur la protection des données et, le cas échéant, à d'autres actes législatifs du canton concerné. Ce qui s'applique à tous les niveaux aux membres d'autorités, c'est le secret professionnel et la responsabilité pénale des membres d'autorités en cas de violation de ce secret.

Au niveau cantonal, il existe par ailleurs précisément de nombreuses notes explicatives des autorités cantonales chargées de la protection des données et de la conférence des préposé-e-s suisses à la protection des données, qui contiennent diverses recommandations en matière d'action, mais qui ne sont que des recommandations.

#### 2. L'informatique en cloud comme état de fait de sous-traitance propre

Dans le cadre de solutions d'informatique en cloud, des données, au lieu d'être traitées dans des ordinateurs ou des serveurs locaux propres, le sont dans des infrastructures informatiques correspondantes de prestataires tiers et elles sont gérées par du personnel externe. Il y a donc ce qu'on appelle un «état de fait de sous-traitance» au sens de la plupart des législations cantonales en matière de protection des données.

Toutefois, les solutions d'informatique en cloud doivent être distinguées des solutions de sous-traitance «outsourcing» classiques, qui sont également considérées comme un état de fait de sous-traitance d'après les dispositions cantonales en vigueur en matière de protection des données. On entend généralement par sous-traitance classique le cas d'un prestataire de services qui, conformément aux instructions spécifiques du client, gère des processus d'entreprise à sa place et, dans ce contexte, a accès à des données et les consulte et/ou crée, traite ou modifie même le contenu des informations stockées dans les données des autorités. En revanche, le client, dans un modèle d'informatique en cloud, reçoit en principe une **prestation standardisée**. L'**individualité ou l'absence d'individualité** de la relation de prestation (niveau technique et organisationnel) est par conséquent un critère de délimitation essentiel entre l'informatique en cloud et la sous-traitance classique. Le passage d'une forme à l'autre est cependant courant; les réglementations en matière de sous-traitance peuvent par conséquent aussi être applicables au cas des constellations d'informatique en cloud. Toutefois, il convient de vérifier précisément en détail si cela est également objectivement justifié.

Généralement, la fourniture de prestations de services informatiques n'est pas une tâche de souveraineté véritable, même si dans certains cas les données elles-mêmes, qui sont traitées et stockées par des tiers lors des services informatiques, effectuent l'exécution de tâches souveraines. La sous-traitance de services informatiques est en principe autorisée par le droit administratif.

#### 3. Étranger

Si, dans le cadre de solutions d'informatique en cloud, des données personnelles sont traitées dans des pays qui présentent un niveau de protection des données inférieur à celui de la Suisse ou de l'UE ou de l'EEE (on parle d'**absence d'équivalence** dans des «pays étrangers peu sûrs»), l'admissibilité du traitement de données correspondant dépend, au-delà de l'exigence générale de contrôle, du respect des conditions supplémentaires (p. ex. existence de mesures contractuelles de protection).

### B. Réglementations en matière de protection des données aux niveaux fédéral et cantonal

#### 1. Généralités

Vu que la Confédération n'a pas la compétence législative totale de légiférer dans le domaine de la protection des données, les cantons sont habilités, en raison de leur droit à une organisation propre, à réglementer de manière indépendante la protection des données dans la mesure où il s'agit du traitement de données personnelles par les autorités cantonales, les communes et les services de l'administration. Cependant, ils sont tenus de respecter les dispositions du droit fédéral, notamment le droit à la protection contre l'utilisation abusive des données personnelles (art. 13, al. 2 Cst.) et le droit international.

Tous les cantons disposent d'actes législatifs sur la protection des données en général. Ceux-ci précisent le droit fondamental à la protection de la vie privée et les principes de l'Etat de droit pour le traitement de données personnelles au niveau cantonal, en définissant les conditions et les principes généraux du traitement de données par les autorités cantonales et communales ainsi que les droits des personnes concernées. Lorsque des organismes publics cantonaux sont mis en concurrence avec l'économie privée, cette activité ne relève pas de l'exercice de fonctions relevant de la puissance publique ou de l'exercice de tâches publiques du droit cantonal (comme dans le cas des banques cantonales).

Les dispositions essentielles des actes législatifs des cantons et de la Confédération sur la protection des données sont résumées dans l'aperçu en annexe.

#### 2. Traitement de données par un tiers en sous-traitance

La plupart des lois cantonales sur la protection des données contiennent des dispositions particulières pour le traitement de données en sous-traitance. Tel est le cas lorsque l'organisme public responsable charge un tiers de l'exécution du processus de traitement des données.

Dans certains cantons, il existe des prescriptions spécifiques sur les conditions d'une sous-traitance des processus de traitement des données à un tiers (p. ex. l'accord dans un contrat écrit, des règles spécifiques sur le recours à des sous-traitants ultérieurs, etc.). Toutefois, la plupart des cantons ne fixent pas de règles particulières à ce sujet.

De manière générale, on peut dire que le traitement de données en sous-traitance est en principe autorisé si aucune obligation légale ou contractuelle de confidentialité ne s'y oppose et si le respect des prescriptions légales sur la protection des données est garanti. Dans cette mesure, le principe de base dans les lois cantonales sur la protection des données est comparable à la situation juridique du domaine privé (selon la loi fédérale sur la protection des données).

En principe, l'organisme public qui donne le mandat reste responsable du respect de la protection des données. Il doit prendre des mesures appropriées pour garantir un niveau de protection des données adéquat. Ce principe de base correspond aussi à cet égard aux règles de base de la loi fédérale sur la protection des données.

### 3. Les exigences les plus courantes de façon détaillée

#### a. Accord contractuel

Avec tout tiers qui prend en charge des processus de traitement de données en sous-traitance pour une autorité (p. ex. Microsoft), un accord de sous-traitance, qui réglemente les garanties eu égard au respect de la protection et de la sécurité des données ainsi que l'utilisation des services en cloud dans un secteur de droit public, doit être signé.

Selon les cantons, il existe des réglementations légales qui précisent des exigences concernant le contenu du contrat avec le sous-traitant. Dans certains cantons, il existe aussi des conditions générales devant être convenues comme faisant partie intégrante des contrats de sous-traitance de services informatiques ou de traitement de données personnelles.<sup>5</sup>

Il est possible en principe de déroger à ces exigences dans l'intérêt de trouver une solution adaptée, notamment si la situation juridique ne révèle aucun motif impérieux de mettre en œuvre ces conditions générales telles quelles ou, s'il résulte d'un contrôle que les exigences de dispositions contractuelles suffisantes en matière de protection et de sécurité des données sont remplies sur la base des dispositifs contractuels du prestataire.

En fonction de la nature d'un cloud informatique avec des offres standardisées pour tous les clients, Microsoft utilise des contrats types pour l'utilisation de l'infrastructure informatique en cloud. La prise en considération d'exigences individuelles dans une plus large mesure est en principe impossible dans l'infrastructure informatique hautement standardisée donnée.

Les conditions standardisées peuvent être considérées par les autorités comme un obstacle à l'introduction de solutions d'informatique en cloud. Microsoft répond à ce défi en proposant des modifications spécifiques du contrat qui répondent aux besoins individuels des autorités cantonales et communales. N'hésitez pas à contacter votre interlocuteur Microsoft ou votre partenaire Microsoft, qui se fera un plaisir de vous aider.

#### b. Traitement selon des instructions et dans l'intérêt de l'organisme public

Le sous-traitant doit procéder au traitement des données uniquement selon les instructions et dans l'intérêt de l'organisme public. Différentes législations cantonales contiennent à ce sujet des dispositions (s'appuyant sur l'art. 10a, al. 1, let. a LPD) selon lesquelles les données peuvent être traitées uniquement dans la mesure dans laquelle l'organisme public est autorisé à le faire.

Les dispositions de Microsoft<sup>6</sup> relatives à la protection des données le stipulent. Microsoft en tant que sous-traitant de données traitera les données du client (et notamment les données personnelles) uniquement de la manière décrite et sous réserve des limitations prévues dans les dispositions relatives à la protection des données, (a) pour fournir au client les produits et services conformément aux instructions documentées du client, et (b) pour les opérations commerciales de Microsoft qui sont liées à la fourniture des produits et services au client. Le dispositif contractuel du client avec la documentation des produits et l'utilisation et la configuration des fonctionnalités des services en ligne représentent à cet égard l'ensemble des instructions complètes et documentées du client vis-à-vis de Microsoft concernant le traitement de données à caractère personnel.

Les données des clients ne sont en particulier pas utilisées à des fins publicitaires, d'études de marché ou de profilage des utilisateurs.

#### c. Recours à des sous-traitants ultérieurs

Le recours à des sous-traitants ultérieurs par le prestataire de services en cloud est en principe autorisé conformément aux prescriptions nationales et cantonales en vigueur dans la mesure où le respect des obligations du prestataire de services en cloud découlant du contrat de traitement est garanti également en cas de sous-traitance ultérieure. Selon le nouveau droit national sur la protection des données (art. 9, al. 3 LPD (version révisée)), les prestataires de services en cloud ont l'obligation légale d'informer les clients du recours à de nouveaux sous-traitants ou du remplacement de sous-traitants existants en tant que sous-traitants ultérieurs et de leur permettre de s'opposer à ce recours, ce qui peut également être obtenu par l'octroi d'un droit de résiliation.

5 Par exemple canton de Berne (Conditions générales sur la sécurité des informations et la protection des données lors de la fourniture de prestations informatiques); canton de Zurich (Conditions générales sur la sous-traitance de processus de traitement de données en recourant à des prestations informatiques)

6 Avenant sur la protection des données pour les services et produits Microsoft: <https://aka.ms/dpa>

Dans les dispositions sur la protection des données de Microsoft<sup>7</sup>, le paragraphe «Notifications et contrôles sur le recours à des sous-traitants ultérieurs» explique comment Microsoft gère les sous-traitants ultérieurs et informe les clients des modifications apportées au portefeuille des sous-traitants ultérieurs, etc. Le présent document décrit les exigences posées par Microsoft à ses sous-traitants ultérieurs et indique que Microsoft assume la responsabilité de faire respecter par le sous-traitant ultérieur toutes les exigences contenues dans les dispositions en matière de protection des données.

Le Service Trust Center<sup>8</sup> tient la liste à jour, incluant les services fournis, le lieu de leur siège social et la limite et les conditions dans lesquelles les sous-traitants ultérieurs peuvent avoir accès aux données des clients: <http://aka.ms/mscloudsubprocessors>.

Ni Microsoft ni les sous-traitants ultérieurs n'ont un accès administratif permanent aux données des clients ou à des solutions des clients. Microsoft Cloud fonctionne avec le principe «Zero standing ADMIN», également connu sous le terme «Least Privilege», avec lequel l'accès administratif est contrôlé par une procédure d'authentification (désignée «Lockbox»), p. ex. dans le cas de clients qui chargent Microsoft d'une activité d'assistance, avec octroi au collaborateur auquel est confiée l'assistance en question de priviléges (qui pourraient permettre l'accès à des données du client). L'attribution de l'accès administratif doit s'effectuer par le biais de plusieurs liens, de Time-Boxes et d'un protocole d'audit complet, et peut aussi comprendre, si le client le souhaite, l'approbation définitive du client, par la mise en place d'un processus de «Lockbox» élargi, appelé «Customer Lockbox»<sup>9</sup>.

#### d. Sécurité des données

Les législations cantonales sur la protection des données et la sécurité des informations exigent en général, dans le cadre de la sous-traitance de prestations de services informatiques ou le traitement de données en sous-traitance, la garantie d'une sécurité des données appropriée par le mandataire. La plupart des actes législatifs cantonaux ne définissent aucune mesure de protection concrète, mais énoncent des principes concernant les objectifs à couvrir en matière de protection, **confidentialité, disponibilité et intégrité**. Les risques ci-après doivent notamment être couverts:

- Destruction accidentelle ou non autorisée;
- Perte accidentelle;
- Erreurs techniques;
- Falsification, vol ou utilisation illicite;
- Modification, copie, accès ou autre traitement non autorisé.

Les données personnelles doivent être protégées par des mesures techniques et organisationnelles adaptées contre de tels risques.

Tous les services en ligne de Microsoft reposent sur un environnement virtualisé. La virtualisation et les infrastructures informatiques évolutives ont une conséquence: le niveau physique des unités informatiques est séparé du niveau d'utilisation que le client du cloud voit. Le matériel est installé de manière à ce qu'un accès des instances utilisateur (également appelées «Virtual Machines» (machines virtuelles)) au matériel ne soit pas possible (l'*'isolement'* de la machine virtuelle). Cet isolement assure la sécurité dans la démarcation de l'instance utilisateur et des applications qui y sont exécutées des fonctions centrales du système d'exploitation sur le matériel. Cette architecture entraîne par ailleurs le fait que les utilisateurs ne peuvent pas exécuter à partir des applications des commandes de lecture, d'écriture ou d'exécution dans le système hôte sous-jacent.

Par ailleurs, Microsoft utilise des méthodes afin qu'à partir de l'instance utilisateur d'un client du cloud, on ne puisse pas avoir accès à des zones centrales (notamment la zone de stockage) d'instances utilisateur d'un autre client. Il en résulte que les infrastructures informatiques utilisées dans le cadre de ce qu'on appelle un «public cloud» n'entraînent pas de préjudice au contrôle du client du cloud. Il est capital que dans les réseaux virtuels qui interviennent pour le client du cloud Microsoft, seules des définitions d'accès explicites (utilisées chacune uniquement pour un client du cloud) soient utilisées.

D'autres aspects de la sécurité, qui existent généralement dans un environnement de cloud, augmentent également la protection des données contre l'accès de tiers: les mises à jour des systèmes d'exploitation et des logiciels de plateforme («patching», c.-à-d. la remise d'un code logiciel sur une installation logicielle existante pour améliorer l'installation existante ou éliminer des défauts) ont lieu en général de façon automatisée, c.-à-d. sans que l'intervention de l'humain soit nécessaire. Microsoft a mis en place d'autres mesures de protection, à savoir des mesures de nature organisationnelle (journalisation des accès logiques, processus collaborateurs, etc.)

Dans les services en ligne, Microsoft utilise de nombreux chiffrements à différents niveaux et a publié à ce sujet des livres blancs et des documentations complètes. D'un côté, différents chiffrements sont utilisés pour des données stockées («données au repos») et ce aussi bien dans les environnements d'exploitation («volume level») qu'au niveau des fichiers de données. La protection par chiffrement peut encore être complétée par l'utilisation de clés que l'on gère soi-même, les BYOK («Bring Your Own Key»). Microsoft utilise également des techniques de chiffrement pour le transfert de données («data in-transit»). Les services en ligne offrent par ailleurs divers autres moyens permettant au client du cloud d'utiliser et de gérer lui-même certaines techniques de chiffrement.

7 Avenant sur la protection des données pour les services et produits Microsoft: <https://aka.ms/dpa>

8 <https://servicetrust.microsoft.com>

9 <https://aka.ms/msazurelockbox> et <https://aka.ms/o365CustomerLockbox>

Par le Trust Center<sup>10</sup> Microsoft et par le contrôle des services au Security & Compliance Center<sup>11</sup>, les clients du cloud peuvent consulter directement, à tout moment, des rapports de certification et d'audit, ainsi que d'autres informations complètes sur les sites de conservation des données, les possibilités d'accès aux données du client du cloud, les mesures prises en matière de sécurité et de protection des données (voir ci-dessus chiffre II.C.3). De cette manière, le client du cloud informatique peut être convaincu, à tout moment, que Microsoft s'acquitte de ses obligations en matière de sécurité.

#### e. Traitements à l'étranger

Certaines lois cantonales sur la protection des données posent des exigences particulières pour des projets dans le cadre desquels la sous-traitance de données est prévue à l'étranger. Mais globalement, les règles à ce sujet sont comparables à celles en vigueur selon la loi fédérale sur la protection des données (LPD).

La règle qui s'applique généralement est celle-ci: les sous-traitances dans un pays qui dispose d'un niveau de protection des données équivalent à celui de la Suisse sont autorisées sans autre mesure à prendre. En font partie notamment tous les Etats de l'UE/EEE.

Microsoft utilise habituellement, pour les services en ligne SaaS (logiciel en tant que service) destinés aux les clients suisses du cloud, les centres de données de la Suisse et parfois de l'Europe (avec des centres de données en Irlande, aux Pays-Bas, en Autriche et en Finlande). Les données des clients d'un grand nombre de services sont stockées exclusivement dans ces centres de données. Si d'autres pays viennent intégrer une région, Microsoft en informe le client du cloud un mois à l'avance. Les sites concrets de conservation des données peuvent être consultés pour chaque service en ligne via le contrôle des services correspondants au Security & Compliance Center<sup>12</sup>.

Les exigences en matière de fourniture de services en ligne peuvent, dans certains cas, faire qu'il est nécessaire que certaines données des clients soient rendues accessibles à des collaborateurs ou sous-traitants de Microsoft hors de cette région de stockage primaire. Il peut également arriver que les collaborateurs Microsoft avec la plus grande expérience technique du traitement de problèmes spécifiques à des services se trouvent sur des sites hors de cette région de stockage primaire et qu'ils aient, le cas échéant, besoin de l'accès à des systèmes ou données pour pouvoir résoudre un problème.

Conformément aux dispositions relatives à la protection des données pour les services en ligne, Microsoft peut en principe transférer des données que Microsoft traite au nom du client du cloud informatique, exceptionnellement vers d'autres pays (entre autres aussi vers les Etats-Unis). Microsoft s'engage à toujours respecter les exigences des lois en vigueur en Suisse en matière de protection des données eu égard à la collecte, à l'utilisation, au transfert, à la conservation et à tout traitement autre de données à caractère personnel provenant de la Suisse.

Dans le cas d'un éventuel traitement à l'étranger hors de l'UE/EEE, Microsoft a pris les mesures suivantes: pour toutes les transmissions de données des clients, de données de services professionnels et de données à caractère personnel provenant de l'Union européenne, de l'Espace économique européen, du Royaume-Uni et de la Suisse pour la fourniture de produits et services, les clauses contractuelles types de l'UE mises en œuvre par Microsoft s'appliquent. Microsoft se conforme aux exigences des lois sur la protection des données de l'Espace économique européen et de la Suisse eu égard à la collecte, à l'utilisation, au transfert, au stockage et à tout traitement autre de données à caractère personnel provenant de l'Espace économique européen, du Royaume-Uni et de la Suisse.



10 <https://www.microsoft.com/fr-ch/trust-center>

11 <https://docs.microsoft.com/fr-ch/microsoft-365/compliance/service-assurance?view=o365-worldwide>

12 <https://docs.microsoft.com/fr-ch/microsoft-365/compliance/service-assurance?view=o365-worldwide>

Microsoft ne transmet pas non plus de données des clients à des autorités chargées des poursuites pénales, à moins que la loi ne l'y oblige. Si des autorités chargées des poursuites pénales contactent Microsoft pour demander des données du client, Microsoft essaiera de rediriger celles-ci pour qu'elles demandent ces données directement au client. Si Microsoft est contrainte de divulguer des données à des autorités chargées des poursuites pénales ou de leur en permettre l'accès, Microsoft informera immédiatement le client et lui fournira une copie de la demande, à moins que la loi ne l'interdise. Microsoft suit une approche rigoureuse et fondée sur des principes en matière de gestion des demandes administratives d'accès à des données des clients qui sont détenues par Microsoft.<sup>13</sup> Microsoft publie des «Law Enforcement Request Reports» (rapports de demande d'application de la loi) tous les six mois afin de garantir la transparence sur l'étendue et la nature de ces événements.<sup>14</sup> Il est possible de se procurer les rapports pour s'en inspirer lors de la réalisation de l'évaluation des risques au plan juridique. Microsoft interagit quotidiennement avec des clients et des gouvernements du monde entier et participe ainsi à la création du cadre juridique international pour ces thèmes critiques. Microsoft a publié six principes directeurs de ce travail, qui sont fondés également sur les efforts constants visant à la protection des données des clients de Microsoft et à l'amélioration de la politique de confidentialité.<sup>15</sup> Selon Microsoft, les principes formulés représentent des droits universels et des exigences minimales de base, qui doivent régir l'accès des autorités chargées des poursuites pénales à des données à notre époque moderne. L'application de ces principes peut varier d'un pays à l'autre, mais les principes de base du contrôle et de l'équilibre, de l'obligation de rendre compte et de la transparence doivent subsister.

Microsoft propose également des modifications du contrat adaptées aux besoins individuels des autorités cantonales et communales. N'hésitez pas à contacter votre interlocuteur Microsoft ou votre partenaire Microsoft, qui se fera un plaisir de vous aider.

#### 4. Prescriptions concernant le maintien du secret

Il y a divulgation punissable au sens des dispositions du droit pénal sur le secret de fonction ou le secret professionnel (en particulier art. 320 et art. 321 Code pénal suisse) lorsqu'une personne extérieure a effectivement eu connaissance des informations à protéger (p. ex. des informations relevant du secret de fonction). Cette prise de connaissance effective peut être également désignée «accès au texte brut» dans le contexte numérique. Révéler ou divulguer signifie «rendre accessibles» des informations, c.-à-d. des indications qui «parlent d'elles-mêmes» et qui peuvent être consultées concrètement. En général, ces révélations ou divulgations n'existent pas dans les services en cloud public.

Dans certaines situations exceptionnelles, un accès extrêmement limité, contrôlé et protégé par des mesures organisationnelles, à des données des clients peut être nécessaire pour pouvoir exploiter les services en ligne pour le client, par exemple dans certains cas d'assistance ou en cas d'événements critiques en termes de sécurité.

Les processus d'exploitation qui règlementent l'accès à des données des clients dans les services en ligne Microsoft sont protégés par des mesures techniques et organisationnelles qui comprennent l'authentification forte et des contrôles d'accès aussi bien physiques que logiques. Microsoft vérifie les contrôles d'accès de manière proactive à tous les niveaux des services en ligne. Les services en ligne Microsoft sont conçus de façon à ce que les techniciens de Microsoft soient en mesure de gérer et de mettre en œuvre le service en ligne sans devoir accéder à des données des clients. Les collaborateurs Microsoft n'ont pas d'accès permanent aux données des clients. Lorsque, exceptionnellement, un accès est nécessaire pour l'exploitation du service, des contrôles des accès basés sur les rôles sont utilisés pour garantir que l'accès est autorisé à des fins appropriées, pour un temps limité et sous la surveillance du management.

Nos clients attendent de nous que nous protégeons leur sphère privée et les données qui nous sont confiées et que nous n'utilisons les informations que de la manière prévue. Pour répondre à cette exigence, nous nous engageons par le biais de contrats étendus vis-à-vis de nos clients. Microsoft est consciente du fait que les données des clients peuvent être soumises à des règles spécifiques concernant le secret. C'est la raison pour laquelle Microsoft s'acquitte rigoureusement de ses obligations en matière de confidentialité conformément aux contrats applicables avec les clients.

#### 5. Données critiques

Par rapport à des informations bien déterminées qui, en raison de l'intérêt public, par exemple du fait d'une relation particulière avec la sécurité d'infrastructures critiques de la collectivité, ne doivent pas tomber entre les mains de tiers, il pourrait y avoir une limite explicite et implicite d'utilisation d'un service en cloud. La collectivité serait à cet égard dans l'obligation de limiter ces données au moyen d'un classement adapté des informations qui ne doivent pas être intégrées dans un projet en cloud. Ces aspects doivent être prévus au cas par cas et des mesures appropriées doivent être prises dans ce sens.

13 Le processus est décrit ici de manière détaillée: <https://aka.ms/mslerh>

14 Disponible ici: <https://aka.ms/mslrr>

15 «Six Principles for International Agreements Governing Law Enforcement Access to Data»: <https://aka.ms/MS6dataaccessPrinciples>

## III. QUESTIONS ET RÉPONSES FRÉQUENTES

### 1. Maîtrise des données; existe-t-il une définition claire et un accord concernant la maîtrise de ses données par le client?

Oui. Dans l'**avant sur la protection des données pour les services et produits Microsoft** (anglais **Data Protection Addendum, DPA<sup>16</sup>**), il est écrit à la page 6, sous «Nature du traitement des données; Propriété» ce qui suit:

*«Microsoft utilise et traite de toute autre manière les données client, les données des services professionnels et les données à caractère personnel uniquement de la manière décrite et sous réserve des limitations prévues ci-dessous (a) pour fournir au client les produits et services conformément aux instructions documentées du client, et (b) pour les opérations commerciales liées à la fourniture des produits et services au client. Entre les parties, le client conserve tous les droits, titres et propriété sur les données du client et les données des services professionnels. Microsoft n'acquiert aucun droit sur les données client ou les données des services professionnels à l'exception du droit qui lui est octroyé par le client dans la présente section.»*

Le respect de ces principes est documenté par le biais de l'adoption de la norme internationale «ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud» (Code de pratique ISO/CEI 27018 pour la protection des données personnelles dans le cloud).<sup>17</sup>

Par ailleurs, Microsoft a été l'un des premiers prestataires de services en cloud qui a obtenu la certification ISO/CEI 27701 «**Privacy Information Management System**» (**système de gestion des informations personnelles**).<sup>18</sup>

### 2. Emplacement des données; le lieu où sont stockées les données des clients et où se trouvent les centres de données est-il clair à tout moment?

Le paragraphe «Transfert et emplacement des données» dans le DPA<sup>19</sup>, page 10, le décrit. D'autres obligations contractuelles, et plus spécifiques, sur le lieu d'hébergement des données sont indiquées ici: <https://www.microsoft.com/licensing/terms/fr-FR/product/PrivacyandSecurityTerms/all>

Le client peut configurer son utilisation des services en cloud Azure de façon à ce que les données de la plupart des services soient stockées uniquement en Suisse ou dans l'UE. Actuellement, plus de 60 régions sont proposées au total, parmi lesquelles deux en Suisse et plusieurs au sein de l'UE. Une vue d'ensemble complète des emplacements des centres de données en cloud Microsoft se trouve sur cette carte interactive: <https://azure.microsoft.com/global-infrastructure/geographies/>

La plupart des services en cloud disponibles proposent des emplacements de données au sein de l'UE (et un nombre croissant en Suisse): <https://azure.microsoft.com/fr-fr/global-infrastructure/services/> et pour les services Office 365 ici: <https://aka.ms/mso365datalokation>

Les clients de Microsoft 365 peuvent également contrôler les emplacements des données via leur centre d'administration Microsoft 365 en accédant à Paramètres | paramètres d'organisation | profil d'organisation | emplacement des données.

Certains «services non régionaux» sont proposés, en raison de leur conception et de leur fonction, sans obligation d'un emplacement de données défini. Le service Azure Active Directory (AAD), qui est d'une importance capitale pour de nombreux services en ligne, en fait notamment partie. Pour ce service également, certaines garanties sont données concernant l'emplacement des données, et on peut les trouver ici: <https://aka.ms/msaadddatalocation>. Les clients doivent veiller à la nature des données qui sont stockées dans l'AAD.<sup>20</sup>

Pour certains services en ligne, Microsoft renvoie à certaines sections du Trust Center Microsoft pour obtenir d'autres informations détaillées sur l'emplacement des données. Vu que les services en ligne Microsoft se composent de plusieurs services spécifiques et que de nouveaux (sous-)services peuvent être ajoutés au fil du temps, Microsoft utilise ce mécanisme de renvoi aux pages d'accueil du Trust Center pour obtenir des informations actualisées sur les emplacements effectifs des données. Il est important de prendre en considération le fait que, bien que Microsoft puisse modifier de temps à autre le contenu de ces pages Internet, les conditions des services en ligne en matière de protection et de sécurité des données<sup>21</sup> stipulent explicitement que:

*«(...) Microsoft n'ajoute[ra] pas d'exceptions pour des services existants dans la version générale (...).»*

16 <https://aka.ms/dpa>

17 Voir: <https://aka.ms/msiso27018> et: <https://docs.microsoft.com/fr-ch/compliance/regulatory/offering-ISO-27018?view=o365-worldwide>

18 Voir: <https://docs.microsoft.com/fr-ch/azure/compliance/offeringsoffering-offering-iso-27701>

19 FN 16

20 Voir: <https://docs.microsoft.com/fr-fr/azure/active-directory/hybrid/reference-connect-sync-attributes-synchronized>

21 Voir: <https://www.microsoft.com/licensing/terms/fr-FR/product/PrivacyandSecurityTerms/all>

Il est également énoncé dans le DPA<sup>22</sup> ce qui suit:

*«Lorsque le client renouvelle son abonnement ou achète un nouvel abonnement à un produit ou conclut un ordre de services pour un service professionnel, les conditions du DPA alors en vigueur s'appliquent et ne seront pas modifiées pendant la durée de l'abonnement du client à ce produit ou la durée de ce service professionnel.»*

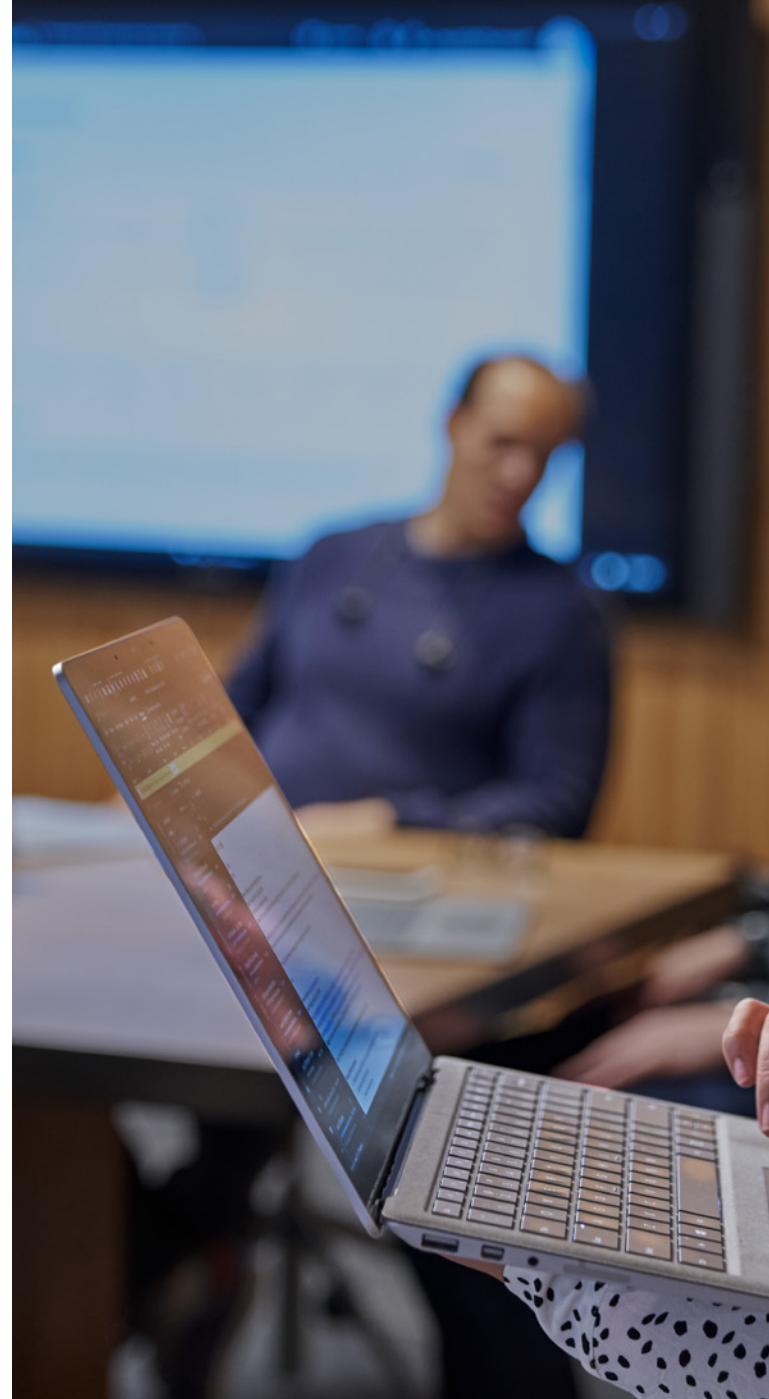
Les contrôles supplémentaires suivants gérés par le client sont disponibles en relation avec l'emplacement des données:

- Au moyen d'«Azure Policies»<sup>23</sup>, le client peut définir ses propres directives pour, p. ex., la conformité et les paramétrages et configurations de la sécurité générale. Ainsi, les exigences minimales devant être remplies lors de la fourniture et de l'utilisation d'un service peuvent être définies, p. ex. le lieu de stockage des données, le nombre de comptes privilégiés, les paramétrages du pare-feu, etc.

- Les «Azure Blueprints»<sup>24</sup> permettent au client de se protéger avant la mise en service de services qui ne sont pas proposés avec le stockage de données dans la région choisie. Les Blueprints sont souvent créés pour garantir le respect d'une norme pertinente ou d'une spécification, comme le Blueprint ISM PROTECTED du gouvernement australien<sup>25</sup>.

- Les clients peuvent ajouter une «Customer Lockbox»<sup>26</sup> pour garantir que l'approbation finale de scénarios impliquant un potentiel accès à distance aux données des clients est au niveau d'une ressource désignée par le client lui-même au sein de l'organisation.

L'arrêt connu sous le nom de Schrems II de la Cour de justice de l'Union européenne a donné l'occasion d'analyser les bases juridiques du transfert de données et les risques associés aux scénarios du transfert de données et d'explorer ce qu'on appelle les «mesures complémentaires» pour minimiser ces risques. Vous trouverez ci-après un exemple de présentation possible d'une telle évaluation lors de l'utilisation des services Azure de Microsoft.



<sup>22</sup> FN 16

<sup>23</sup> [https://docs.microsoft.com/fr-ch/azure/governance/policy/tutorials/create-and-manage?WT.mc\\_id=msignitethetour2019-slides-afun80](https://docs.microsoft.com/fr-ch/azure/governance/policy/tutorials/create-and-manage?WT.mc_id=msignitethetour2019-slides-afun80)

<sup>24</sup> <https://aka.ms/azureblueprints>

<sup>25</sup> <https://docs.microsoft.com/fr-ch/azure/governance/blueprints/samples/ism-protected/control-mapping>

<sup>26</sup> <https://docs.microsoft.com/fr-ch/azure/security/fundamentals/customer-lockbox-overview>

## ETAPE

## DESCRIPTION

**Possibles scénarios de transfert****Maintenance et élimination des défauts initiées par Microsoft.**

Maintenance et élimination des défauts initiées par Microsoft.

Circonstance du transfert: Accès à distance avec priviléges, qui divulguent peut-être les données des clients aux ingénieurs chargés de la maintenance et de l'élimination des défauts.

Fréquence et probabilité: La grande majorité des tâches opérationnelles est automatisée, aucun transfert n'a lieu. Occasionnellement, des tâches importantes ne peuvent pas être exécutées automatiquement et le recours à des techniciens est nécessaire – la plupart de ces scénarios ne requièrent aucune autorisation d'accès aux données des clients. Seule une quantité partielle de ces rares cas, dans lesquels de tels priviléges sont nécessaires, implique l'accès à distance en provenance de pays ne faisant pas partie de l'UE/EEE.

Pays à partir desquels un accès à distance peut avoir lieu dans de rares cas: Etats-Unis, Australie, Japon, Canada, Inde, Irlande, Israël, République tchèque, Allemagne, Serbie, Pays-Bas et Royaume-Uni.

Finalité du transfert: Comme défini à la page 6 du DPA<sup>27</sup>, le but du traitement est la fourniture de services en ligne au client, ce qui comprend ce qui suit:

- La fourniture de fonctions qui sont autorisées, configurées et utilisées par le client et ses utilisateurs, y compris la fourniture d'expériences utilisateurs personnalisées;
- L'élimination des défauts (prévention, détection et résolution de problèmes); et
- L'amélioration en continu (installation des mises à jour les plus récentes et améliorations concernant la productivité, la fiabilité, l'efficacité et la sécurité des utilisateurs).

Dans le cadre de la fourniture des services en ligne, Microsoft n'utilisera ni traitera d'une quelconque autre manière les données des clients ou données à caractère personnel aux fins suivantes: (a) à des fins de profilage des utilisateurs, (b) de publicité ou à des fins commerciales similaires ou (c) pour des études de marché visant à créer de nouvelles fonctionnalités, de nouveaux services ou produits ou tout autre but, à moins que cette utilisation ou ce traitement ne soit conforme aux instructions documentées du client.

**Mécanisme de transfert utilisé**

Tous les potentiels transferts de données qui peuvent avoir lieu dans le cadre des services en ligne Microsoft sont régis par les clauses contractuelles types de l'UE conformément au DPA<sup>28</sup>, telles qu'elles sont également reconnues pour la Suisse comme garantie adaptée.

**Caractère approprié du mécanisme de transfert**

Selon des déclarations du PFPDT à la suite de l'arrêt Schrems II, les clauses contractuelles types de l'UE ne pourraient plus être considérées aisément comme des garanties suffisantes pour certains transferts de données, notamment en ce qui concerne des transferts vers les Etats-Unis. Dans le cas de certains transferts ou accès à distance, des mesures complémentaires doivent par conséquent être examinées.

**Des mesures complémentaires peuvent-elles être prises?**

Oui, le responsable (exportateur) et le chargé du traitement (importateur) peuvent prendre des mesures complémentaires.

27 FN 16

28 FN 16

**Mesures complémentaires appropriées:**

Par Microsoft en qualité de sous-traitant des données: En plus des contrôles déjà garantis dans le DPA29 (en particulier l'annexe A – Mesures de sécurité; l'annexe C – Avenant sur les mesures complémentaires; l'annexe 2 – Conditions du règlement général sur la protection des données de l'Union européenne), les contrôles suivants sont effectués pour les tâches d'exploitation:

- L'accès productif est limité à des identités isolées et à des postes de travail rigoureusement contrôlés.
- Les accès sont octroyés sur la base d'un contrôle des accès basé sur les rôles.
- Une authentification multifacteur est nécessaire.
- La méthode Just-In-Time «JIT» garantit que des droits d'accès de niveau supérieur ne sont donnés que temporairement et avec les droits les plus faibles possibles.
- Les demandes d'accès sont examinées, consignées et surveillées, et les augmentations à risque sont signalées.
- Surveillance 24 × 7 × 365 par le Cyber Defense Operations Center Microsoft.
- Toutes les données sont cryptées en mode veille et lors du transfert. Conformément au DPA30, Microsoft ne saurait fournir à un tiers:  
«a) un accès direct, indirect, général ou illimité aux données traitées; (b) les clés de cryptage utilisées pour sécuriser les données traitées de la plateforme, ou la capacité de déchiffrer un tel cryptage; (...)»
- Par Microsoft en qualité d'importateur:
  - Microsoft Corporation a une obligation de protection des données depuis de longues années: <https://aka.ms/MSCloudPrivacy>
  - Microsoft s'est engagée pendant des années pour les droits des clients sur leurs propres données et le droit à la transparence concernant les demandes d'accès aux données par la justice et a mené des combats juridiques à ce sujet (exemple: <https://aka.ms/MSScrecyOrders>)
  - Après l'arrêt Schrems II, Microsoft a annoncé d'autres obligations en matière de protection des données des clients (<https://aka.ms/MSdyd>) et a intégré ces obligations dans les dispositions en matière de protection des données.
  - Les processus et l'historique de l'importateur concernant le traitement des demandes d'accès de tiers à des données des clients peuvent être consultés sur <https://aka.ms/MSLERH> et
  - <https://aka.ms/MSLERR> – on peut déduire de ces rapports que ces mesures complémentaires de l'importateur font baisser effectivement la probabilité de l'accès
  - à des données des clients par les services Azure de Microsoft à «presque zéro» ou à «un niveau bas acceptable».
- Par le client en qualité de responsable ou d'exportateur:
  - Service Customer Lockbox Azure. Avant l'attribution des priviléges qui permettent un potentiel accès aux données des clients, le client doit autoriser l'attribution. Informations plus détaillées sur: <https://aka.ms/msazurelockbox>
  - Service Azure Policy. Limitation effective de la disponibilité de services en ligne à ceux qui proposent, par exemple, un lieu d'hébergement de données en Europe.
  - Service de surveillance Azure. Analyse des journaux et notification des accès aux données.

**Réévaluation**

Microsoft met à disposition une structure de gouvernance et des technologies de soutien pour vérifier régulièrement tous les éléments mentionnés ci-dessus, notamment: notification automatique des modifications apportées à la documentation, aux audits, aux certifications et aux accords à l'aide de la fonction My-Library dans le Service Trust Portal Microsoft.

Customer Lockbox Azure, pour permettre une évaluation ponctuelle de scénarios de transferts de données pendant la maintenance, l'élimination des défauts et les instances d'assistance.

Service Azure Policy au niveau du tenant, pour une configuration et une accessibilité pilotées par les directives des services pertinents exclusivement.

Surveillance des protocoles d'audit des clients. fourniture de fonctions qui sont autorisées, configurées et utilisées par le client et ses utilisateurs, y compris la fourniture d'expériences utilisateurs personnalisées;

**3. Comment les modifications de la documentation relative à la sécurité, à la protection des données et à la conformité, des listes de sous-traitants, des conditions générales, etc. sont-elles gérées?**

Toute la documentation est publiée sur le «Service Trust Portal»<sup>31</sup> et le client peut sélectionner certains documents, certificats et rapports d'audit pour lesquels il souhaite être avisé des modifications via la fonction MyLibrary.

**4. Le client a-t-il la possibilité de réaliser lui-même des contrôles ou de les faire réaliser par un organe de contrôle indépendant, accrédité et choisi par le client?**

Oui. Dans le paragraphe «Respect des audits» à la page 9 du DPA<sup>32</sup>, des droits d'audit du client sont stipulés, y compris les conditions dans lesquelles le client peut faire réaliser un audit spécial par un tiers.

**5. Comment les journaux d'audit sont-ils sécurisés? – De quelle manière et à quelle fréquence sont-ils contrôlés pour la protection contre des événements non découverts en termes de sécurité?**

Microsoft dispose de technologies de surveillance et d'élaboration de protocoles pour offrir aux clients une transparence maximale sur les activités de ses réseaux, applications et appareils basés sur le cloud et pour identifier les potentiels points faibles en matière de sécurité. Les services en ligne contiennent des fonctions avec lesquelles les clients peuvent limiter et surveiller l'accès de leurs collaborateurs aux services, parmi lesquelles le «Azure AD Privileged Identification Management System» et une authentification multifacteur.

Les services en ligne contiennent par ailleurs des scripts «Windows PowerShell» intégrés, autorisés par Windows, qui contrôlent les priviléges d'accès et réduisent par conséquent au minimum la possibilité d'une mauvaise configuration.

Microsoft permet aux clients d'enregistrer l'accès et l'utilisation des systèmes d'information, y compris les identifiants d'accès utilisés, l'heure, les autorisations octroyées ou refusées, ainsi que d'autres activités pertinentes.

Une équipe interne Microsoft indépendante contrôle le journal au moins une fois par trimestre. Les clients ont accès à ces journaux d'audit.

Microsoft contrôle par ailleurs régulièrement les niveaux d'accès afin de garantir que seuls les utilisateurs avec une autorisation en bonne et due forme ont l'accès.

**6. Microsoft s'engage-t-elle explicitement à respecter les lois et règlements en matière de protection des données?**

Oui. Conformément au paragraphe «Respect de la réglementation applicable» à la page 5 du DPA<sup>33</sup>:

*«Microsoft s'engage à se conformer à toutes les lois et réglementations applicables à la fourniture des produits et des services, y compris à la législation relative à la notification des violations de sécurité et aux obligations de protection des données.»*

Microsoft se conforme également aux exigences des lois sur la protection des données de l'Espace économique européen et de la Suisse eu égard à la collecte, à l'utilisation, au transfert, au stockage et à tout traitement autre de données à caractère personnel provenant de l'Espace économique européen, du Royaume-Uni et de la Suisse (paragraphe «Transferts et emplacement des données – Transferts des données», page 10 DPA<sup>34</sup>).

**7. La convention sur le traitement des données respecte-t-elle les exigences minimales légales?**

Oui. L'avenant sur la protection des données<sup>35</sup> pour les services et produits Microsoft remplit toutes les exigences des lois nationales et cantonales en matière de protection des données.

Par ailleurs, Microsoft actualise régulièrement la convention à partir des retours des clients et des autorités de surveillance. Par exemple, le ministère de la justice des Pays-Bas a effectué plusieurs évaluations approfondies de la protection dont les résultats ont été mis à la disposition des clients dans le monde entier, voir: <https://aka.ms/DutchPrivacyDPIA> et <https://news.microsoft.com/de-de/einfuehrung-von-mehr-datenschutz-transparenz-fuer-unsere-kommerziellen-cloud-kunden/>

**8. Microsoft peut-elle soutenir la «stratégie de sortie» d'un client? – Comment?**

Oui. Au terme ou à la résiliation, le client peut extraire ses données. Comme décrit dans le DPA<sup>36</sup>, Microsoft conservera les données du client stockées dans le service en ligne dans une version fonctionnelle limitée du service pendant 90 jours à partir du terme ou de la fin de l'abonnement du client. Le client peut ainsi extraire les données. Lorsque le délai de conservation de 90 jours est écoulé, Microsoft désactive le compte du client et supprime les données du client au maximum 180 jours à partir du terme ou de la fin de l'utilisation d'un service en ligne par le client.

<sup>31</sup> <https://servicetrust.microsoft.com>

<sup>32</sup> FN 16

<sup>33</sup> FN 16

<sup>34</sup> FN 16

<sup>35</sup> FN 16

<sup>36</sup> FN 16

Les 90 jours à partir du terme ou de la fin sont prévus comme «filet de sécurité» pour d'éventuelles données résiduelles. Lorsqu'un client a besoin ou prévoit une sortie, l'une des premières étapes, dans un plan de sortie structuré, ne doit pas consister à simplement résilier l'abonnement. Il est conseillé au client de démarrer un processus coordonné d'extraction des données, dans lequel une nouvelle destination est définie pour les données. Microsoft propose, en plus du mécanisme standard, plusieurs autres options pour l'extraction des données des clients. Veuillez tenir compte également à ce sujet des stipulations figurant dans le DPA<sup>37</sup>:

*«Pendant toute la durée de l'abonnement du client ou des prestations de services professionnels applicables, ce dernier aura la possibilité d'accéder aux données client stockées sur chaque service en ligne et données de services professionnels, de les en extraire et de les supprimer.»*

Les documents, enregistrements et autres données restent la propriété du client et ne sont pas transférés à Microsoft ou à une autre partie.

Par ailleurs, Microsoft a élaboré des principes directeurs sur la mise en place d'une «stratégie de sortie», que vous trouverez dans le Service Trust Portal, sous le point de menu «FAQ and White Papers» (FAQ et livres blanc)<sup>38</sup>.

## 9. Existe-t-il de la documentation sur la méthode d'exploitation, de sécurisation et de maintenance des services en ligne?

Les clients ont, à tout moment, accès à un portefeuille actualisé de certifications et d'audits de l'exploitation des services en ligne par des tiers.

Un résumé accessible au public<sup>39</sup> présente également une description de la manière dont la Microsoft Cloud Infrastructure Organisation (MCIO) garantit la fiabilité et la sécurité élevées des plateformes en cloud. Le document est abordé de façon globale et comprend des explications sur la préparation physique de l'infrastructure du cloud, sur les processus robustes de gestion des incidents, sur l'assistance du service, sur l'architecture générale en matière de sécurité, sur la gestion des modifications, sur la conformité, sur la conception du matériel des centres de données, les réseaux, les logiciels ainsi que la stratégie de durabilité.

Les centres de données de la MCIO sont gérés selon le concept de l'«Operational Security Assurance»<sup>40</sup> (OSA), qui garantit l'intégration de toutes les expériences individuelles de menaces à la cybersécurité que rassemble Microsoft par le biais de SDL, le Security Response Center<sup>41</sup> de Microsoft, et le Cyber Defense Operations Center<sup>42</sup> de Microsoft. L'OSA limite ainsi les risques au minimum parce qu'elle permet de garantir que les activités d'exploitation courantes sont conformes à des directives strictes en matière de sécurité, et de valider également que les directives sont effectivement respectées. Lorsque des problèmes surviennent, une boucle de retour bien établie permet de garantir que les futurs révisions de l'OSA comporteront des mesures correctives pour supprimer ces problèmes. De cette manière, l'OSA évolue en permanence pour refléter l'image de la menace globale actuelle.

Une description détaillée du Information Security Management System (ISMS) de la MCIO, qui a obtenu la certification ISO (27001), se trouve ici: <https://aka.ms/MSISMS>

Pour finir, les Security Fundamentals<sup>43</sup> Microsoft Azure donnent des informations détaillées sur les fonctions intégrées dans la plateforme et un «Cloud Services Due Diligence Checklist Framework», orienté sur les normes internationales pour les accords de services en cloud (Cloud Services Agreements) (normes telles que ISO/CEI 19086, avec référence à ISO/CEI 19941).

## 10. Dans quelle mesure les normes internationales en matière de sécurité et de protection des données sont-elles prises en charge?

Le portefeuille de certifications selon des normes des services en ligne Microsoft est le meilleur point de départ pour la protection des informations commerciales sensibles et importantes. La liste complète des normes selon lesquelles le cloud Microsoft est certifié, se trouve ici: <https://aka.ms/mscloudcomplianceofferings>

La certification ISO27001<sup>44</sup>, ainsi que les deux qui en dérivent, ISO27018<sup>45</sup> (PII in Cloud) et ISO27701<sup>46</sup> (Privacy Information Management System ou PIMS) en constituent certainement la base.

En 2014, la norme ISO/CEI 27018:2014 a été adoptée en complément de la norme ISO/CEI 27001 et elle est par conséquent devenue le premier «Code of Practice» (code de bonnes pratiques) international pour la protection des données en cloud. La certification est basée sur le droit de l'UE en matière de protection des données et fournit aux prestataires de services en cloud qui agissent en tant qu'entités de traitement de données à caractère personnel (PII) des instructions spécifiques sur l'évaluation des risques et les contrôles en matière de sécurité et de protection des données selon l'état de la technique de la protection de PII.

37 FN 16

38 Voir: [https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=4aa0c653-312f-4098-b78a-0d499e07825e&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad\\_FAQ\\_and\\_White\\_Papers](https://servicetrust.microsoft.com/ViewPage/TrustDocuments?command=Download&downloadType=Document&downloadId=4aa0c653-312f-4098-b78a-0d499e07825e&docTab=6d000410-c9e9-11e7-9a91-892aae8839ad_FAQ_and_White_Papers)

39 <https://aka.ms/mscloudoperations>

40 <https://aka.ms/msopsec>

41 <https://www.microsoft.com/fr-fr/msrc?rtc=1>

42 <https://www.microsoft.com/fr-fr/msrc/cdoc?rtc=1>

43 <https://docs.microsoft.com/fr-ch/azure/security/fundamentals/technical-capabilities>

44 <https://aka.ms/mscloudiso>

45 <https://aka.ms/msiso27018>

46 <https://aka.ms/PIMS3pager>

Microsoft a été le premier grand fournisseur d'informatique en cloud «hyperscale» à viser et à obtenir la certification ISO27018.

Au moins une fois par an, un organisme de certification accrédité tiers contrôle que les normes ISO/CEI 27001 et ISO/CEI 27018 sont bien respectées par la plateforme du cloud Microsoft. Cette validation indépendante garantit ainsi que les contrôles de sécurité applicables existent et fonctionnent de manière efficace.

Dans le cadre de ce processus de contrôle de la conformité, les auditeurs confirment dans leur «Statement of Applicability» que les services en ligne et services d'assistance technique commerciale de Microsoft comprennent les contrôles selon ISO/CEI 27018 pour la protection PII.

La nouvelle norme internationale ISO/CEI 2770175 Privacy Information Management System (PIMS) (connue sous le nom de ISO/CEI 27552 pendant la période de projet), aide les organisations à respecter les exigences légales en matière de protection des données. La norme décrit un ensemble complet de contrôles d'exploitation qui peuvent être représentés dans différentes prescriptions, y compris le RGPD. Après l'affectation, les contrôles d'exploitation PIMS sont mis en œuvre par des experts en protection des données et vérifiés par des contrôleur internes ou externes, ce qui conduit à une certification ou à une preuve de conformité totale. Immédiatement après la publication de la norme ISO27701 en août 2019, Microsoft a demandé le début de la certification et elle a informé le 13 janvier 2020 que la certification était terminée.

Pour des informations complémentaires, voir <https://aka.ms/MSComplianceDokumentation> et <https://aka.ms/mscloudprivacystandards>

Vous trouverez une vue d'ensemble générale des certifications de la plate-forme Microsoft Cloud ici:

<https://aka.ms/mscloudcomplianceofferings>

## 11. Comment est assurée la résilience géographique?

L'infrastructure en cloud de Microsoft est actuellement répartie sur plus de 60 régions, séparées géographiquement par souci de protection contre des menaces externes non numériques.

Les données des clients dans Azure sont stockées dans la région sélectionnée et y sont mises en miroir plusieurs fois. Dans de nombreuses régions, il y a plus de deux centres de données; certains services peuvent donc être proposés de façon dédiée dans ces régions, ce qui augmente encore la sécurité en cas de défaillance en fonction de l'emplacement géographique.

Une description très détaillée de la manière dont on active la résidence de données dans les régions Microsoft Azure se trouve dans le livre blanc «Data Residency et protection des données dans les régions Microsoft Azure»<sup>47</sup> d'avril 2021. Dans ce document figurent les informations et les outils nécessaires pour l'optimisation de l'emplacement des données et l'accès aux données, y compris une présentation détaillée de l'infrastructure régionale Azure, des garanties de l'emplacement des données par service et la manière dont les clients peuvent gérer l'emplacement et l'accès aux données.

On y trouve également des informations sur le service ExpressRoute<sup>48</sup>, qui permet aux clients d'étendre leurs réseaux locaux via une connexion privée fournie par un prestataire de connectivité dans le cloud Microsoft. La connexion peut avoir lieu via un réseau «Any-to-Any» (IP VPN), un réseau Ethernet «Point-To-Point» ou une connexion croisée virtuelle via un prestataire de connectivité dans un centre de colocation. Les connexions ExpressRoute ne passent pas par l'Internet public. Par conséquent, ces connexions ExpressRoute offrent des latences cohérentes, une plus grande fiabilité, des vitesses supérieures et une plus grande sécurité que les connexions habituelles via l'Internet.

## 12. Comment est gérée la conservation des données?

Cela est expliqué en détail dans la CCM23 CSA, section «Data Governance» (Gouvernance des données).

Vous trouverez, spécialement pour Microsoft 365, des informations détaillées sur la conservation des données sur: <https://docs.microsoft.com/fr-fr/compliance/assurance/assurance-data-retention-and-destruction-overview>

Veuillez noter que le client a le contrôle total sur la conservation des données au sein des services en ligne Microsoft.

Pour Microsoft 365: <https://docs.microsoft.com/fr-fr/microsoft-365/compliance/manage-data-governance?view=o365-worldwide>

Pour Microsoft Azure: <https://docs.microsoft.com/fr-fr/azure/purview/>

Les disques durs ne sont ni réutilisés ni réparés.

## 13. Des tests de pénétration, aussi bien pour les réseaux que pour les applications, sont-ils réalisés?

Oui. Microsoft exécute régulièrement des tests de pénétration afin de garantir une amélioration permanente de la sécurité globale et du processus «Incident Response» (réaction aux incidents). Ces tests internes aident les experts en sécurité de Microsoft à parvenir à un processus de réaction progressive méthodique, réplicable et optimisé, ainsi qu'à une automatisation.

Des rapports sur les tests de pénétration sont publiés dans l'onglet «Pentest and Security Test» (Test de pénétration et test de sécurité), au paragraphe Protection des données dans le Security Trust Portal<sup>49</sup>.

Par ailleurs, la «Microsoft Red Team» exécute des tests de pénétration en direct sur des programmes et services de l'infrastructure en cloud gérée par Microsoft sur site. Cette équipe simule de violations «réelles» de la sécurité et effectue des exercices permanents sur la surveillance de la sécurité et sur la réaction à des incidents en vue de valider et d'améliorer la sécurité dans Microsoft Azure, Microsoft 365 et Dynamics 365.

Ces expériences avec des processus de sécurité constituent une base solide pour les clients qui veulent utiliser et gérer des solutions d'informatique en cloud de manière sûre.

47 <https://azure.microsoft.com/fr-fr/resources/achieving-compliant-data-residency-and-security-with-azure/en-us/>

48 <https://azure.microsoft.com/fr-fr/services/expressroute/>

49 <https://aka.ms/stp>

#### 14. Comment la récupération par le client de ses données en cas d'erreurs ou de pertes est-elle assurée?

Les données des clients sont répliquées de façon permanente et enregistrées plusieurs fois dans la région sélectionnée. Cela permet la récupération des données en cas d'erreurs dans cette infrastructure locale. Le client est tenu de prendre d'autres mesures pour parvenir à une tolérance aux erreurs supérieure, par exemple, créer des sauvegardes d'historiques des données du client, stocker des sauvegardes des données du client hors de l'environnement du cloud, mettre en œuvre des «Compute Instances» redondantes dans et entre les centres de données ou sécuriser l'«état» et les données dans une machine virtuelle.

Microsoft offre au client la possibilité de mettre cette fonction en place, par exemple, sur Azure Storage. Pour soutenir la diligence raisonnable, il est bon de mentionner que la CCM23 CSA: Control ID DG-04 Gouvernance des données – Politique de conservation exige ce qui suit:

*«Des politiques et procédures de conservation et de stockage des données doivent être établies et des mécanismes de sauvegarde ou de redondance mis en œuvre pour assurer la conformité avec les exigences réglementaires, statutaires, contractuelles ou professionnelles. Des tests de récupération des sauvegardes sur disque ou sur bande doivent être mis en œuvre à intervalles planifiés.»*

Dans la réponse de Microsoft, qui se trouve dans le document «Réponse standard Microsoft Azure à une demande d'information – Sécurité et Respect de la vie privée»<sup>50</sup>, figure ce qui suit:

*«Des politiques et procédures de conservation des données sont définies et mises en œuvre conformément aux exigences réglementaires, statutaires, contractuelles ou professionnelles. Le programme Microsoft Azure de sauvegarde et de redondance est soumis à une révision et une validation annuelles. Microsoft Azure sauvegarde régulièrement les données de l'infrastructure et valide la restauration des données périodiquement à des fins de récupération en cas de catastrophe. Microsoft Azure inclut les fonctions de réPLICATION détaillées ci-dessous pour contribuer à empêcher la perte de données des clients en cas de panne dans un centre de données Microsoft.*

[...]

*La sauvegarde des informations est assurée selon les normes ISO 27001; elle est abordée de façon plus détaillée dans l'annexe A, paragraphe 10.5.1. Pour de plus amples informations, il est conseillé de consulter les normes ISO accessibles au public pour lesquelles nous sommes certifiés.»*

Une géoréplication est par ailleurs fournie pour sécuriser les données en cas de catastrophe importante dans le centre de données ou de panne temporaire de matériel. Le client dispose de trois options pour la réplication des données:

**Le stockage localement redondant (LRS)** est répliqué trois fois au sein d'un centre de données. Lorsque des données sont écrites dans un blob, une file d'attente ou un tableau, le processus d'écriture est exécuté de manière synchrone dans les trois réplications. Le LRS protège vos données des pannes normales de la partie matérielle.

**Le stockage géo-redondant (GRS)** est répliqué trois fois au sein d'une seule région et répliqué également de manière asynchrone dans une deuxième région qui est à des centaines de kilomètres de la région primaire. Le GRS conserve l'équivalent de six copies (répliques) des données (trois dans chaque région). Le GRS permet un basculement sur une deuxième région lorsque la première région ne peut pas être restaurée en raison d'une panne importante ou d'une catastrophe. Le GRS est recommandé par rapport au stockage localement redondant.

**Le stockage géo-redondant avec accès en lecture (RA-GRS)** présente tous les avantages cités ci-dessus du stockage géo-redondant et permet par ailleurs l'accès en lecture aux données dans la région secondaire pour le cas où la région primaire n'est plus disponible. Le stockage géo-redondant avec accès en lecture est recommandé pour une disponibilité maximale avec une durabilité supplémentaire.

Vous trouverez un guide pour les clients sur la manière d'élaborer, de gérer et de tester un plan de sauvegarde et de restauration pour les services Azure, qui correspond à leur tolérance par rapport à une fonctionnalité limitée pendant une catastrophe sur <https://docs.microsoft.com/fr-ch/azure/architecture/framework/resiliency/backup-and-recovery>



50 <https://aka.ms/MSazurescsa>

Grâce aux solutions SaaS (Software as a Service) telles que Microsoft 365, la plateforme dispose déjà en soi d'une résilience de données intégrée<sup>51</sup>, mais les clients doivent réfléchir à la manière dont ils peuvent protéger au mieux leurs données des menaces modernes (p. ex. les attaques de rançongiciels) en utilisant des solutions de protection contre les menaces<sup>52</sup> et des options de restauration<sup>53</sup> et en configurant une sauvegarde du service (p. ex. avec Exchange Online<sup>54</sup>).

## 15. Dans quelle mesure un chiffrement est-il utilisé pour des données «au repos» et pour des données «en transit»?

Conformément au DPA<sup>55</sup>

«Les données client et les données des services professionnels (y compris les données à caractère personnel qui s'y trouvent) en transit sur les réseaux publics entre le client et Microsoft, ou entre les centres de données de Microsoft, sont chiffrées par défaut.

*Microsoft chiffre également les données client stockées au repos dans les services en ligne et les données des services professionnels stockées au repos. Dans le cas des services en ligne sur lesquels le client ou un tiers agissant pour le compte du client peut construire des applications (par exemple, certains services Azure), le chiffrement des données stockées dans lesdites applications peut être mis en œuvre à la discréption du client, en utilisant soit les moyens fournis par Microsoft, soit ceux obtenus par le client auprès de tiers.»*

Les données des clients dans les services Enterprise Cloud de Microsoft sont protégées par une multitude de technologies et procédés, y compris par différentes formes de chiffrement. Microsoft propose plusieurs fonctions de chiffrement intégrées pour soutenir la protection des données:

- pour Microsoft 365, Microsoft utilise des normes industrielles de cryptographie comme TLS/SSL et AES pour protéger la confidentialité et l'intégrité des données des clients. Pour les données en transit, tous les serveurs avec des réunions des clients négocient une session sécurisée avec TLS/SSL avec les ordinateurs clients pour protéger les données des clients. Pour les données au repos, Microsoft 365 installe BitLocker avec chiffrement AES 256 bits sur tous les serveurs sur lesquels sont stockées des données de messagerie, y compris les entretiens par courriel et chat, ainsi que toutes les données dans SharePoint Online et OneDrive for Business. Microsoft dispose également de quelques scénarios sur un chiffrement utilisateur au niveau du fichier.
- Chez Azure, des mesures techniques de sécurité comme la communication et les processus d'exploitation cryptés aident à protéger les données des clients. Microsoft permet également aux clients de mettre en œuvre un chiffrement complémentaire et de gérer leurs propres clés. Pour les données en transit, Azure utilise des protocoles de transport sûrs, selon une norme industrielle comme TLS/SSL, entre les appareils des utilisateurs et les centres de données Microsoft. Pour les données au repos, Azure propose de nombreuses options de chiffrement, par exemple le support AES 256, qui offre une flexibilité aux clients en leur permettant de choisir le scénario de stockage de données qui répond le mieux à leurs exigences.
- Microsoft utilise certains des protocoles de chiffrement les plus puissants et les plus sûrs qui sont disponibles pour créer des barrières empêchant l'accès non autorisé aux données des clients. Une gestion en bonne et due forme des clés est également un élément important des solutions de chiffrement optimales, et Microsoft garantit que toutes les clés de chiffrement qu'elle gère sont sécurisées selon les règles.

La validation de la directive Microsoft relative au chiffrement et sa mise en œuvre ont été vérifiées par plusieurs instances de contrôle indépendantes et les rapports de contrôle sont disponibles sur le Service Trust Portal<sup>56</sup>.

Microsoft 365 propose par ailleurs le «Customer Key Encryption», qui ajoute une autre dimension de chiffrement au niveau de l'application: <https://docs.microsoft.com/de-ch/microsoft-365/compliance/customer-key-overview?view=o365-worldwide>

Pour des informations spécifiques sur le chiffrement:

- Comment la plateforme du cloud Microsoft utilise le chiffrement de manière générale:  
<https://docs.microsoft.com/fr-fr/compliance/assurance/assurance-encryption>
- Chiffrement Microsoft Azure: <https://docs.microsoft.com/fr-ch/azure/security/fundamentals/encryption-overview>
- Chiffrement Microsoft O365: <https://docs.microsoft.com/fr-ch/microsoft-365/compliance/encryption?view=o365-worldwide>
- <https://aka.ms/o365IntroTilKryptering>
- Chiffrement des mails: <https://docs.microsoft.com/fr-ch/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview?view=o365-worldwide>
- Pour une initiation rapide à un grand nombre de ces thèmes, des vidéos de Microsoft Security sont également disponibles:
- Chiffrement M365 de données au repos:  
<https://www.youtube.com/watch?v=Dk380mk-xh0&t=41s>
- Protection des données Azure:  
<https://www.youtube.com/watch?v=dRgZJpKj7hU&t=818s>

<sup>51</sup> <https://docs.microsoft.com/fr-ch/compliance/assurance/assurance-data-resiliency-overview>

<sup>52</sup> <https://docs.microsoft.com/fr-ch/microsoft-365/security/office-365-security/protect-against-threats?view=o365-worldwide>

<sup>53</sup> <https://docs.microsoft.com/fr-ch/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide>

<sup>54</sup> <https://docs.microsoft.com/fr-ch/exchange/back-up-email>

<sup>55</sup> <https://aka.ms/dpa>

<sup>56</sup> <https://servicetrust.microsoft.com>

## 16. Le client a-t-il accès à des technologies de chiffrement supplémentaires, notamment BYOK, etc.?

En principe, Microsoft gère les clés pour les chiffrements standards performants utilisés dans les services en ligne, mais les clients peuvent aussi utiliser leur propre chiffrement.

D'un point de vue contractuel, il convient d'attirer l'attention sur le fait que Microsoft ne fournit (a) aucun accès direct, indirect, général ou illimité aux données traitées ni (b) aucune clé de chiffrement utilisée pour sécuriser les données traitées sur la plateforme à des tiers, et (c) ne donne pas la possibilité à des tiers de contourner ce chiffrement.

Vous trouverez d'autres informations sur le chiffrement dans la réponse à la question précédente.

Lorsqu'un client utilise ou ajoute un chiffrement propre, la règle applicable en ce qui concerne la gestion des clés de chiffrement est la suivante: le chiffrement et l'authentification n'améliorent pas la sécurité si les clés elles-mêmes ne sont pas correctement protégées. On considère de manière générale la gestion des cycles de vie des clés comme une tâche critique en matière de sécurité informatique, car une bonne gestion des clés est importante pour garantir un niveau de sécurité élevé, une grande fiabilité et des frais généraux moindres.

### a. Bring-Your-Own-Key/Hold-Your-Own-Key (BYOK/HYOK)

Azure Key Vault<sup>57</sup> est un service en cloud permettant le stockage et l'accès en toute sécurité aux secrets. Toutes les informations pour lesquelles des clients souhaitent contrôler strictement l'accès, comme des clés API, des mots de passe, des certificats ou des clés cryptographiques, peuvent être un secret. Cela permet à des organisations de toute taille de stocker et d'utiliser leurs propres clés avec une extrême sécurité – en conformité avec les directives d'accès du coffre-fort – car on mise sur des modules matériels de sécurité (HSM) éprouvés dans le domaine et conformes à la norme FIPS de différents prestataires HSM<sup>58</sup>. La capacité du BYOK permet à ces entreprises de générer et d'importer leur clé sur site et de déléguer les droits d'utilisation à un nombre croissant de services en cloud Microsoft (comme Microsoft 365 et différents services Azure), qui prennent en charge l'intégration avec Azure Key Vault pour le chiffrement côté services, le chiffrement côté client et/ou le chiffrement des contenus pour la protection de leurs données.

La solution est conçue de telle manière que Microsoft ne peut ni voir ni extraire les clés des clients. Vous trouverez ici une explication plus précise de la manière de planifier et de mettre en œuvre l'utilisation du service Azure Key Vault: <https://aka.ms/azurekeyvaultplanning>

Microsoft propose aussi un autre nouveau service, le «Double Key Encryption» (<https://docs.microsoft.com/fr-ch/microsoft-365/compliance/double-key-encryption?view=o365-worldwide>): avec ce service, Microsoft stocke l'une des clés dans Microsoft Azure et le client conserve l'autre clé. Avec le service «Double Key Encryption», le client conserve le contrôle total sur l'une des deux clés du client. Ainsi, la protection, avec Azure Information Protection Unified Labeling Client, peut être appliquée sur ses contenus les plus sensibles.

### Remarque:

Les solutions BYOK/HYOK (telles que Double Key Encryption) ne sont conçues que pour les données les plus sensibles, qui sont soumises aux exigences les plus strictes en matière de protection. La solution Double Key Encryption n'est donc pas conçue pour toutes les données, parce qu'elle entraîne des conséquences importantes aussi bien en termes de coûts, de complexité, de nouveaux risques en matière de sécurité (potentielle perte de la disponibilité de données) et enfin en termes de limitations fonctionnelles occasionnelles. De manière générale les clients doivent utiliser la Double Key Encryption uniquement pour protéger une petite partie de l'ensemble des données. Avant l'utilisation de la Double Key Encryption ou d'une autre solution BYOK/HYOK il convient de procéder à une diligence raisonnable pour l'identification des données correctes pour l'utilisation de ces solutions. Dans certains cas les responsables des données doivent limiter le domaine d'application et utiliser pour la plupart des données d'autres solutions – des solutions comme Microsoft Information Protection avec Microsoft-managed Keys ou BYOK. Ces solutions sont très probablement suffisantes pour des documents/données qui ne sont pas soumis à une protection étendue ou en tout cas à des exigences réglementaires étendues.

Vous trouverez ci-après une liste de services qui ne peuvent pas être utilisés complètement avec des contenus cryptés par Double Key Encryption:

- règles de transport comme Anti-Malware et Spam, qui requièrent une consultation des documents annexés.
- Microsoft Delve et MyAnalytics.
- eDiscovery.
- Recherche de contenus et indexation.
- Applications Office Web, y compris la fonctionnalité de Co-Authoring.

Tous les services ou applications externes qui ne sont pas intégrés à Double Key Encryption (avec l'utilisation de Microsoft Information Protection), ne peuvent exécuter aucune action avec les données cryptées.

Pour une initiation rapide à ces thèmes, des vidéos sont également disponibles, p. ex.:

57 <https://azure.microsoft.com/fr-fr/services/key-vault/>

58 <https://docs.microsoft.com/fr-ch/azure/key-vault/keys/hsm-protected-keys>

M365 Double Key Encryption:

<https://www.youtube.com/watch?v=0d-A4OYxaEA&t=2s>

MyAnalytics: <https://www.youtube.com/watch?v=43i-lXo4wN8>

## 17. Quels contrôles en matière de sécurité et de protection des données effectue Microsoft en ce qui concerne ses propres collaborateurs et les collaborateurs des sous-traitants?

Pour certains services en ligne de base dans Office 365 et Azure, les collaborateurs (y compris les collaborateurs des sous-traitants) avec un potentiel accès aux données des clients sont soumis à un contrôle de leurs antécédents (dans la limite autorisée par la loi) et doivent suivre une formation à la sécurité.

Le contrôle des antécédents est dans tous les cas effectué avant qu'il soit possible (dans de rares cas) de donner éventuellement au collaborateur l'autorisation d'accéder aux données des clients. Les cas de fraude, d'abus de confiance, de blanchiment d'argent ou de divulgation au niveau professionnel d'informations fausses, de falsification ou de détournement relevant du droit pénal peuvent exclure un candidat de l'activité ou entraîner la résiliation du contrat de travail.

Voir également la Cloud Control Matrix CSA (matrice de contrôle du cloud CSA)<sup>59</sup>, pages 40 à 46 «Human Resources: Controls» et autres informations détaillées dans le «Microsoft Provider Security and Privacy Assurance Program»: <https://aka.ms/mssspa>

## 18. Comment Microsoft contrôle-t-elle la gestion des identités et des accès?

Toutes les mesures de sécurité font partie du Control Kit Microsoft, qui a été vérifié dans les rapports SSAE 18 SOC 1, type II et SSAE 18 SOC 2, type II.

Microsoft s'engage dans le DPA<sup>60</sup> à effectuer plusieurs contrôles qui sont nécessaires conformément à la norme ISO/CEI 27002: 2013 «Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information» et les intégralement mis en œuvre.

Vous trouverez ci-après une vue d'ensemble (une description détaillée des contrôles se trouve également dans les Cloud Control Matrices CSA<sup>61</sup>):

### Autorisation d'accès

- Microsoft gère et tient à jour une liste des collaborateurs qui ont l'autorisation d'accès aux systèmes Microsoft contenant des données des clients.
- Microsoft désactive les moyens d'authentification qui n'ont pas été utilisés pendant une période de six mois maximum.
- Microsoft identifie les collaborateurs qui peuvent octroyer, modifier ou suspendre l'accès autorisé à des données et ressources.
- Microsoft s'assure que, lorsque plusieurs personnes ont accès à des systèmes qui contiennent des données des clients, celles-ci disposent d'identifications/de connexions séparées.
- Least Privilege: le personnel de l'assistance technique ne peut accéder à des données des clients que lorsque cela est absolument indispensable et sous réserve du processus de Lockbox défini et vérifié.
- Microsoft limite l'accès aux données des clients aux personnes qui ont besoin de cet accès pour s'acquitter de leur mission professionnelle.
- Azure Active Directory<sup>62</sup> permet, par ailleurs, au client de gérer lui-même l'accès à ses instances en cloud. Par ailleurs, l'authentification multifacteur<sup>63</sup> et les services de surveillance des accès<sup>64</sup> permettent d'assurer une meilleure sécurité.
- Découvrez d'autres conseils utiles sur le thème de la gestion des identités et des accès sur: <https://aka.ms/MScloudidam>

## 19. Comment Microsoft gère-t-elle la séparation des données des clients dans un environnement multi-tenant?

Microsoft isole dans tous les services en ligne de manière logique les données des clients des autres données qu'elle stocke. Le stockage et le traitement des données pour chaque mandant sont répartis dans une structure «Azure Active Directory» qui isole les clients par le biais de limites de sécurité («silos»). Les silos protègent les données du client afin que celles-ci ne puissent pas être appelées sur la plateforme ou compromises par d'autres clients.

Pour l'explication de la méthode d'isolement dans Microsoft Azure voir: <https://docs.microsoft.com/fr-ch/azure/security/fundamentals/isolation-choices>

Pour l'isolement dans Microsoft 365 voir: <https://docs.microsoft.com/de-ch/microsoft-365/enterprise/microsoft-365-tenant-isolation-overview?view=o365-worldwide>

Voir également contrôle CCM23 CSA «AAC-03.1», «IVS-08.3», «IVS-09.4».

## 20. Comment sont traitées les demandes d'accès aux données ou de communication de données émises par les autorités?

Depuis des années, Microsoft œuvre pour la promotion de la sécurité publique, en garantissant que les êtres humains peuvent faire confiance à la technologie. Nous espérons que nos contributions conduiront à la modernisation de lois, qui fonctionneront pour tous; voir: <https://aka.ms/datalaw>.

Nous pensons que les clients doivent connaître nos directives internes en rapport avec nos réponses aux demandes du gouvernement concernant leurs données. Cette transparence aide aussi les décideurs politiques dans leur travail sur la modernisation de lois qui concernent nos clients.

59 <https://aka.ms/csamatrizona> ou <https://aka.ms/csamatriono365>

60 FN 16

61 <https://aka.ms/csamatrizona> et <https://aka.ms/csamatriono365>

62 <https://docs.microsoft.com/fr-ch/azure/active-directory/>

63 <https://docs.microsoft.com/fr-ch/azure/active-directory/authentication/concept-mfa-howitworks>

64 <https://docs.microsoft.com/fr-ch/azure/active-directory/reports-monitoring/overview-reports>

Microsoft estime que les clients doivent avoir le droit d'être protégés par leurs propres lois. Par ailleurs, Microsoft pense qu'à notre époque moderne, les principes formulés représentent des droits universels et des exigences minimales de base, qui doivent régir l'accès des autorités chargées des poursuites pénales aux données. L'application de ces principes peut varier d'un pays à l'autre, mais les principes de base du contrôle et de la proportionnalité, la responsabilité et la transparence subsistent dans toutes nos opérations à l'échelle mondiale.

Microsoft adopte une approche rigoureuse et attachée aux principes dans la gestion des demandes des autorités d'accéder aux données des clients qui sont détenues par Microsoft. Les principales directives que nous respectons pour tous nos services sont les suivantes:

- Microsoft n'accorde à aucun gouvernement l'accès direct et libre aux données de ses clients, et nous ne donnons à aucun gouvernement nos clés de chiffrement ou la possibilité de passer outre le chiffrement.
- Si un gouvernement souhaite avoir des données des clients, il doit respecter les procédures légales en vigueur. Il doit nous présenter un mandat de perquisition ou une décision judiciaire pour des données de contenus ou une disposition procédurale pour des informations relatives à un abonnement ou des données autres que des données de contenus.
- Toutes les demandes doivent se rapporter à des comptes et des identifiants définis.
- L'équipe du service Legal & Compliance de Microsoft contrôle toutes les demandes pour s'assurer qu'elles sont valables, rejette celles qui ne le sont pas et ne fournit que les données indiquées.

Le processus est décrit ici de manière détaillée: <https://aka.ms/MSLERH>

Une partie du travail de Microsoft en rapport avec les demandes des gouvernements comprend la publication tous les six mois de «Law Enforcement Request Reports» pour garantir la transparence sur l'étendue et la nature de ces événements. Les rapports se trouvent ici: <https://aka.ms/MSLERR> et peuvent être utilisés par le client; ils peuvent l'aider lors de la réalisation d'évaluations des risques.

Pour une évaluation du risque d'accès des autorités, il peut être pertinent de prendre en considération les chiffres réels concernant l'étendue dans les Law Enforcement Request Reports de Microsoft qui sont disponibles sous le lien ci-dessus.

Comme les rapports sur les demandes et les documentations à la base le montrent, Microsoft ne reçoit au niveau mondial qu'une poignée par semestre de demandes des autorités chargées des poursuites pénales aux Etats-Unis concernant des clients d'entreprises commerciales qui ont obtenu plus de 50 «seats» pour l'une de nos offres de commerce en cloud, ayant entraîné la divulgation de données de contenus relatives aux clients d'entreprises non américaines et dont les données étaient stockées hors des États-Unis.

- Pour le nombre estimé de comptes d'entreprise dans les services en ligne Microsoft, les chiffres ci-dessus montrent clairement que ...
- la probabilité qu'une entreprise cliente déterminée soit la cible d'une telle demande est minime;
- la probabilité qu'une telle demande ne soit PAS refusée ou redirigée est encore plus faible et
- la probabilité qu'une telle demande de données, qui sont stockées hors du pays d'origine de la demande, ne soit PAS refusée ou redirigée, est de 1 sur le nombre total de clients utilisant les services en ligne Microsoft.

Si l'on se base sur ces rapports, sur la conception du processus général et sur l'histoire de Microsoft concernant la protection des droits des clients à la sphère privée, les clients doivent pouvoir réaliser une évaluation des risques qui montre que la probabilité, et par conséquent le risque global, de demandes des autorités chargées des poursuites pénales de pays tiers est absolument minime.

Il convient également de prendre en compte le fait que la différence en termes de quantité entre les demandes relatives aux comptes d'utilisateurs et les comptes d'entreprises reflète aussi les diverses directives formelles<sup>65</sup> du Département de la cybercriminalité et de la propriété intellectuelle du ministère américain de la justice, qui conseille aux procureurs de s'adresser directement aux entreprises lorsqu'ils souhaitent avoir accès à leurs données, lorsque cela est possible et que les investigations ne sont pas compromises d'une quelconque autre manière, plutôt que d'essayer de passer par le fournisseur de services en cloud. Extrait de directives:

*«(...) Les procureurs doivent chercher les données directement dans l'entreprise plutôt que chez le fournisseur de stockage en cloud, dans la mesure où cela ne compromet pas les investigations. (...) En travaillant avec des avocats et la technologie de l'information de l'entreprise, l'organisme chargé d'application de la loi peut identifier et demander la divulgation d'informations pertinentes. (...) Si l'organisme d'application de la loi a des raisons de croire que l'entreprise n'est pas disposée à se conformer ou si l'entreprise elle-même est essentiellement vouée à se conduire de façon délictueuse, demander la divulgation directement chez le fournisseur de cloud peut être la seule option possible. (...) Par conséquent, pour toute grande entreprise, notamment si elle doit respecter des normes professionnelles de niveau élevé, il serait difficile pour l'organisme d'application de la loi de soutenir [(MSFT): devant un juge indépendant aux Etats-Unis] que des faits spécifiques existent selon lesquels la notification compromettrait les investigations.»*

Dans l'arrêt Schrems II, certaines lois américaines sur la surveillance, qui laissent penser que les Etats-Unis seraient à considérer comme un pays tiers non sûr, sont citées. Bien que...

- Microsoft ait une longue tradition aussi bien de la contestation des demandes des services de renseignements<sup>66</sup> que des processus autour de ces demandes<sup>67</sup>,

65 <https://aka.ms/USDoJSeekingEnterpriseData>

66 <https://aka.ms/MSSecrecyOrdersHistory>

67 <https://aka.ms/MSSecrecyOrders2021>

- Microsoft puisse assurer qu'aucune tierce partie n'a un accès libre ni aux données ni aux clés de chiffrement (et n'en a jamais eu),
- Microsoft améliore en permanence les mécanismes de protection dans l'infrastructure du cloud Microsoft<sup>68</sup>,
- Microsoft encourage les réformes<sup>69</sup> des pratiques de surveillance, et notamment que
- Microsoft se batte<sup>70</sup> pour pouvoir offrir la meilleure transparence possible sur l'étendue et les résultats de ces demandes...

... la transparence totale n'est actuellement pas possible juridiquement pour des raisons de sécurité nationale. Cependant, les rapports que publie Microsoft, sur la base des lois américaines sur la surveillance, concernant ces demandes fournissent suffisamment d'informations pour permettre aux entreprises clientes d'évaluer si elles ont des risques que leurs données puissent faire l'objet de demandes des services de renseignements. Comme pour les Law Enforcement Requests, la probabilité totale (et par conséquent le risque) est absolument minime, et ce dans la mesure où la plupart des experts en sécurité la considéreraient comme acceptable, voire négligeable. Les rapports que Microsoft peut légalement publier se trouvent ici: <https://aka.ms/MSLERNsO>

Veuillez noter que les processus et obligations contractuelles de Microsoft en rapport avec la réponse aux demandes des gouvernements sont valables également pour les demandes qui concernent la sécurité nationale. Microsoft interagit quotidiennement avec des clients et des gouvernements du monde entier et participe ainsi à la création du cadre juridique international pour ces thèmes critiques. Microsoft a publié six principes directeurs pour ce travail:

«SIX PRINCIPLES FOR INTERNATIONAL AGREEMENTS GOVERNING  
LAW ENFORCEMENT ACCESS TO DATA» (SIX PRINCIPES POUR LES  
ACCORDS INTERNATIONAUX RÉGISSANT  
L'ACCÈS AUX DONNÉES DANS LE CADRE DE L'APPLICATION DE LA LOI):  
<https://aka.ms/MS6dataaccessPrinciples>

68 <https://aka.ms/MSProtectingDataFromGovernments>

69 <https://aka.ms/MSReformGovernmentSurveillance>

70 <https://aka.ms/MSSecrecyOrders>



Microsoft s'engage contractuellement à être responsable de cette gestion telle qu'elle est définie explicitement dans le DPA<sup>71</sup> sous «Divulgation des données traitées», page 6. Par ailleurs, après l'arrêt Schrems II, un autre engagement a été repris dans le DPA, à savoir contester toute injonction de tiers visant à la divulgation de données de clients (annexe C – Avenant sur les mesures complémentaires), qui s'applique à l'utilisation par l'entreprise dans son ensemble des services en ligne Microsoft.

#### **21. Des sous-traitants sont-ils engagés? Et si oui, dans quelles conditions et pour quoi faire?**

Dans le DPA<sup>72</sup>, le paragraphe «Notifications et contrôles sur le recours à des sous-traitants ultérieurs» explique comment Microsoft gère les sous-traitants ultérieurs et informe les clients des modifications apportées dans le portefeuille des sous-traitants ultérieurs, etc.

Dans le Service Trust Center, une liste est tenue sur les services fournis par les sous-traitants ultérieurs, le lieu de leur siège social et la portée et les conditions dans lesquelles ils peuvent avoir accès aux données des clients: <http://aka.ms/mscloudsubprocessors>.

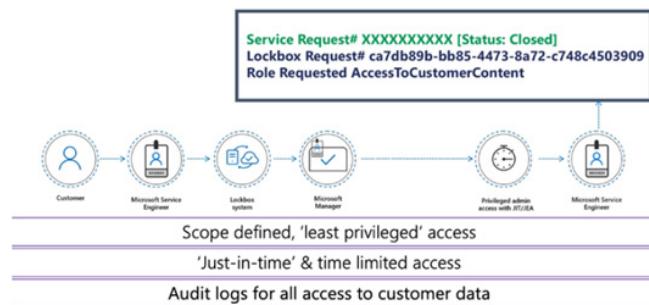
Les conditions précises du recours à des sous-traitants ultérieurs et de l'accès aux données par ceux-ci se trouvent dans le DPA<sup>73</sup> et un guide de lecture succinct se trouve ici: <https://aka.ms/msclouddataaccess>, pour Azure ici: <https://aka.ms/AzureDataAccess> et pour O365 ici: <https://aka.ms/o365dataaccess>

On y trouve la description des exigences auxquelles Microsoft soumet les sous-traitants ultérieurs (y compris le sous-groupe considéré comme sous-traitant les données) et il y est stipulé que Microsoft est tenue de faire appliquer toutes les exigences en vertu du DPA par les sous-traitants ultérieurs.

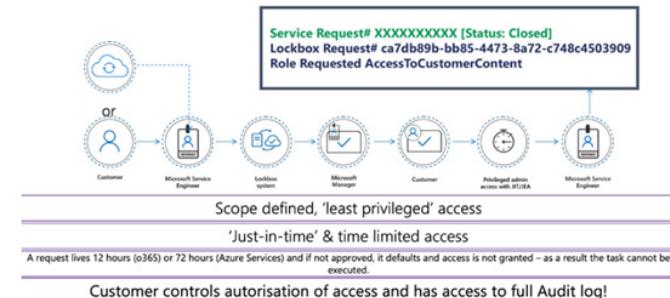
Ni Microsoft ni les sous-traitants ultérieurs n'ont un accès administratif permanent aux données des clients ou aux solutions des clients. Microsoft Cloud fonctionne avec le principe «Zero standing ADMIN», également connu sous le terme «Least Privilege», avec lequel l'accès administratif est contrôlé par une procédure d'authentification (désignée «Lockbox»), par exemple, dans le cas de clients, qui chargent Microsoft d'une activité d'assistance, avec octroi au collaborateur auquel est confiée l'assistance en question de priviléges (qui pourraient permettre l'accès dans un cas précis à des données du client). L'attribution de cet accès administratif doit se faire par le biais de plusieurs liens, des Time-Boxes et un protocole d'audit complet, et peut aussi comprendre, si le client le souhaite, l'approbation finale du client, par la mise en place d'un processus de «Lockbox» élargi, appelé «Customer Lockbox».

Les deux procédures sont présentées ci-après:

#### **Microsoft Lockbox approval workflow**

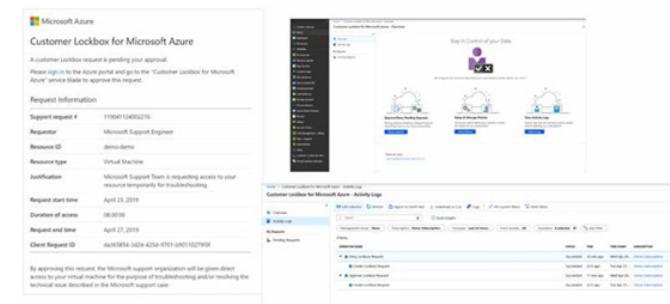


#### **Customer Lockbox approval workflow**



Lockbox, pouvant être élargi avec la validation finale par le client:

Le client peut librement choisir de faire réaliser la tâche telle que décrite:



En savoir plus sur la commande «Customer Lockbox» en suivant ces liens:

<https://aka.ms/msazurelockbox> et

<https://aka.ms/o365CustomerLockbox>

71 FN 16

72 FN 16

73 FN 16

**22. Dans quelle mesure des données sont-elles transférées dans des pays hors de l'UE/EEE? Quels contrôles juridiques, quelles mesures en matière de sécurité et de protection des données sont à la disposition du client pour réaliser une évaluation des risques et documenter des transferts?**

Le DPA<sup>74</sup> définit sous «Transfert et emplacement des données» dans quels cas un transfert (au sens juridique) peut avoir lieu.

L'exploitation standard des services de base en ligne Microsoft<sup>75</sup> ne requiert en général pas d'accès ou de consultation des données des clients. Les directives internes standard de Microsoft prévoient que, si un tel accès doit être octroyé, celui-ci suit le processus de «Lockbox» décrit ci-dessus à la question 21. Et si le client a implémenté et configuré la fonction «Customer Lockbox», cela nécessite en plus le consentement du client. Que la fonction «Customer Lockbox» ait été intégrée ou non, tous les cas d'accès sont documentés dans les protocoles d'audit réguliers du client et peuvent ainsi être intégrés dans la documentation de la conformité.

Une description détaillée de la manière dont l'accès aux données est géré dans le cloud Microsoft se trouve ici: <https://aka.ms/azuredataaccess> & <https://aka.ms/o365dataaccess>

**23. Existe-t-il des aides pour l'obtention, la fourniture, la migration et la garantie de la conformité des services en ligne?**

**a. Cas d'utilisation par des clients existants**

Des millions de clients de toutes les secteurs d'activité dans le monde entier utilisent aujourd'hui les nombreux services en cloud Microsoft disponibles – diverses descriptions de cas sont en ligne et peuvent vous inspirer: <https://aka.ms/msazurerecipes>

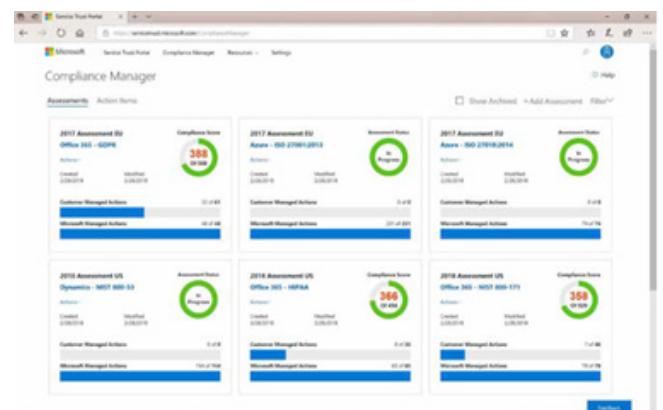
Le portail <https://azure.microsoft.com/en-us/industries/government/> donne accès à une multitude d'informations sur des solutions, qui sont spécialement orientées vers des secteurs sélectionnés (p. ex. le secteur public<sup>76</sup>), documentation technique et de conformité, outils pour les développeurs, formations<sup>77</sup> pour les développeurs comme pour les exploitants et les utilisateurs, etc. Des informations similaires sont également disponibles pour Microsoft 365 et Dynamics 365.

**b. Analyse des coûts des services en cloud (TCO):**

Le «Microsoft Configuration and Pricing Portal»<sup>78</sup> permet aux clients d'évaluer et de prévoir les coûts de la mise en service et de l'exploitation de tous les services en cloud.

**c. Tâches relatives à la conformité**

Le Compliance Manager<sup>79</sup> Microsoft simplifie la tâche consistant à réaliser les évaluations des risques liés à l'utilisation des services en cloud Microsoft. Avec le Compliance Manager, les entreprises peuvent gérer leurs activités de conformité de l'implémentation au reporting et tenir la liste des mesures techniques et organisationnelles appropriées. Le Compliance Manager renvoie aussi au catalogue complet des certifications selon des normes et des rapports d'audit pour les services en cloud Microsoft, jusqu'à tous les contrôles/toutes les mesures de sécurité et donne ainsi au client un aperçu des contrôles que Microsoft a mis en œuvre en tant que sous-traitant de données conformément à la bonne pratique en vigueur ou à la norme choisie (ISO27001, PCI, FedRAMP, etc.).



<sup>74</sup> FN 16

<sup>75</sup> FN 16

<sup>76</sup> <https://azure.microsoft.com/fr-fr/industries/government/>

<sup>77</sup> <https://docs.microsoft.com/fr-ch/learn/azure/>

<sup>78</sup> <https://aka.ms/MSCloudTCO>

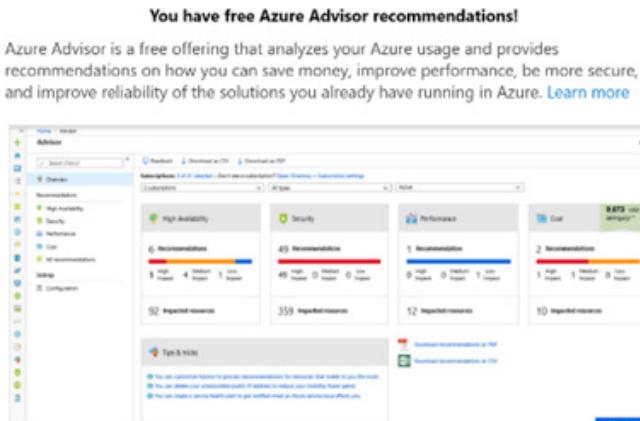
<sup>79</sup> <https://aka.ms/mscompliancemanager>

#### d. Optimisation de la mise en œuvre des services en cloud

Azure Advisor<sup>80</sup> est un conseiller personnel en matière de cloud, qui aide les clients à optimiser les mises en œuvre Azure en suivant les bonnes pratiques. Il analyse la configuration et l'utilisation des ressources et recommande ensuite des solutions qui peuvent contribuer à l'amélioration de la rentabilité, de la performance, de la disponibilité élevée et de la sécurité globale.

#### e. Surveillance et optimisation de la sécurité et de la conformité

Tableau de bord de sécurité et de conformité dans le Security Center<sup>81</sup>:



Via le «Secure Score»<sup>82</sup>, le tableau de bord donne un aperçu de la sécurité de la fourniture des services en cloud et des recommandations en matière de bonnes pratiques pour la priorisation qui suivra (voir question 10).

Pour Azure, le tableau de bord montre, par exemple, de fréquentes erreurs de configuration pour des ressources de l'infrastructure en tant que service (IaaS) et de la plateforme en tant que service (PaaS) Azure, comme des omissions lors de la mise en œuvre de mises à jour du système sur des machines virtuelles.

- Exposition inutile sur Internet par le biais des terminaux destinés au public.
- Données non cryptées lors du transfert ou du stockage.

Pour Microsoft 365, le respect des recommandations du Secure Score peut protéger les entreprises des menaces. Grâce à un tableau de bord centralisé dans le centre de sécurité Microsoft 365, des organisations peuvent travailler à l'amélioration de la sécurité de leurs applications, appareils et identités Microsoft 365. Secure Score aide les organisations à:

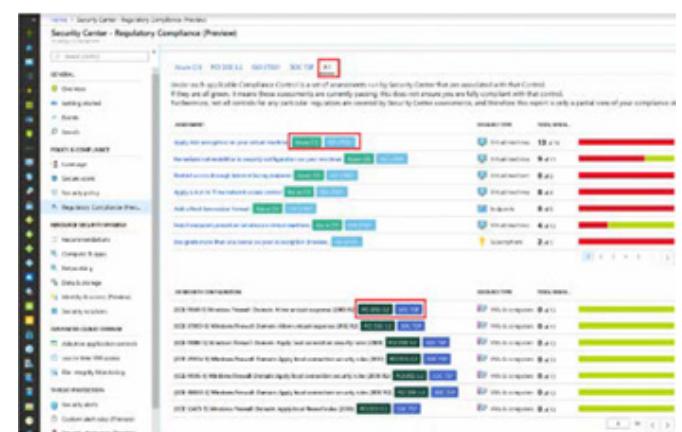
créer des rapports sur le niveau actuel de la sécurité de l'organisation.

améliorer leur niveau de sécurité en garantissant la visibilité, la transparence, l'orientation et le contrôle.

effectuer des comparaisons avec des référentiels et définir des indicateurs clés de performance.

Les organisations peuvent ainsi accéder à des visualisations de tendances et de métriques robustes, des intégrations avec d'autres produits Microsoft, des comparaisons avec des scores d'entreprises comparables, etc. Le score peut aussi être saisi quand des solutions de prestataires tiers ont mis en œuvre les mesures recommandées.

#### f. Conformité réglementaire



Le Compliance Center<sup>83</sup> M365 donne des informations détaillées sur la conformité globale<sup>84</sup>, sur la base d'évaluations permanentes de l'implémentation. Le Security Center analyse les facteurs de risques dans un environnement de cloud (potentiellement hybride également) conformément aux bonnes pratiques en matière de sécurité. Ces évaluations sont liées à la surveillance de la conformité selon une série de normes prises en charge. Le tableau de bord de la conformité indique le statut de toutes les évaluations par rapport à une norme donnée ou à une réglementation spécifique. Lorsque les recommandations<sup>85</sup> et les facteurs de risques dans la configuration sont réduits, la conformité globale est améliorée.

80 <https://aka.ms/msazureadvisor>

81 <https://aka.ms/AzureSecurityCenterDoc>

82 <https://aka.ms/m365SecureScore> et <https://aka.ms/AzureSecureScore>

83 <https://aka.ms/m365ComplianceCenter>

84 <https://aka.ms/MSComplianceDashboard>

85 <https://aka.ms/azuresccd>

Le Security Center peut également intégrer la gestion des paramétrages de la sécurité et la protection contre des menaces dans les implémentations avec d'autres fournisseurs de services en cloud et machines virtuelles dans l'environnement local, et préparer des Server Agents pour l'exécution dans l'environnement local/sur site. Il peut aussi établir une connexion avec des outils et processus existants, comme Security Information and Incident Management (SIEM) ou intégrer des solutions de sécurité de partenaires.

Azure Sentinel<sup>86</sup> étend les domaines de SIEM aux capacités d'un service en ligne. Par ailleurs, Sentinel comprend des fonctions d'orchestration automatisée de la sécurité pour fournir des analyses de sécurité intelligentes et des données concernant la menace dans l'ensemble de l'entreprise et offrir une solution unique pour la détection d'alarmes, la visibilité des menaces, la recherche proactive et la réaction aux menaces.

Collecte de données sur tous les utilisateurs, les appareils, les applications et les infrastructures, aussi bien sur site que dans plusieurs cloud.

Détection de menaces non identifiées jusqu'à-là et réduction au minimum des «False Positives» à l'aide de Microsoft Analytics et de Threat Intelligence.

Examen des menaces avec l'intelligence artificielle et recherche d'activités suspectées, en s'appuyant sur le travail effectué par Microsoft pendant de nombreuses années dans le domaine de la cybersécurité.

Réaction rapide aux incidents grâce à l'orchestration intégrée et à l'automatisation de tâches générales.

#### **g. Garantie d'une configuration et d'une implémentation optimales**

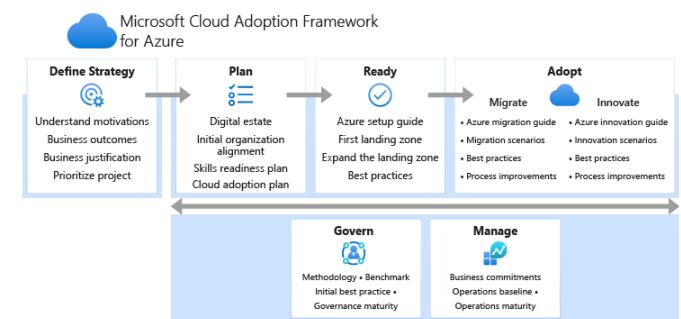


Les Azure Blueprints<sup>87</sup> et Azure Policy Blueprints<sup>88</sup> sont des ressources en cloud qui aident à créer et à lancer des applications en cloud, en tenant compte des règles, directives et normes définies par les responsables des données. Elles comprennent:

- Aperçu et guides spécifiques aux diverses branches.
- Matrice pour la responsabilité du client.
- Architectures de référence avec modèles de menaces.
- Contrôle des matrices d'implémentation.
- Automatisation pour l'implémentation d'architectures de référence.

Azure Policy est un service avec lequel des directives peuvent être créées, affectées et gérées. Ces directives imposent des règles sélectionnées pour les ressources utilisées dans la solution, afin que celles-ci correspondent aux normes de l'entreprise, aux exigences en matière de conformité et aux accords de niveau de service. Azure Policy répond à cette exigence en contrôlant que les ressources respectent bien les directives affectées. Par exemple, une directive peut établir que seule une certaine taille d'UGS est autorisée sur des machines virtuelles dans l'environnement. Dès que cette directive est mise en œuvre, la conformité des ressources, nouvelles et existantes, est évaluée pour garantir qu'elles respectent/sont conformes aux directives sélectionnées et aux normes de l'entreprise.

#### **h. Guide d'utilisation du cloud**



<sup>86</sup> Service: <https://aka.ms/AzureSentinel> et description: <https://aka.ms/MSAzureSentinel>

<sup>87</sup> <https://aka.ms/azureblueprints>

<sup>88</sup> <https://aka.ms/msazurepolicies>

Le cadre d'adoption du cloud informatique (Cloud Adoption Framework (CAF)<sup>89</sup> Microsoft est le guide de synthèse de Microsoft pour l'introduction et l'implémentation du cloud informatique. Le CAF consolide et partage des bonnes pratiques de Microsoft, de ses partenaires et de ses clients. Il offre une série d'outils et de documents explicatifs qui aident à créer des stratégies en matière de technologies, de business et de ressources et soutiennent ainsi les résultats souhaités par la société en utilisant le cloud informatique. Les documents explicatifs sont adaptés sur une série de phases du cycle de vie de l'implémentation du cloud et garantissent un accès aisément aux bons documents explicatifs au bon moment: stratégie, planification, préparation, migration, développement, gouvernance et exploitation.

Le Azure Migration Service<sup>90</sup> sert lors de l'évaluation, la planification, la migration, l'optimisation et la gestion de la migration vers l'environnement du cloud. Vous avez ici accès à tous les outils et ressources nécessaires<sup>91</sup> au rythme que vous souhaitez et sans soucis inutiles.

Pour ses partenaires, Microsoft propose également le Cloud Migration Playbook<sup>92</sup>, qui apporte une aide et des conseils pour la migration de workloads ou la modernisation d'anciennes applications/solutions en cloud Microsoft. Des guides semblables existent pour des domaines de solutions spécifiques comme AI, IoT, Operations, le développement d'applications en cloud, etc.

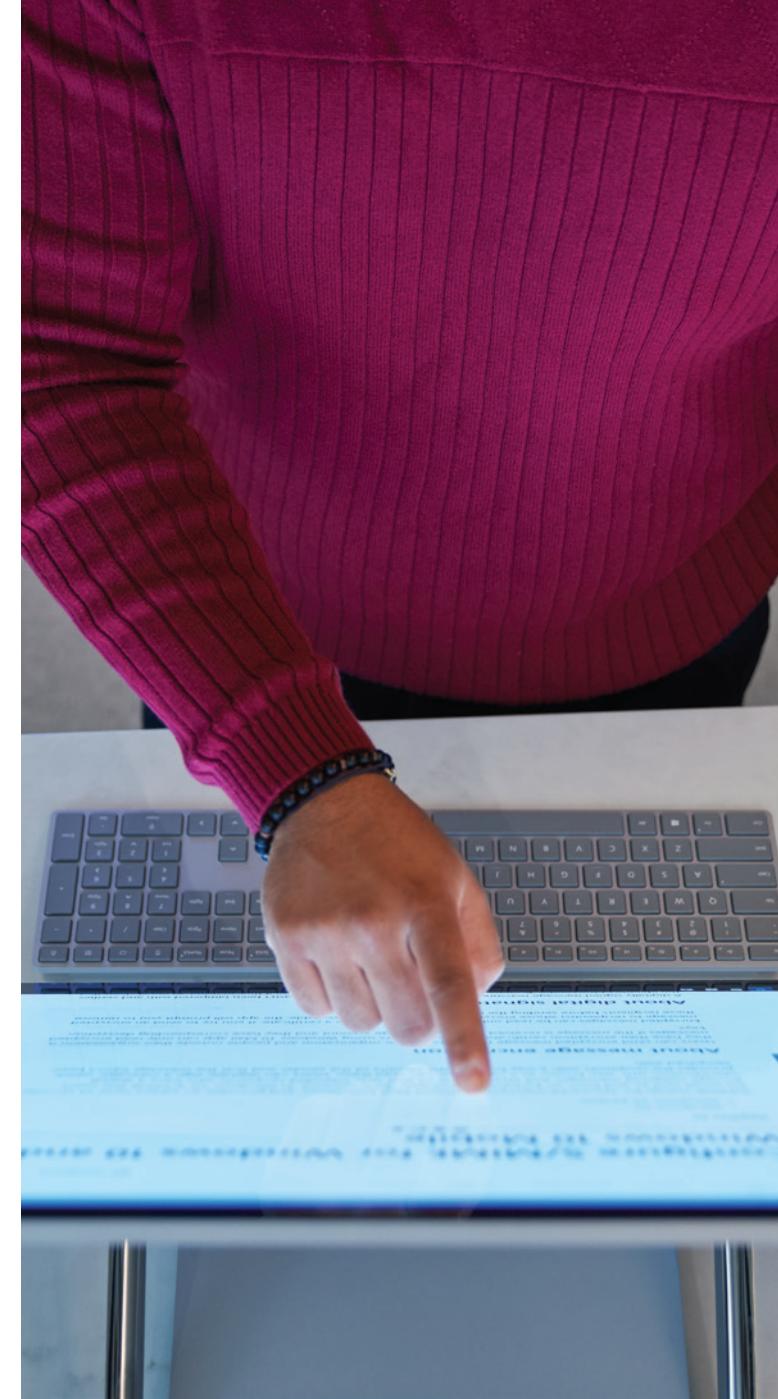
Les fonctions et solutions citées ci-dessus s'appliquent à tous les services en cloud Microsoft. Pour certains services, il existe des outils complémentaires qui donnent un aperçu et recommandent des mesures pour respecter les prescriptions et améliorer la sécurité générale. Par exemple pour la plateforme Microsoft 365:

Microsoft Secure Score: <https://aka.ms/m365secscore>

Office 365 Security & Compliance Center:  
<https://aka.ms/m365seccmplcenter>

### i. Insider Risk Management

L'Insider Risk Management<sup>93</sup> Microsoft 365 aide à réduire les risques internes au minimum en permettant aux clients d'identifier et d'examiner les activités malveillantes et involontaires dans leur propre entreprise et d'y réagir. Avec les directives concernant les risques internes, les types de risques qui doivent être identifiés et découverts au sein de l'entreprise peuvent être définis, y compris la réaction aux cas et la remontée des cas à Microsoft Advanced eDiscovery, si nécessaire. Les personnes chargées de l'analyse des risques dans l'entreprise peuvent ainsi prendre des mesures adaptées rapidement pour garantir que les utilisateurs respectent les normes de l'entreprise en matière de conformité.



<sup>89</sup> <https://aka.ms/MScaf>

<sup>90</sup> <https://aka.ms/azuremigrering>

<sup>91</sup> <https://aka.ms/azurermigrationtools>

<sup>92</sup> <https://assets.microsoft.com/en-us/mpn-playbook-cloud-migration.pdf>

<sup>93</sup> <https://aka.ms/M365InsiderRisk>

## IV. ANNEXE – RÉGLEMENTATIONS DANS LA CONFÉDÉRATION ET DANS LES CANTONS EN MATIÈRE DE PROTECTION DES DONNÉES

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Bund</b> Datenschutzverordnung (DSV) Direktionsverordnung über Informationsicherheit und Datenschutz (ISDS DV) Allgemeine Geschäftsbedingungen des Kantons Bern über die Informationsicherheit und den Datenschutz (ISDS) bei der Erbringung von Informatikdienstleistungen (AGB ISDS)	<a href="https://www.lexfind.ch/fe/de/tol/23528/versions/191742/de">https://www.lexfind.ch/fe/de/tol/23528/versions/191742/de</a> <a href="https://www.lexfind.ch/fe/de/tol/23528/versions/191742/de">https://www.lexfind.ch/fe/de/tol/23528/versions/191742/de</a> <a href="https://www.kaios.fin.be/v/content/dam/kaios/dokumente/de/startseite/themen/rechtliche-grundlagen/isdsv.pdf?la=de">https://www.kaios.fin.be/v/content/dam/kaios/dokumente/de/startseite/themen/rechtliche-grundlagen/isdsv.pdf?la=de</a>	<b>Art. 10a DSG Datenbearbeitung durch Dritte</b> 1 Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. 2 Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet. 3 Dritte können dieselben Rechtfertigungsgründe geltend machen wie der Auftraggeber.	<b>Art. 7 DSG Datensicherheit</b> 1 Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. 2 Der Bundesrat erlässt nähere Bestimmungen über die Mindestanforderungen an die Datensicherheit. <b>Art. 8 VDSG Technische und organisatorische Massnahmen – Allgemeine Massnahmen</b> 1 Wer als Privatperson Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten, um einen angemessenen Datenschutz zu gewährleisten. Insbesondere schützt er die Systeme gegen folgende Risiken: a. unbefugte oder zufällige Vernichtung; b. zufälligen Verlust; c. technische Fehler; d. Fälschung, Diebstahl oder widerrechtliche Verwendung; e. unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. 2 Die technischen und organisatorischen Massnahmen müssen angemessen sein. Insbesondere tragen sie folgenden Kriterien Rechnung: a. Zweck der Datenbearbeitung; b. Art und Umfang der Datenbearbeitung; c. Einschätzung der möglichen Risiken für die betroffenen Personen; d. gegenwärtiger Stand der Technik. 3 Diese Massnahmen sind periodisch zu überprüfen. <b>Art. 9 VDSG Technische und organisatorische Massnahmen – Besondere Massnahmen</b> 1 Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden: a. Zugangskontrolle: unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren; b. Personendatenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen; c. Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können; d. Bekanntgebotskontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können; e. Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern; f. Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern; g. Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen; h. Eingabekontrolle: in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden. 2 Die Datensammlungen sind so zu gestalten, dass die betroffenen Personen ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen können.	<b>Art. 6 DSG Grenzüberschreitende Bekanntgabe</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn: a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; b. die betroffene Person im Einzelfall eingewilligt hat; c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt; d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; g. die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten. 3 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Beauftragte, Art. 26) muss über die Garantien nach Absatz 2 Buchstabe a und die Datenschutzregeln nach Absatz 2 Buchstabe g informiert werden. Der Bundesrat regelt die Einzelheiten dieser Informationspflicht. <b>Art. 6 VDSG Informationspflicht</b> 1 Der Inhaber der Datensammlung informiert den Beauftragten vor der Bekanntgabe ins Ausland über die Garantien und Datenschutzregeln nach Artikel 6 Absatz 2 Buchstaben a und g DSG. Ist die vorgängige Information nicht möglich, so hat sie unmittelbar nach der Bekanntgabe zu erfolgen. 2 Wurde der Beauftragte über die Garantien und die Datenschutzregeln informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die: a. unter denselben Garantien erfolgen, soweit die Kategorien der Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfinden, soweit die Datenschutzregeln weiterhin einen angemessenen Schutz gewährleisten. 3 Die Informationspflicht gilt ebenfalls als erfüllt, wenn Daten gestützt auf Musterverträge oder Standardvertragsklauseln übermittelt werden, die vom Beauftragten erstellt oder anerkannt wurden, und die Beauftragte vom Inhaber der Datensammlung in allgemeiner Form über die Verwendung dieser Musterverträge oder Standardvertragsklauseln informiert wurde. Der Beauftragte veröffentlicht eine Liste der von ihm erstellten oder anerkannten Musterverträge und Standardvertragsklauseln. 4 Der Inhaber der Datensammlung trifft angemessene Massnahmen um sicherzustellen, dass der Empfänger die Garantien und die Datenschutzregeln beachtet. 5 Der Beauftragte prüft die Garantien und die Datenschutzregeln, die ihm mitgeteilt werden (Art. 31 Abs. 1 Bst. e DSG) und teilt dem Inhaber der Datensammlung das Ergebnis seiner Prüfung innerst 30 Tagen ab dem Empfang der Information mit. <b>Art. 7 VDSG Liste der Staaten mit angemessener Datenschutzgesetzgebung</b> Der Beauftragte veröffentlicht eine Liste der Staaten, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet.	<b>Art. 320 StGB Verletzung des Amtsgeheimnisses</b> 1. Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Die Verletzung des Amtsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses strafbar. 2. Der Täter ist nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde geoffenbart hat.

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Revidiertes Datenschutzgesetz</b> Bundesgesetz über den Datenschutz; Revision; Text gemäß Schlusabstimmung vom 25. September 2020 (revDSG) <a href="https://www.parlament.ch/centers/epeu/cuan/2017/20170059/Schlussabstimmungstext%20%20NS%20.pdf">https://www.parlament.ch/centers/epeu/cuan/2017/20170059/Schlussabstimmungstext%20%20NS%20.pdf</a>	<b>Art. 9 revDSG Bearbeitung durch Auftragsbearbeiter</b> 1 Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun durfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. 2 Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. 3 Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen. 4 Er kann dieseben Rechtfertigungsgründe geltend machen wie der Verantwortliche	<b>Art. 8 revDSG Datensicherheit</b> 1 Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Maßnahmen eine dem Risiko angemessene Datensicherheit. 2 Die Maßnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden. 3 Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	<b>Art. 16 revDSG – Bekanntgabe von Personendaten ins Ausland – Grundsätze</b> 1 Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet. 2 Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch: a. einen völkerrechtlichen Vertrag; b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden; c. spezifische Garantien, die das zuständige Bundesamt erarbeitet und dem EDÖB vorgängig mitgeteilt hat; d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder e. verbindliche unternehmensinterne Datenschutzzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden. 3 Der Bundesrat kann andere geeignete Garantien im Sinne von Absatz 2 vorsehen.	<b>Art. 17 revDSG – Bekanntgabe von Personendaten ins Ausland – Ausnahmen</b> 1 Abweichungen von Artikel 16 Absätze 1 und 2 dürfen in den folgenden Fällen Personendaten ins Ausland bekanntgegeben werden: a. Die betroffene Person hat ausdrücklich in die Bekanntgabe eingewilligt. b. Die Bekanntgabe steht im unmittelbaren Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags: 1. zwischen dem Verantwortlichen und der betroffenen Person, oder 2. zwischen dem Verantwortlichen und seiner Vertragspartnerin oder seinem Vertragspartner im Interesse der betroffenen Person. c. Die Bekanntgabe ist notwendig für: 1. die Wahrnehmung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde. d. Die Bekanntgabe ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen. e. Die betroffene Person hat die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt. f. Die Daten stammen aus einem gesetzlich vorgeesehenen Register, das öffentlich oder Personen mit einem schutzwürdigen Interesse zugänglich ist, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. 2 Der Verantwortliche oder der Auftragsbearbeiter informiert den EDÖB auf Anfrage über die Bekanntgabe von Personendaten nach Absatz 1 Buchstaben b Ziffer 2, c und d.	<b>DISPOSITIONS RELATIVES AU DROIT AU SECRET</b>

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Aargau</b> Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG)	<a href="https://www.legifind.ch/fc/de/tot/1371/de">https://www.legifind.ch/fc/de/tot/1371/de</a> <a href="https://www.legifind.ch/fc/de/tot/934/versions/193648/de">https://www.legifind.ch/fc/de/tot/934/versions/193648/de</a>	<b>§ 18 IDAG Datenbearbeitung im Auftrag</b> 1 Lasst ein öffentliches Organ Personendaten durch Dritte bearbeiten, stellt es den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicher. Insbesondere dürfen Auftragsdatenbearbeitende Bearbeitungen von Personendaten ohne vorgängige schriftliche Zustimmung des öffentlichen Organs keinen weiteren Auftragnehmenden übertragen. 2 Das öffentliche Organ bleibt für die Einhaltung des Datenschutzes verantwortlich. Die Rechte der Betroffenen sind ihm gegenüber geltend zu machen.	<b>§ 12a VIDAG Datenerarbeitung im Auftrag</b> 1 Auftragnehmende für die Bearbeitung von Personendaten sind vom öffentlichen Organ unter besonderer Berücksichtigung der von jenen getroffenen technischen und organisatorischen Massnahmen sorgfältig auszuwählen. Durch Vertrag oder Auflagen sind festzulegen: (...) g) Kontrollrechte des auftraggebenden öffentlichen Organs und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmenden; d) Durchsetzung von Ansprüchen betroffener Personen; e) Verpflichtung zur Verschwiegenheit und Überbindung dieser Pflicht auf alle Datenbearbeitenden; f) allfällige Berechtigung zur Vergabe von Unteraufträgen; g) Kontrollrechte des auftraggebenden öffentlichen Organs und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmenden; h) Mitteilungspflicht des Auftragnehmenden bei Verletzungen der Datensicherheit; i) Weisungsbefugnis des öffentlichen Organs; j) die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmenden gespeicherter Daten. 2 Stellt die Bearbeitung von Personendaten nicht die Hauptpflicht des Auftragnehmenden dar, haben sich die Vereinbarung oder die Auflagen sinngemäß am Inhalt gemäss Abs. 1 zu orientieren.	<b>§ 12 IDAG Datensicherheit</b> 1 Personendaten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. 2 Das verantwortliche öffentliche Organ ist verpflichtet, den Nachweis zu erbringen, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt die Einzelheiten durch Verordnung.  Konkretisierungen in § 4 f. VIDAG.	(ev. analoge Anwendung gewisser Regeln in § 14 Abs. 3 und 4 IDAG in der Praxis)
<b>Appenzell Ausserrhoden</b> Gesetz über den Datenschutz (DSGAR)	<a href="https://www.legifind.ch/fc/de/tot/2310/versions/8398/de">https://www.legifind.ch/fc/de/tot/2310/versions/8398/de</a>	<b>Art. 15 DSGAR Bearbeitung durch Drittpersonen</b> 1 Überträgt das Organ die Bearbeitung von Daten einer Drittperson, so stellt es den Datenschutz durch Auflagen, durch Vereinbarungen oder auf andere Weise sicher.	<b>Art. 16 DSGAR Datensicherheit</b> 1 Wer Daten bearbeitet, sichert sie durch technische und organisatorische Vorkehrungen vor Verlust, Entwendung sowie unbefugter Kenntnisnahme und Bearbeitung.	<b>Art. 13a DSGAR Bekanntgabe ins Ausland</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, nämlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn: a) hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; b) die betroffene Person im Einzelfall eingewilligt hat; c) die Bekanntgabe im Einzelfall für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; d) die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; e) die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	(ev. analoge Anwendung gewisser Regeln in Art. 16 DIAG (Bekanntgabe ins Ausland an öffentlich Organe) in der Praxis)
<b>Appenzell Innerrhoden</b> Datenschutz-, Informations- und Archivgesetz (DIAG)	<a href="https://www.legifind.ch/fc/de/tot/1199/versions/189794/de">https://www.legifind.ch/fc/de/tot/1199/versions/189794/de</a>	<b>Art. 6 DIAG Übertragung an Dritte</b> 1 Das Bearbeiten von Personendaten kann übertragen werden, wenn: a) dafür eine einschneidige oder schriftliche vereinbarte Regelung besteht, b) der Auftrag klar umschrieben ist und c) die Einhaltung der gesetzlichen Vorgaben durch geeignete Massnahmen sichergestellt ist. 2 Das beauftragende öffentliche Organ bleibt mitverantwortlich. Eine Weiterübertragung ist nur mit seiner schriftlichen Zustimmung möglich.	<b>Art. 9 DIAG Schutz und Verantwortung</b> 1 Personendaten sind durch technische und organisatorische Massnahmen angemessen gegen unbefugtes Bearbeiten zu schützen. 2 Für den Schutz und die Sicherheit von Daten ist das Organ verantwortlich, welches diese bearbeitet oder bearbeiten lässt. 3 Bearbeiten mehrere Organe einen gemeinsamen Datenbestand, trägt innerer Linie der Inhaber oder der Inhaberin des Bestandes die Verantwortung. Jedes Organ bleibt für seinen Bereich verantwortlich.		(ev. analoge Anwendung gewisser Regeln in Art. 16 DIAG (Bekanntgabe ins Ausland an öffentlich Organe) in der Praxis)

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Basel-Landschaft</b> Gesetz über die Information und den Datenschutz (IDGBL) Verordnung zum Gesetz über die Information und den Datenschutz (IDVBL) Verordnung über die Informationssicherheit (VISBL)	<a href="https://www.lexfind.ch/fe/tol/3003/versions/19590/de/">https://www.lexfind.ch/fe/tol/3003/versions/19590/de/</a> <a href="https://www.lexfind.ch/fe/tol/2999/versions/192396/de">https://www.lexfind.ch/fe/tol/2999/versions/192396/de</a> <a href="https://www.lexfind.ch/fe/tol/3788/versions/16289/de">https://www.lexfind.ch/fe/tol/3788/versions/16289/de</a>	<b>§ 7 IDGBL Bearbeiten im Auftrag</b> 1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn: a. keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und b. sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun durfte. 2 Das öffentliche Organ bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.	<b>§ 8 IDGBL Informations sicherheit</b> 1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen vor Verlust, Entwendung sowie unrechtmäßiger Bearbeitung und Kenntnisnahme. 2 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik. 3 Der Regierungsrat regelt das Nähere.  Konkretisierungen in § 1ff. IDVBL und VISBL.	<b>§ 21 IDGBL Grenzüberschreitende Bekanntgabe von Personendaten</b> 1 Öffentliche Organe dürfen Personendaten anderen Organen oder Privaten, die nicht der Rechts hoheit eines Staates unterstehen, der dem Europarat übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogene Daten beigetreten ist, nur bekannt geben, wenn: a. die Gesetzgebung des Empfängerstaates einen angemessenen Schutz gewährleistet; b. durch vertragliche Vereinbarungen ein angemessener Schutz garantiert wird; c. dies im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; oder d. im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf. 2 Vorbehalten bleiben die gesetzlichen Bestimmungen über den Austausch und die Weiterverarbeitung von Personendaten im Rahmen des Schengener Informationssystems (SIS).
<b>Basel-Stadt</b> Gesetz über die Information und den Datenschutz (IDGBS) Verordnung über die Information und den Datenschutz (IDVBS)	<a href="https://www.lexfind.ch/fe/tol/32090/versions/187180/de">https://www.lexfind.ch/fe/tol/32090/versions/187180/de</a> <a href="https://www.lexfind.ch/fe/tol/4772/versions/186723/de">https://www.lexfind.ch/fe/tol/4772/versions/186723/de</a>	<b>§ 7 IDGBS Bearbeiten im Auftrag</b> 1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn: a) keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und b) sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun durfte. 2 Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.	<b>§ 8 IDGBS Informations sicherheit</b> 1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen. 2 Die Massnahmen richten sich nach den folgenden Schutzzügen: a) Informationen dürfen nicht unrechtmäßig zur Kenntnis gelangen (Vertraulichkeit); b) Informationen müssen richtig und vollständig sein (Integrität); c) Informationen müssen bei Bedarf vorhanden sein (Zurechenbarkeit); d) Informationsbearbeitungen müssen einer Person zugerechnet werden können (Zurechenbarkeit); e) Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (Nachvollziehbarkeit). 3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik. 4 Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung.	<b>§ 23 IDGBS Grenzüberschreitende Bekanntgabe von Personendaten</b> 1 Öffentliche Organe dürfen Personendaten anderen Organen oder Privaten, die nicht der Rechts hoheit eines Staates oder einer Organisation unterstehen, welche dem Europarat übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogene Daten beigetreten sind, nur bekannt geben, wenn: a) die Gesetzgebung des Empfängerstaates einen angemessenen Schutz gewährleistet oder b) durch vertragliche Vereinbarungen ein angemessener Schutz garantiert wird oder c) dies im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; oder d) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf.
<b>Bern</b> Datenschutzgesetz (KDSG) Datenschutzverordnung (DSV) Direktionsverordnung über Informationssicherheit und Datenschutz (IDS DV) Allgemeine Geschäftsbedingungen des Kantons Bern über die Informationssicherheit und den Datenschutz (IDS) bei der Erbringung von Informatikdienstleistungen (AGB IDS)	<a href="https://www.lexfind.ch/fe/tol/22859/versions/191738/de">https://www.lexfind.ch/fe/tol/22859/versions/191738/de</a> <a href="https://www.lexfind.ch/fe/tol/23528/versions/191742/de">https://www.lexfind.ch/fe/tol/23528/versions/191742/de</a> <a href="https://www.bern.ch/de/lexfind/content/dam/ids/berne/mediathek/startseite/themen/rechtsgrundlagen/ids/1_AGB%20IDS%20IDS%20%2020.pdf">https://www.bern.ch/de/lexfind/content/dam/ids/berne/mediathek/startseite/themen/rechtsgrundlagen/ids/1_AGB%20IDS%20IDS%20%2020.pdf</a>	<b>Art. 16 KDSG Bearbeiten im Auftrag</b> 1 Wer Personendaten im Auftrag einer Behörde bearbeitet, untersteht dem Gesetz wie der Auftraggeber. Zur Bekanntgabe von Personendaten an Dritte bedarf der ausdrücklichen Zustimmung des Auftraggebers.	<b>Art. 17 KDSG Datensicherung</b> 1 Wer Personendaten bearbeitet, sorgt für ihre Sicherung.  Konkretisierungen in Art. 4 ff. DSV.	<b>§ 11 IDVBS Grenzüberschreitende Bekanntgabe von Personendaten</b> 1 Das öffentliche Organ kann für die Frage, ob die Gesetzgebung eines Empfängerstaates einen angemessenen Schutz im Sinne von § 23 Bst. a IDG gewährleistet, auf die vom Eidgenössischen Datenschutz- und Offenheitskeitsbeauftragten gestützte Art. 1 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz erläuterte Liste abstimmen. 2 Wer bei einer Datensicherung an eine Empfängerin oder einen Empfänger in einem Staat, dessen Gesetzgebung keinen angemessenen Schutz gewährleistet, der Schutz durch vertragliche Vereinbarungen im Sinne von § 23 Bst. b IDG garantiert werden soll, hat das öffentliche Organ die oder den Datenschutzbeauftragten vorab über die vereinbarten Sicherheitsvorkehrungen zu informieren.
				<b>Art. 14 KDSG d ins Ausland</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Trotz fehlender Gesetzgebung, die einen angemessenen Schutz gewährleistet, können Personendaten ins Ausland bekannt gegeben werden, wenn a hinreichende Garantie, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleistet, b die betroffene Person im Einzelfall eingewilligt hat, c die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt, d die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist, e die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen oder f die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten. 3 Die Aufsichtsstellen muss vor der Bekanntgabe der Personendaten ins Ausland rechtzeitig über die Garantien nach Absatz 2 Buchstabe a informiert werden.

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Freiburg</b> Gesetz über den Datenschutz (DSchG) E-Government-Gesetz <a href="https://www.legifind.ch/fe/fe/tol/4251/versions/2008086/de">https://www.legifind.ch/fe/fe/tol/4251/versions/2008086/de</a> <a href="https://www.legifind.ch/fe/fe/tol/33324/versions/2008074/de">https://www.legifind.ch/fe/fe/tol/33324/versions/2008074/de</a>	<b>Art. 12b DSchG Auslagerung – Grundsätze</b> 1 Die Bearbeitung personenbezogener Daten, einschliesslich besonders schützenswerter Daten, kann unter den in diesen Bestimmungen festgelegten Bedingungen ausgelagert werden. 2 Die Daten müssen jederzeit auf dem Gebiet der Schweiz oder auf dem Gebiet eines Staates, der einen gleichwertigen Datenschutz gewährleistet, bearbeitet werden. 3 Wenn die Auslagerung eine Delegation von Aufgaben an Dritte im Sinne von Artikel 54 der Kantonsverfassung vom 16. Mai 2004 zur Folge hat, gelten sondernde Anforderungen gemäss dieser Bestimmung. 4 Der Staatsrat unterbreitet der Finanz- und Geschärtsprüfungskommission alle zwei Jahre einen Bericht über die Auslagerung. <b>Art. 12c DSchG Auslagerung – Verantwortung [...]</b> <b>Art. 12d DSchG Auslagerung – Sicherheitsmaßnahmen [...]</b> <b>Art. 12e DSchG Auslagerung – Massnahmen für besonders schützenswerte Personendaten</b> 1 Das Bearbeiten von besonders schützenswerten Personendaten bei dem ein konkretes Risiko besteht, dass gegen das Recht der betroffenen Personen verstossen wird, und das Bearbeiten von Daten die einer gesetzlichen oder vertraglichen Gehältnispflicht unterliegen, darf dann ausgelagert werden, wenn die Vertraulichkeit gegenüber dem Auftragsbearbeiter sichergestellt ist, so dass dieser auf deren Inhalt keinen Zugriff hat. 2 Wenn der Auftragsbearbeiter aus technischen Gründen unbedingt Zugriff auf die Daten haben muss, werden im Auslagerungsvertrag die nötigen besonderen Anforderungen festgelegt, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklichem Einverständnis des öffentlichen Organs, welches die Daten auslagergt, auf den Inhalt der Daten zuzugreifen, und die Pflicht, ein Zugriffsjournal zu führen. <b>Art. 18 DSchG Verantwortung – Auftragsbearbeitung</b> 1 Das öffentliche Organ, das Personendaten von einem Auftragsbearbeiter bearbeiten lässt, bleibt für den Datenschutz verantwortlich. Es muss namentlich dem Auftragsbearbeiter die nötigen Weisungen geben und dafür sorgen, dass er die Daten nur für die Ausführung des Auftrags verwendet oder bekanntigt. 2 Ist dieses Gesetz auf die beauftragte Drittperson nicht anwendbar und gewährleisten keine anderen gesetzlichen Bestimmungen einen genügenden Datenschutz, so hat das öffentliche Organ den Datenschutz durch einen Vertrag sicherzustellen.	<b>Art. 12c DSchG Auslagerung – Verantwortung</b> 1 Das öffentliche Organ, das Daten auslagergt, bleibt für den Schutz der Personendaten, insbesondere für die Vertraulichkeit und die Kontinuität ihrer Aufbewahrung und Nutzung, verantwortlich. Insbesondere: [...] b) gewährleistet es den Schutz und die Sicherheit der Daten und deren eigenen Informationssysteme, indem sie einen Vertrag abschliesst, der mindestens Folgendes beschreibt: 1. den Gegenstand, die Art, den Zweck und die Dauer der Auslagerung; 2. die betroffenen Datenkategorien; 3. die Pflichten und Rechte jeder Partei; 4. die Rechte und die Kontrollmöglichkeiten der Aufsichtsbehörde im Bereich des Datenschutzes; 5. das an den Auftragsbearbeiter gerichtete Verbot, ohne vorherige Genehmigung des für die Datensammlung Verantwortlichen seinerseits einen weiteren Auftragsbearbeiter für die Bearbeitung zu beauftragen; 6. die Pflicht des Auftragsbearbeiters, den Verantwortlichen der Datensammlung unverzüglich zu informieren, wenn er aufgrund eines ausländischen Gesetzes oder einer richterlichen Entscheids die Daten einer ausländischen Behörde bekanntgeben muss oder Gefahr läuft, dass er es tun muss. [...] <b>Art. 12c DSchG Auslagerung – Sicherheitsmaßnahmen</b> 1 Die Universalität, die Authentizität, die Verfügbarkeit und die Vertraulichkeit der Personendaten, die von einer Auslagerung betroffen sind, sowie deren ständige Aufbewahrung und Verwendung müssen mit geeigneten organisatorischen und technischen Maßnahmen, die der Entwicklung der verfügbaren Technologien angepasst sind, sichergestellt werden. 2 Die Definition von Sicherheitsmaßnahmen berücksichtigt die Gefahren, die das Bearbeiten der fraglichen Daten für die Persönlichkeit und die Grundrechte der betroffenen Personen mit sich bringt. 3 Wenn die Auslagerung Daten betrifft, die für den Betrieb der Verwaltung unbedingt nötig sind, muss die Fortführung der ausgelagerten Tätigkeiten bei einem Zwischenfall mit einem angemessenen Dispositiv sichergestellt werden. <b>Art. 22 DSchG Organisatorische und technische Massnahmen</b> 1 Das öffentliche Organ, das Personendaten bearbeitet, muss die geeigneten organisatorischen und technischen Massnahmen treffen, um die Daten gegen jedes unerlaubte Bearbeiten zu schützen. 2 Der Staatsrat bestimmt die Mindestanforderungen in diesem Bereich. Er holt vorgängig die Stellungnahme der kantonalen Öffentlichkeits- und Datenschutzkommission ein.	<b>Art. 12a DSchG Bekanntgabe ins Ausland</b> 1 Personendaten dürfen nur in Staaten bekannt gegeben werden, die einen angemessenen Schutz gewährleisten. 2 In Staaten, die keinen angemessenen Schutz gewährleisten, dürfen Personendaten jedoch bekannt gegeben werden, wenn eine der folgenden Bedingungen erfüllt ist: a) Hinreichende Garantien, insbesondere vertragliche Garantien, gewährleisten einen angemessenen Schutz im Ausland. b) Die betroffene Person hat im Einzelfall ausdrücklich eingewilligt. c) Die Bearbeitung steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags und es handelt sich um Personendaten des Vertragspartners. d) Die Bekanntgabe ist im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich. e) Die Bekanntgabe ist im Einzelfall erforderlich, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen. 3 Vor der Bekanntgabe der Daten ins Ausland informiert das öffentliche Organ die kantone Datenschutzbeauftragte oder den kantonalen Datenschutzbeauftragten über die Garantien nach Absatz 2 Bst. a.	<b>Art. 28 E-GovG Wahren besonderer Geheimnisse</b> 1 Das Bearbeiten von Daten, für die eine gesetzliche oder vertragliche Geheimhaltungspflicht gilt, darf nur ausgelagert werden, wenn die Vertraulichkeit gegenüber dem Auftragsbearbeiter sichergestellt wird, so dass dieser keinen Zugriff auf ihren Inhalt hat. 2 Wenn der Auftragsbearbeiter aus technischen Gründen unbedingt Zugriff auf die Daten haben muss, werden im Auslagerungsvertrag die nötigen besonderen Anforderungen festgelegt, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklichem Einverständnis der Aufsichtsbehörde, welche die Daten auslagergt, auf den Inhalt zu zugreifen, und die Pflicht, ein Zugriffsjournal zu führen.	

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	DISPOSITIONS RELATIVES AU DROIT AU SECRET
				TRANSFERTS À L'ÉTRANGER
<b>Genève</b> Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD)  Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD)	<a href="https://www.legifind.ch/fe/tol/31380/">https://www.legifind.ch/fe/tol/31380/</a> <a href="https://www.legifind.ch/fe/tol/31889/">https://www.legifind.ch/fe/tol/31889/</a> <a href="https://www.legifind.ch/fe/tol/31889/">https://www.legifind.ch/fe/tol/31889/</a> <a href="https://www.legifind.ch/fe/tol/31889/">https://www.legifind.ch/fe/tol/31889/</a>	<b>Art. 13A) Sous-traitance (art. 37, al. 2, de la loi RIPAD)</b> 1 Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdisse. 2 L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même. 3 La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant. 4 Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article. 5 Si l'impose un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat. 6 Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat.	<b>Art. 13A(15) Sous-traitance (art. 37, al. 2, de la loi RIPAD [...])</b> 3 La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant. [...]	<b>Art. 37 LIPAD Sécurité des données personnelles</b> 1 Les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées. 2 Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter. 3 Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. Si l'implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.
<b>Glarus</b> Gesetz über den Schutz von Personendaten (DSGGL)  Datenschutzverordnung (DSVGL)	<a href="https://www.legifind.ch/fe/tol/6770/">https://www.legifind.ch/fe/tol/6770/</a> <a href="https://www.legifind.ch/fe/tol/7334/">https://www.legifind.ch/fe/tol/7334/</a> <a href="https://www.legifind.ch/fe/tol/7334/">https://www.legifind.ch/fe/tol/7334/</a>	<b>Art. 6 DSGGL Verantwortlichkeiten, Auslagerung, Strafbestimmung</b> [...] 2 Das Bearbeiten von Personendaten darf an Dritte ausgelagert werden, a. .... b. wenn das den Auftrag vergebende öffentliche Organ dafür sorgt, dass die Daten nur so bearbeitet werden, wie es ihm selbst erlaubt ist, und c. wenn keine Geheimhaltungspflichten entgegenstehen. 3 Die Einhaltung der Bestimmungen über den Datenschutz und die Datensicherheit seitens des beauftragten Dritten ist mittels Weisungen, Kontrollrechten, Auflagen, Vereinbarungen oder mit andern geeigneten Mitteln sicherzustellen. Der Beauftragte darf die zur Verfügung gestellten Personendaten nur dem Auftraggeber bekannt geben und nicht in eigenem Ermessen bearbeiten, unter Vorbehalt anderslautender Vereinbarung. 4 Wer als beauftragte Person für das Bearbeiten von Personendaten ohne anderslautende ausdrückliche Ermächtigung des auftraggebenden Organs Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Buße bestraft.	<b>Art. 6 DSGGL Verantwortlichkeiten, Auslagerung, Strafbestimmung</b> [...] 3 Die Einhaltung der Bestimmungen über den Datenschutz und die Datensicherheit seitens des beauftragten Dritten ist mittels Weisungen, Kontrollrechten, Auflagen, Vereinbarungen oder mit andern geeigneten Mitteln sicherzustellen. Der Beauftragte darf die zur Verfügung gestellten Personendaten nur dem Auftraggeber bekannt geben und nicht in eigenem Ermessen bearbeiten, unter Vorbehalt anderslautender Vereinbarung. 4 Wer als beauftragte Person für das Bearbeiten von Personendaten ohne anderslautende ausdrückliche Ermächtigung des auftraggebenden Organs Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Buße bestraft.	<b>Art. 8 DSGGL Datensicherheit</b> 1 Wer Personendaten bearbeitet, sorgt durch angemessene organisatorische und technische Vorkehrungen für ihre Sicherung vor Verlust sowie vor unbefugter Beeinträchtigung oder Kenntnisnahme. 2 Der Regierungsrat erlässt hinsichtlich einzelzahlernder Mindestanforderungen nach Anhörung insbesondere der mit der Informatik befassten Facheinheit sowie des Landesarchivs ausführende Vorschriften.  Konkretisierungen in Art. 1 ff. DSVGL.
<b>Graubünden</b> Kantonales Datenschutzgesetz (KDGS)	<a href="https://www.legifind.ch/fe/tol/9382/">https://www.legifind.ch/fe/tol/9382/</a> <a href="https://www.legifind.ch/fe/tol/49658/">https://www.legifind.ch/fe/tol/49658/</a>	<b>Art. 3 KDSG 2. Bekanntgabe in besonderen Fällen</b> 1 Entstehen Anstände zwischen zwei Behörden über die Bekanntgabe von Personendaten, so entscheidet die gemeinsame übergeordnete Instanz. 2 Wer Personendaten in Auftrag einer Behörde bearbeitet, bedarf zur Bekanntgabe von Personendaten an Dritte der ausdrücklichen Zustimmung des Auftraggebers.	<b>Art. 2 KDSG Bearbeiten von Personendaten 1. Grundsätze</b> 1 Das Bearbeiten von Personendaten hat die Grundsätze der Rechtmäßigkeit, der Verhältnismäßigkeit, der Zweckmäßigkeit, der Zweckgebundenheit, der Richtigkeit und der Datensicherheit zu beachten. 2 Die Vorschriften des Bundesgesetzes für das Bearbeiten von Personendaten durch Bundesorgane finden sinngemäss Anwendung. 3 Soweit das kantonale Datenschutzgesetz und die Ausführungsbestimmungen keine abweichenden oder ergänzenden Bestimmungen enthalten, gelten die Definitionen des Bundesgesetzes sinngemäss.	<b>Art. 39 LIPAD Communication</b> [...] <b>A une corporation ou un établissement de droit public étranger</b> 6 La communication de données personnelles à une corporation ou un établissement de droit public étranger n'est possible que si, cumulativement : a) l'entité requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait à des exigences légales assurant un niveau de protection de ces données équivalent aux garanties offertes par la présente loi; b) la communication des données considérées n'est pas contraire à une loi ou un règlement. 7 En l'absence du niveau de protection des données requis par l'alinéa précédent, la communication n'est possible que si elle n'est pas contraire à une loi ou un règlement et si, alternativement : a) elle intervient avec le consentement explicite, libre et éclairé de la personne concernée ou dans son intérêt manifeste; b) elle est dictée par un intérêt public important manifestement prépondérant reconnu par l'organe requis et que l'entité requérante fournit des garanties fiables suffisantes quant au respect des droits fondamentaux de la personne concernée; c) le droit fédéral ou un traité international le prévoit. [...]

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
Jura Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE)	<a href="https://www.legifind.ch/fc/fd/tot/933/versions/30443/fr">https://www.legifind.ch/fc/fd/tot/933/versions/30443/fr</a>	<b>Art. 54 CPDT-JUNE Communication transfrontière</b> 1 Le traitement de données ne peut être confié à un tiers qu'aux conditions suivantes: a) une base légale ou une convention avec le tiers le prévoit; b) le mandant ne peut confier que des traitements qu'il est lui-même en droit d'effectuer; c) aucune obligation légale ou contractuelle dégager le secret ne l'interdit; d) la sécurité des données est assurée. 2 Le mandant demeure responsable de la protection des données; il veille notamment à ce que ne soient pas effectués des traitements autres que ceux qu'il a confiés. 3 Le tiers est assujetti aux mêmes contrôles que le mandant.	<b>Art. 20 CPDT-JUNE Sécurité des données</b> 1 Les entités doivent s'assurer que les données sont protégées contre un emploi abusif en prenant des mesures organisationnelles et techniques appropriées. 2 Les entités veillent à l'intégrité, à la disponibilité et à la confidentialité des données.	<b>Art. 27 CPDT-JUNE Communication transfrontière</b> 1 Des données ne peuvent être communiquées à l'étranger que si les conditions requises par la législation fédérale sur la protection des données sont remplies. 2 Les entités informent le préposé des garanties prises en vertu de cette législation avant la communication de données.	
Luzern Gesetz über den Schutz von Personendaten (DSGLU) Informatikgesetz (IGLU) Verordnung zum Datenschutzgesetz (DSVLU) Verordnung über die Informatik Sicherheit und über die Nutzung von Informatikmitteln (VISLU)	<a href="https://www.legifind.ch/fc/fd/tot/1039/versions/18460/de">https://www.legifind.ch/fc/fd/tot/1039/versions/18460/de</a> <a href="https://www.legifind.ch/fc/fd/tot/10489/versions/55678/de">https://www.legifind.ch/fc/fd/tot/10489/versions/55678/de</a> <a href="https://www.legifind.ch/fc/fd/tot/1038/versions/42259/de">https://www.legifind.ch/fc/fd/tot/1038/versions/42259/de</a> <a href="https://www.legifind.ch/fc/fd/tot/1173/versions/62259/de">https://www.legifind.ch/fc/fd/tot/1173/versions/62259/de</a>	<b>§ 13 IGLU Auslagerung – Zulässigkeit</b> 1 Die Auslagerung von Informatikdienstleistungen ist zulässig, sofern die Vorschriften über den Datenschutz sowie die Bestimmungen dieses Gesetzes eingehalten werden. Die finanziellen Vorschriften bleiben vorbehalten. 2 Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt: a. Inhalt der Dienstleistung, b. Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten, c. Verantwortlichkeiten, d. verwendete Techniken, einschliesslich Entwicklung und Wartung, e. Zugriffs- und Zutrittsrechte, f. Sicherheits- und Datenlöschkonzept, g. Standorte der Hardware und der Datenbearbeitung, h. Kontrollrechte, i. Bezug von Dritten, j. Archivierung, k. Rückführung und Löschung der Daten im Fall der Vertragsauflösung. 3 Das auslagernde Organ stellt durch organisatorische oder technische Massnahmen sowohl vertraglich sicher, dass die staatliche Aufgabenerfüllung auch dann ohne wesentliche Beeinträchtigung gewährleistet ist, wenn der Auftragnehmer Abbrüche nicht einhält oder die Geschäftstätigkeit einstellt.	<b>§ 13 IGLU Zulässigkeit</b> 1 [...] 2 Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt: a. Inhalt der Dienstleistung, b. Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten, c. Verantwortlichkeiten, d. verwendete Techniken, einschliesslich Entwicklung und Wartung, e. Zugriffs- und Zutrittsrechte, f. Sicherheits- und Datenlöschkonzept, g. Standorte der Hardware und der Datenbearbeitung, h. Kontrollrechte, i. Bezug von Dritten, j. Archivierung, k. Rückführung und Löschung der Daten im Fall der Vertragsauflösung. 3 [...]	<b>§ 7 DSGLU Datensicherung</b> 1 Organe sorgen durch angemessene technische und organisatorische Massnahmen für die Sicherung von Personendaten. Sie sichern sie insbesondere vor Verlust, Fälschung, Entwendung sowie vor Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte. 2 Der Regierungsrat kann weitere Vorschriften erlassen.  Konkretisierung in § 6 DSVLU.  Siehe auch § 13 Abs. 3 IGLU; § 12 ff. V VISLU	<b>§ 12a DSGLU Grenzüberschreitende Bekanntgabe</b> 1 Personendaten dürfen nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, nämlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, können persönliche Daten nur ins Ausland bekanntgegeben werden, wenn a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten, b. die betroffene Person im Einzelfall eingewilligt hat, c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages steht und es sich um Personendaten des Vertragspartners handelt, d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist, e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen, f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. 3 Der Beauftragte für den Datenschutz muss über die Garantien nach Absatz 2a informiert werden. Der Regierungsrat regelt das Nähere.

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Neuchâtel</b> Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE)	<a href="https://www.legifind.ch/fc/de/tot/9531/versions/50445/fr">https://www.legifind.ch/fc/de/tot/9531/versions/50445/fr</a>	<b>Art. 54 CPDT-JUNE Communication transfrontière</b> 1 Le traitement de données ne peut être confié à un tiers qu'aux conditions suivantes: a) une base légale ou une convention avec le tiers le prévoit; b) le mandant ne peut confier que des traitements qu'il est lui-même en droit d'effectuer; c) aucune obligation légale ou contractuelle dégager le secret ne l'interdit; d) la sécurité des données est assurée. 2 Le mandant demeure responsable de la protection des données; il veille notamment à ce que ne soient pas effectués des traitements autres que ceux qu'il a confiés. 3 Le tiers est assujetti aux mêmes contrôles que le mandant.	<b>Art. 20 CPDT-JUNE Sécurité des données</b> 1 Les entités doivent s'assurer que les données sont protégées contre un emploi abusif en prenant des mesures organisationnelles et techniques appropriées. 2 Les entités veillent à l'intégrité, à la disponibilité et à la confidentialité des données.	<b>Art. 27 CPDT-JUNE Communication transfrontière</b> 1 Des données ne peuvent être communiquées à l'étranger que si les conditions requises par la législation fédérale sur la protection des données sont remplies. 2 Les entités informer le préposé des garanties prises en vertu de cette législation avant la communication de données.	
<b>Nidwalden</b> Gesetz über den Datenschutz (kDSG)	<a href="https://www.legifind.ch/fc/de/tot/13410/versions/68708/de">https://www.legifind.ch/fc/de/tot/13410/versions/68708/de</a>	<b>Art. 9 kDSG Datenbearbeitung durch Dritte</b> 1 Die Datenbearbeitung kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn: 1. die Daten nur so bearbeitet werden, wie die Auftraggeberin oder der Auftraggeber selbst es tun dürfte; 2. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. 2 Die Auftraggeberin oder der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.	<b>Art. 7 kDSG Datensicherheit</b> 1 Daten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugte Bearbeitung geschützt werden. 2 Der Regierungsrat erlässt Vorschriften über die Mindestanforderungen an die Datensicherheit.	<b>Art. 6 kDSG Bekanntgabe ins Ausland</b> 1 Daten dürfen nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen am gemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, können Daten ins Ausland nur bekanntgegeben werden, wenn: 1. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; 2. die betroffene Person im Einzelfall zugestimmt hat; 3. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist. 4. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; 5. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. 3 Die Aufsichtsstelle muss über die Garantien nach Abs. 2 Ziff. 1 informiert werden.	
<b>Obwalden</b> Gesetz über den Datenschutz (DSGOW)	<a href="https://www.legifind.ch/fc/de/tot/13721/versions/69832/de">https://www.legifind.ch/fc/de/tot/13721/versions/69832/de</a>	Keine Angaben im DSGOW. Deshalb gelten sinngemäss die Vorschriften des Bundesgesetzes über den Datenschutz (Art. 2 Abs. 1 DSGOW).	<b>Art. 13 DSGH Bearbeiten im Auftrag</b> 1 Beauftragt das verantwortliche Organ ein anderes öffentliches Organ oder Dritte mit dem Bearbeiten von Personendaten, ist der Datenschutz durch Vereinbarung, Auflagen oder auf andere Weise sicherzustellen. 2 Ohne ausdrückliche anderslautende Ermächtigung darf die beauftragte Stelle Personendaten nur für den Auftraggeber verwenden und nur diesem bekanntgeben.	<b>Art. 14 DSGSH Datensicherung</b> Personendaten sind durch angemessene technische und organisatorische Massnahmen vor Verlust, Entwendung und unbefugtem Bearbeiten zu schützen.	<b>Art. 11b DSGSH Bekanntgabe von Personendaten an Drittstaaten</b> 1 An Drittstaaten dürfen Personendaten unter Vorbehalt von Art. 8 ff. nur bekannt gegeben werden, sofern diese ein angemessenes Datenschutzniveau gemäss Art. 2 Ziff. 2 des Zusatzprotokolls des Europarates vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (SEV Nr. 108) gewährleisten. 2 Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die für die Datenübermittlung von Bedeutung sind. 3 Gewährleistet ein Drittstaat kein angemessenes Datenschutzniveau, so können ihm Personendaten im Einzelfall bekannt gegeben werden, wenn: a) die betroffene Person ohne jeden Zweifel eingewilligt hat; handelt es sich um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, so muss die Einwilligung ausdrücklich sein; b) die Bekanntgabe erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; oder c) die Bekanntgabe zur Wahrung überwiegender öffentlicher Interessen oder zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist. 4 Die Übermittlung unterbleibt, soweit Grund zur Annahme besteht, dass sie gegen die schweizerische Rechtsordnung verstossen würde oder die Übermittlung der ordre public widerspricht. 5 Personendaten können bekannt gegeben werden, wenn im Einzelfall hinreichende vertragliche Garantien einen angemessenen Schutz der betroffenen Person gewährleisten.
<b>Schaffhausen</b> Gesetz über den Schutz von Personendaten (DSGSH) Verordnung über den Schutz von Personendaten (DSVSH)	<a href="https://www.legifind.ch/fc/de/tot/14095/versions/7121/de">https://www.legifind.ch/fc/de/tot/14095/versions/7121/de</a> <a href="https://www.legifind.ch/fc/de/tot/14084/versions/7112/de">https://www.legifind.ch/fc/de/tot/14084/versions/7112/de</a>	<b>Art. 13 DSGH Bearbeiten im Auftrag</b> 1 Beauftragt das verantwortliche Organ ein anderes öffentliches Organ oder Dritte mit dem Bearbeiten von Personendaten, ist der Datenschutz durch Vereinbarung, Auflagen oder auf andere Weise sicherzustellen. 2 Ohne ausdrückliche anderslautende Ermächtigung darf die beauftragte Stelle Personendaten nur für den Auftraggeber verwenden und nur diesem bekanntgeben.	<b>§ 3 DSVSH Datensicherung – Allgemeine Massnahmen</b> Das verantwortliche Organ hat eine angemessene Datensicherung zu gewährleisten und Personendaten insbesondere vor folgenden Gefahren zu schützen: a) unbefugte oder zufällige Vernichtung; b) zufälliger Verlust; c) technische Fehler; d) Fälschung, Diebstahl oder widerrechtliche Verwendung; e) unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. 2 Die technischen und organisatorischen Massnahmen müssen verhältnismässig sein und periodisch überprüft werden. 3 Sie tragen insbesondere folgenden Kriterien Rechnung: a) Zweck der Datenbearbeitung; b) Art und Umfang der Datenbearbeitung; c) mögliche Gefährdung der Persönlichkeitrechte betroffener Personen; d) Stand der Technik.	<b>§ 4 DSVSH Besondere Massnahmen</b> Das verantwortliche Organ trifft namentlich bei der automatisierten Bearbeitung von Personendaten die geeigneten technischen und organisatorischen Massnahmen, um folgende Ziele zu erreichen: a) Zugangskontrolle: Unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren; b) Benutzerkontrolle: Unbefugten Personen ist die Benutzung von Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren; c) Datenträgerkontrolle: Unbefugten Personen ist das Lesen, Kopieren, Verändern, Zerstören oder Entfernen von Personendatenträgern zu verunmöglichen; d) Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf die Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgaben benötigen; e) Empfängeridentifikation: Empfängerinnen und Empfänger von bekanntzugebenden Personendaten müssen identifiziert werden können.	

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Schwyz</b> Gesetz über die Öffentlichkeit der Verwaltung und den Datenschutz (ÖDSG) Verordnung zum Öffentlichkeits- und Datenschutzgesetz (ÖDSV) Verordnung über die Informations- und Kommunikations-Technologie (IKTV)	<a href="https://www.legifind.ch/fe/de/tot/16395/versions/193501/de">https://www.legifind.ch/fe/de/tot/16395/versions/193501/de</a> <a href="https://www.legifind.ch/fe/de/tot/17469/versions/65893/de">https://www.legifind.ch/fe/de/tot/17469/versions/65893/de</a> <a href="https://www.legifind.ch/fe/de/tot/17544/versions/188692/de">https://www.legifind.ch/fe/de/tot/17544/versions/188692/de</a>	<b>§ 20 ÖDSG Besondere Formen der Datenbearbeitung – durch Dritte</b> 1 Lässt ein öffentliches Organ Personendaten durch Dritte bearbeiten, stellt es durch Vereinbarung oder in anderer verbindlicher Weise wirksam sicher, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ tun durfte. Der Regierungsrat regelt die Einzelheiten. 2 Der beauftragte Dritte darf die Personendaten nur im Unterauftragsverhältnis bearbeiten lassen, wenn das öffentliche Organ: a) vorgängig seine schriftliche Zustimmung erteilt hat; b) die Einhaltung der Datenschutzpflichten uneingeschränkt einfordert kann; c) seine Kontrollrechte ungehindert ausüben kann. 3 Die Verantwortung für die Datenbearbeitung nach diesem Gesetz bleibt beim öffentlichen Organ. Betroffene Personen haben ihre Rechte gegenüber dem öffentlichen Organ geltend zu machen.	<b>§ 20 ÖDSG Besondere Formen der Datenbearbeitung – durch Dritte</b> 1 Lässt ein öffentliches Organ Personendaten durch Dritte bearbeiten, stellt es durch Vereinbarung oder in anderer verbindlicher Weise wirksam sicher, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ tun darf. Der Regierungsrat regelt die Einzelheiten. 2 Der beauftragte Dritte darf die Personendaten nur im Unterauftragsverhältnis bearbeiten lassen, wenn das öffentliche Organ: a) vorgängig seine schriftliche Zustimmung erteilt hat; b) die Einhaltung der Datenschutzpflichten uneingeschränkt einfordert kann; c) seine Kontrollrechte ungehindert ausüben kann. 3 Die Verantwortung für die Datenbearbeitung nach diesem Gesetz bleibt beim öffentlichen Organ. Betroffene Personen haben ihre Rechte gegenüber dem öffentlichen Organ geltend zu machen.	<b>§ 18 ÖDSG Bekanntgabe ins Ausland</b> Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.	Siehe § 30 Abs. 2 lit. b) IKTV
<b>Solothurn</b> Informations- und Datenschutzgesetz (InfoDG) Informations- und Datenschutzverordnung (InfoDV) Allgemeine Geschäftsbedingungen des Kantons Solothurn über die Informationssicherheit und den Datenschutz bei der Erbringung von Informatiokndienstleistungen (AGB ISDS)	<a href="https://www.legifind.ch/fe/de/tot/15899/versions/79057/de">https://www.legifind.ch/fe/de/tot/15899/versions/79057/de</a> <a href="https://www.legifind.ch/fe/de/tot/15873/versions/79698/de">https://www.legifind.ch/fe/de/tot/15873/versions/79698/de</a> <a href="https://solothurn.ch/hinweise-daten-schutz/">https://solothurn.ch/hinweise-daten-schutz/</a> <a href="https://solothurn.ch/lehrgang-daten-schutz/">https://solothurn.ch/lehrgang-daten-schutz/</a> <a href="https://solothurn.ch/lehrgang-daten-schutz-2022/">https://solothurn.ch/lehrgang-daten-schutz-2022/</a> <a href="https://solothurn.ch/lehrgang-daten-schutz-2023/">https://solothurn.ch/lehrgang-daten-schutz-2023/</a> <a href="https://solothurn.ch/lehrgang-daten-schutz-2024/">https://solothurn.ch/lehrgang-daten-schutz-2024/</a>	<b>§ 17 InfoDG Datenbearbeiten durch Dritte</b> 1 Lässt eine Behörde Personendaten durch Dritte bearbeiten, stellt sie den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicher.	<b>§ 16 InfoDG Grundsätze</b> 1 Wer Personendaten bearbeitet, a) [...] b) [...] c) schützt die Daten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten. 2 [...] 3 [...]	<b>§ 12 InfoDV Datensicherheit – Technische und organisatorische Massnahmen</b> 1 Technische und organisatorische Massnahmen (§ 16 Abs. 1 lit. c InfoDG) sind insbesondere gegen folgende Risiken zu treffen: a) unbefugte oder zufällige Vernichtung; b) zufälligen Verlust; c) technische Fehler; d) Fälschung, Diebstahl, widerrechtliche Verwendung; e) unbefugtes Ändern, Kopieren, Zugreifen. 2 Die Massnahmen richten sich nach dem Zweck, der Art und dem Umfang der Datenbearbeitung sowie den möglichen Gefahren für die Persönlichkeitrechte betroffener Personen. Sie entsprechen dem Stand der Technik und müssen periodisch auf ihre Zweck- und Verhältnismäßigkeit überprüft werden.	<b>§ 21bis InfoDG Grenzüberschreitende Bekanntgabe</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet wird, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn: a) hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten; b) die betroffene Person im Einzelfall eingewilligt hat; c) die Bekanntgabe im Einzelfall entweder für die Wahrung eines wichtigen öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist; d) die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; e) die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>St. Gallen</b> Datenschutzgesetz (DSG) Verordnung über die Informatik Sicherheit (VI)	<a href="https://www.legifind.ch/fe/tde/tol/16372/versions/83364/de/">https://www.legifind.ch/fe/tde/tol/16372/versions/83364/de/</a> <a href="https://www.legifind.ch/fe/tde/tol/15457/versions/185092/de">https://www.legifind.ch/fe/tde/tol/15457/versions/185092/de</a>	<b>Art. 9 DSG Bearbeitung durch Dritte</b> 1 Das öffentliche Organ kann die Bearbeitung von Personendaten an Dritte übertragen, wenn die Übertragung nicht durch Gesetz oder Verordnung ausgeschlossen ist und die beauftragten Dritten Gewähr für die datenschutzrechtlich einwandfreie Bearbeitung bieten. 2 Es stellt die Einhaltung des Datenschutzes sicher und legt insbesondere fest, dass die Personendaten: a) nur so bearbeitet werden, wie das öffentliche Organ es selbst tun dürfte; b) nach den für das öffentliche Organ geltenden gesetzlichen Bestimmungen bearbeitet werden; c) vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten gesichert werden. 3 Es prüft durch geeignete regelmäßige Kontrollen, ob der Datenschutz eingehalten wird. Stellt es die Nichteinhaltung von Auflagen nach Abs. 2 dieser Bestimmung oder Verstöße gegen andere Datenschutzvorschriften fest, macht es die Übertragung rückgängig. 4 Die Weiterübertragung der Datenbearbeitung bedarf der vorgängigen schriftlichen Zustimmung des auftraggebenden öffentlichen Organs.	<b>Art. 9 DSG Bearbeitung durch Dritte</b> 1 [...] 2 [...] 3 Es [das öffentliche Organ] trifft organisatorische und technische Massnahmen zur Sicherung der Daten vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten.  Konkretisierungen in VI.	<b>Art. 16 DSG Bekanntgabe ins Ausland</b> 1 Die Bekanntgabe von Personendaten ins Ausland richtet sich sachgemäß nach den Bestimmungen der Bundesgesetzgebung über den Datenschutz. 2 Das öffentliche Organ informiert vor der Bekanntgabe die zuständige Fachstelle für Datenschutz über die von der Bundesgesetzgebung geforderten Garantien, wenn der Staat nicht auf der von der oder vom eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten veröffentlichten Liste der Staaten mit angemessener Datenschutzgesetzgebung aufgeführt ist. 3 Die kantonale Fachstelle für Datenschutz beschafft bei der oder beim eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten Informationen über den Datenschutz im Ausland. Sie stellt die Informationen zur Verfügung: a) den öffentlichen Organen in ihrem Zuständigkeitsbereich; b) den Fachstellen der Gemeinden zur Weiterleitung an die öffentlichen Organe in deren Zuständigkeitsbereich.	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Tessin</b> Legge sulla protezione dei dati personali (LPDP) Regolamento di applicazione alla legge cantonale sulla protezione dei dati personali (RLPDP)	<a href="https://www.legifind.ch/fe/tde/tol/21501/versions/718492/de/">https://www.legifind.ch/fe/tde/tol/21501/versions/718492/de/</a> <a href="https://www.legifind.ch/fe/tde/tol/21427/versions/11791/de">https://www.legifind.ch/fe/tde/tol/21427/versions/11791/de</a>	<b>Art. 16 LPDP Elaborazione su mandato</b> 1 Se l'organo responsabile incarica un altro organo pubblico o terzi di elaborare dati personali, la protezione dei dati secondo la presente legge deve essere garantita da condizioni, convenzioni o in altro modo. 2 Senza esplicita autorizzazione derogante, il servizio mandatario può utilizzare dati personali soltanto per il mandante e trasmetterli solo a quest'ultimo.	<b>Art. 17 LPDP Sicurezza</b> Chi elabora dati personali deve prendere misure appropriate di sicurezza contro la perdita, il furto, l'elaborazione e la consultazione illecita.	<b>Art. 14a LPDP Trasmissione all'estero</b> 1 I dati personali non possono essere trasmessi all'estero qualora la personalità della persona interessata possa subire grave pregiudizio, dovuto in particolare all'assenza di una legislazione che assicuri una protezione adeguata. 2 Se manca una legislazione che assicuri una protezione adeguata, dati personali possono essere trasmessi all'estero soltanto se: a) garanzie sufficienti, segnatamente contrattuali, assicurano una protezione adeguata all'estero; b) la persona interessata ha dato il suo consenso nel caso specifico; c) nel caso specifico la trasmissione è indispensabile per tutelare un interesse pubblico pregevolissimo oppure per accettare, esercitare o far valere un diritto in giustizia; d) nel caso specifico la trasmissione è necessaria per proteggere la vita o l'incolumità fisica della persona interessata; e) la persona interessata ha reso i dati accessibili a chiunque e non si è opposta formalmente alla loro elaborazione. 3 L'organo responsabile informa l'incaricato cantonale della protezione dei dati sulle garanzie ai sensi del capoverso 2 lettera a). Il Consiglio di Stato disciplina i particolari. 4 Laddove una protezione adeguata sia assicurata, la trasmissione è lecita se sono adempiute le condizioni valide per la trasmissione di dati in Svizzera.	<b>Art. 12a RLPD Obligo di trasmissione</b> 1 L'organo responsabile che intende trasmettere dati personali all'estero deve rispettare i principi generali della LPDP e accertarsi preventivamente della adeguatezza della protezione dei dati nello Stato di destinazione. 2 Prima della trasmissione all'estero, esso informa l'incaricato sulle garanzie e sulle regole di protezione dei dati ai sensi dell'art. 14a cpv. 2 lett. a LPDP. 3 L'obbligo di informare è considerato adempiuto se i dati sono trasmessi mediante contratto modello o clausole standard allestite o riconosciuti dall'incaricato e se l'organo responsabile informa in modo generale l'incaricato dell'utilizzo di tali contratti modello o clausole standard. 4 L'incaricato pubblica un elenco di tali contratti modello o clausole standard. 5 L'organo responsabile può applicare anche altre garanzie, quali una concezione specifica di protezione dei dati o clausole contenute in altri contratti; queste garanzie speciali devono assicurare un livello di protezione adeguato. 6 L'organo responsabile prende misure adeguate per garantire che il destinatario rispetti le garanzie e le regole sulla protezione dei dati. 7 L'incaricato esamina le garanzie e le regole sulla protezione dei dati che gli sono state comunicate (art. 14 cpv. 2 LPDP) e comunica il risultato del suo esame all'organo responsabile entro 30 giorni dalla ricezione dell'informazione.

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Thurgau</b> Gesetz über den Datenschutz (DSG) Verordnung des Regierungsrates über den Datenschutz (DSV) Informatikreglement (ITR)	<a href="https://www.legifind.ch/fe/tol/17654/versions/192915/de/">https://www.legifind.ch/fe/tol/17654/versions/192915/de/</a> <a href="https://www.legifind.ch/fe/tol/17907/versions/184579/de/">https://www.legifind.ch/fe/tol/17907/versions/184579/de/</a> <a href="https://www.legifind.ch/fe/tol/18444/versions/201883/de/">https://www.legifind.ch/fe/tol/18444/versions/201883/de/</a>		<p><b>§ 12 DSG Bearbeitung durch Dritte</b></p> <p>1 Werden Personendaten durch Dritte bearbeitet, ist der Datenschutz im Sinne dieses Gesetzes vom verantwortlichen Organ durch Vertrag oder Verfügung sicherzustellen.</p> <p>2 Ohne ausdrückliche Ermächtigung darf der Dritte Personendaten nur für das verantwortliche Organ verwenden und nur diesem bekanntgeben.</p> <p><b>§ 13 DSG Datensicherung</b></p> <p>1 Wer Personendaten bearbeitet, sorgt für deren angemessene Sicherung vor Verlust, Entwendung, unbefugter Bearbeitung oder Kenntnisnahme.</p> <p><b>§ 12 DSV Massnahmen</b></p> <p>1 Das verantwortliche Organ hat eine angemessene Datensicherheit zu gewährleisten und trifft Massnahmen zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, Datenexistenz und Nachvollziehbarkeit.</p> <p>2 Personendaten sind vor folgenden Gefahren zu schützen:</p> <ol style="list-style-type: none"> <li>1. unbefugte Vernichtung;</li> <li>2. zufälliger Verlust;</li> <li>3. technische Fehler;</li> <li>4. Fälschung, Diebstahl oder widerrechtliche Verwendung;</li> <li>5. unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.</li> </ol> <p>3 Die technischen und organisatorischen Massnahmen müssen angemessen sein. Insbesondere haben sie folgenden Kriterien Rechnung zu tragen:</p> <ol style="list-style-type: none"> <li>1. Zweck der Datenbearbeitung;</li> <li>2. Art und Umfang der Datenbearbeitung;</li> <li>3. Einschätzung der möglichen Risiken für die betroffenen Personen;</li> <li>4. aktueller Stand der Technik.</li> </ol> <p>4 Die Massnahmen sind von der Aufsichtsstelle periodisch zu überprüfen</p>		<p><b>§ 9a DSG Grenzüberschreitender Datenverkehr</b></p> <p>1 Personendaten dürfen an Empfänger, welche der Rechtshoheit von Staaten oder Organisationen unterliegen, die nicht Vertragspartie des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogene Daten sind, nur übermittelt werden, wenn diese Staaten oder Organisationen einen angemessenen Schutz für die beabsichtigte Datenübermittlung bieten.</p> <p>2 Vorbehalten bleiben die Zustimmung der betroffenen Person im Einzelfall und Artikel 2 Absatz 2 des Zusatzprotokolls vom 8. November 2001 zum Abkommen gemass Absatz 1.</p> <p><b>§ 3 DSV Angemessener Datenschutz</b></p> <p>1 Ein angemessener Datenschutz im grenzüberschreitenden Datenverkehr ist dann gegeben, wenn im Empfängerstaat ein adäquates Datenschutzniveau sichergestellt ist.</p> <p>2 Ein solches liegt unter Berücksichtigung aller Umstände insbesondere dann vor, wenn:</p> <ol style="list-style-type: none"> <li>1. die Grund- und Menschenrechte eingehalten werden;</li> <li>2. das Datenschutzniveau europäischen Standard entspricht.</li> </ol>
<b>Uri</b> Gesetz über den Schutz von Personendaten (DSG)	<a href="https://www.legifind.ch/fe/tol/17774/versions/87634/de/">https://www.legifind.ch/fe/tol/17774/versions/87634/de/</a>		<p><b>Artikel 11 DSG Datensicherung</b></p> <p>Wer Personendaten bearbeitet, sorgt für ihre Sicherung vor Verlust, Entwendung, unbefugter Bearbeitung oder Kenntnisnahme.</p>		<p><b>Artikel 8a DSG Bekanntgabe von Personendaten ins Ausland</b></p> <p>1 Personendaten dürfen ausländischen Stellen der Europäischen Union sowie Vertragsstaaten des Abkommens über den europäischen Wirtschaftsraum bekannt gegeben werden, wenn die Voraussetzungen erfüllt sind, die für die Bekanntgabe von Daten im Inland erfüllt sein müssen.</p> <p>2 Drittstaaten dürfen Personendaten nur bekannt gegeben werden, wenn zusätzlich zu den Voraussetzungen nach Absatz 1 feststeht, dass dadurch die Persönlichkeit der betroffenen Person nicht schwerwiegend gefährdet wird. Namentlich muss die Gesetzgebung des ersuchenden Drittstaats einen Datenschutz gewährleisten, der dem vorliegenden Gesetz entspricht. Der ersuchende Drittstaat hat das nachzuweisen.</p> <p>3 Im Zweifelsfall entscheidet die beauftragte Person für Datenschutz, ob die datenschutzrechtlichen Voraussetzungen für den Datenaustausch erfüllt sind.</p>
<b>Vaud</b> Loi sur la protection des données personnelles (LPrD) Règlement d'application de la loi du 11 septembre 2007 sur la protection des données personnelles (RLPrD)	<a href="https://www.legifind.ch/fe/tol/21923/versions/193659/fr/">https://www.legifind.ch/fe/tol/21923/versions/193659/fr/</a> <a href="https://www.legifind.ch/fe/tol/24196/versions/192168/fr/">https://www.legifind.ch/fe/tol/24196/versions/192168/fr/</a>		<p><b>Art. 18 LPrD Traitement des données par un tiers</b></p> <p>1 Le traitement de données peut être confié à un tiers aux conditions cumulatives suivantes:</p> <ul style="list-style-type: none"> <li>a. le traitement par un tiers est prévu par la loi ou par un contrat;</li> <li>b. le responsable du traitement est légitimé à traiter lui-même les données concernées;</li> <li>c. aucune obligation légale ou contractuelle de garder le secret ne l'interdit.</li> </ul> <p>2 Le tiers est responsable de la sécurité des données qu'il traite.</p> <p><b>Art. 10 LPrD Sécurité</b></p> <p>1 Le responsable du traitement prend les mesures appropriées pour garantir la sécurité des fichiers et des données personnelles, soit notamment contre leur perte, leur destruction, ainsi que tout traitement illicite.</p>		<p><b>Art. 17 LPrD Communication transfrontière de données</b></p> <p>1 La communication vers un pays tiers de données personnelles faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement, ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat.</p> <p>2 L'alinéa précédent n'est pas applicable:</p> <ol style="list-style-type: none"> <li>a. si la personne concernée a donné son consentement, qui doit dans tous les cas être explicite ;</li> <li>b. si la communication de données est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures pré-contractuelles prises à la demande de la personne concernée ;</li> <li>c. si la communication est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à concilier, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;</li> <li>d. si la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public, soit à la constatation, l'exercice ou la défense d'un droit en justice ;</li> <li>e. si la communication est, en l'espèce nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ;</li> <li>f. si la communication intervient d'un registre public qui, en vertu de dispositions légales ou réglementaires, est destiné à l'information du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier ;</li> <li>g. si des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger.</li> </ol>

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	TRANSFERTS À L'ÉTRANGER	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<b>Wallis</b> Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (GIDA) Ausführungsreglement zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (ARGIDA)	<a href="https://www.lexfind.ch/fe/ide/tol/19462/">https://www.lexfind.ch/fe/ide/tol/19462/</a> <a href="https://www.lexfind.ch/fe/ide/tol/19464/">https://www.lexfind.ch/fe/ide/tol/19464/</a> <a href="https://www.lexfind.ch/fe/ide/tol/19677/">https://www.lexfind.ch/fe/ide/tol/19677/</a> <a href="https://www.lexfind.ch/fe/ide/tol/19569/">https://www.lexfind.ch/fe/ide/tol/19569/</a>	<b>Art. 29 GIDA Bearbeitung im Auftrag</b> 1 Beauftragt der Inhaber der Datensammlung einen Dritten mit dem Bearbeiten von Daten, muss er dafür sorgen, dass der Schutz dieser Informationen und des Bearbeitungsergebnisses gemäss den obigenannten Bestimmungen gewährleistet ist.	<b>Art. 21 GIDA Datensicherheit</b> 1 Zum Schutz der registrierten Daten gegen das Risiko von Fälschung, Vernichtung, Diebstahl, Verlust, Kopie und anderen widerrechtlichen Bearbeitungen sind geeignete Massnahmen zu treffen.	<b>Art. 25 GIDA Grenzüberschreitende Bekanntgabe von Daten</b> 1 Es dürfen keinerlei Daten bekannt gegeben werden, wenn der Empfänger der Rechtshoheit von Staaten oder Organisationen unterliegt, die kein angemessenes Schutzniveau für die beabsichtigte Datenübermittlung gewährleisten. 2 Bei fehlendem angemessenem Schutz können personenbezogene Daten ausschliesslich unter einer der folgenden Bedingungen ins Ausland mitgeteilt werden: a) Die betroffene Person hat für die vorgesehene Datenübermittlung ihre vorgängige und ausdrückliche Einwilligung gegeben; b) die Bekanntgabe ist zur Wahrung eines überwiegenden öffentlichen Interesses unerlässlich; c) die Bekanntgabe ist für die Feststellung, die Ausübung oder die Verteidigung eines Rechtes vor Gericht unerlässlich; d) die Bekanntgabe ist notwendig, um das Leben oder die körperliche Integrität der betroffenen Person oder einer Drittperson zu schützen; e) die Bekanntgabe ist für den Abschluss oder die Erfüllung eines Vertrages unerlässlich und die bearbeiteten Daten betreffen den Vertragspartner; f) hinreichende, insbesondere vertragliche Garantien gewährleisten ein angemessenes Schutzniveau fürs Ausland. 3 Der Beauftragte muss die in Absatz 2 Buchstabe f vorgesehenen Garantien genehmigen.	<b>Art. 27 GIDA Weitere Einschränkungen der Bekanntgabe der Daten</b> 1 [...] 2 Stehen Personendaten unter dem Schutz des Berufs- oder Amtsgeheimnisses, können sie nur bekannt gegeben werden, wenn der Empfänger einer gleichwertigen Geheimhaltungspflicht untersteht. 3 Gesetzliche Bestimmungen, welche die Zustimmung der betroffenen Person verlangen, bleiben vorbehalten.
<b>Zug</b> Datenschutzgesetz (DSG) Verordnung über die Informationssicherheit von Personendaten (VIP)	<a href="https://www.lexfind.ch/fe/ide/tol/20055/">https://www.lexfind.ch/fe/ide/tol/20055/</a> <a href="https://www.lexfind.ch/fe/ide/tol/19012/">https://www.lexfind.ch/fe/ide/tol/19012/</a> <a href="https://www.lexfind.ch/fe/ide/tol/21100/">https://www.lexfind.ch/fe/ide/tol/21100/</a> <a href="https://www.lexfind.ch/fe/ide/tol/192334/">https://www.lexfind.ch/fe/ide/tol/192334/</a>	<b>§ 6 DSG Auftragsdatenbearbeitung</b> 1 Ein Organ kann das Bearbeiten von Personendaten Dritten übertragen, wenn: a) die Personendaten nur so bearbeitet werden, wie es das Organ selbst tun darf; und b) keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. 2 Das Organ stellt mittels Aufgaben, Vereinbarungen oder in anderer Weise sicher, dass die Auftragsdatenbearbeiterin oder der -bearbeiter die Informationsicherheit gewährleistet und die Rechte der betroffenen Person wahrt. 3 Das Organ bleibt für den gesetzmässigen Umgang mit den Personendaten verantwortlich. 4 Die Auftragsdatenbearbeiterin oder der -bearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Organs einer anderen Auftragsdatenbearbeiterin oder einem anderen -bearbeiter übertragen.	<b>§ 7 DSG Informationssicherheit</b> 1 Die Organe sorgen durch angemessene technische und organisatorische Massnahmen für die Sicherheit aller Personendaten. Personendaten sind insbesondere vor Verlust, Fälschung, Entwendung, Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern. 2 Der Regierungsrat erlässt innerhalb eines Jahres nach Inkrafttreten dieses Gesetzes entsprechende Vorschriften, insbesondere über die Sicherheitsgrundsätze und das Bewilligungsverfahren im Bereich des elektronischen Datenaustausches.	<b>§ 10a DSG Grenzüberschreitende Datenbekanntgabe</b> 1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen gefährdet wird. Eine Gefährdung liegt insbesondere bei Fehlen einer Gesetzgebung vor, die einen angemessenen Schutz gewährleistet. 2 Fehlt eine Gesetzgebung gemäss Abs. 1, dürfen Personendaten ins Ausland nur bekannt gegeben werden, wenn eine der folgenden Voraussetzungen erfüllt ist: a) hinreichende Garantien, insbesondere durch Vertrag, gewährleisten einen angemessenen Schutz im Ausland; über diese Garantien muss die Datenschutzstelle vor der Bekanntgabe der Daten ins Ausland informiert werden; b) die betroffene Person hat im Einzelfall ausdrücklich eingewilligt; c) die Bekanntgabe ist im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich; d) die Bekanntgabe im Einzelfall ist erforderlich, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen. 3 Eine Datenbekanntgabe ins Ausland darf nicht erfolgen, wenn dadurch in schwerwiegender Weise gegen die öffentliche Ordnung verstossen würde.	

ACTES LÉGISLATIFS	GESTION DES MANDATS	DROITS DE CONTRÔLE	EXIGENCES EN MATIÈRE DE SÉCURITÉ DES DONNÉES	DISPOSITIONS RELATIVES AU DROIT AU SECRET
<p><b>Zürich</b></p> <p>Gesetz über die Information und den Datenschutz (IDG)</p> <p>Gesetz über die Auslagerung von Informatikdienstleistungen (GAVI)</p> <p>Verordnung über die Information und den Datenschutz (IDV)</p> <p>Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen</p> <p>Allgemeine datenschutzrechtliche Geschäftsbedingungen bei der Datenbearbeitung durch Dritte</p>	<p><a href="https://www.levfind.ch/fe/fe/tol/21437/version/188522/de">https://www.levfind.ch/fe/fe/tol/21437/version/188522/de</a></p> <p><a href="https://www.levfind.ch/fe/fe/tol/21874/version/120873/de">https://www.levfind.ch/fe/fe/tol/21874/version/120873/de</a></p> <p><a href="https://www.levfind.ch/fe/fe/tol/21875/version/120874/de">https://www.levfind.ch/fe/fe/tol/21875/version/120874/de</a></p> <p><a href="https://www.ch.ch/content/dam/chweb/bilder-dokumente/organisation/finanzdirektion/af/agb_datenbearbeitung_durch_dritte.pdf">https://www.ch.ch/content/dam/chweb/bilder-dokumente/organisation/finanzdirektion/af/agb_datenbearbeitung_durch_dritte.pdf</a></p> <p><b>§ 6. IDG Bearbeiten im Auftrag</b></p> <p>1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht.</p> <p>2 Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.</p> <p><b>§ 25. IDV Auftragserteilung an Dritte</b></p> <p>1 Soweit die Informationsbearbeitung durch Dritte gemäss § 6 IDG gesetzlich nicht geregelt ist, ergehen entsprechende Aufträge an Dritte schriftlich.</p> <p>2 Der Auftrag regelt insbesondere:</p> <ul style="list-style-type: none"> <li>a. den Gegenstand und den Umfang der übertragenen Aufgaben,</li> <li>b. den Umgang mit Personendaten,</li> <li>c. die Geheimhaltungsverpflichtungen,</li> <li>d. die Behandlung von Informationszugangsgerüchten,</li> <li>e. zum Schutz der Informationen vorzuherrschenden Massnahmen,</li> <li>f. die Kontrolle der Auftragsfüllung,</li> <li>g. die Pflichtverletzung vorgesehene Sanstrafen,</li> <li>h. die Vertragsdauer und die Voraussetzungen der Vertragsauflösung.</li> </ul> <p>3 Die vorgesetzte Stelle genehmigt Aufträge für das Bearbeiten besonderer Personendaten.</p>	<p><b>§ 7. IDG Informationssicherheit</b></p> <p>1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.</p> <p>2 Die Massnahmen richten sich nach den folgenden Schutzzielen:</p> <ul style="list-style-type: none"> <li>a. Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen,</li> <li>b. Informationen müssen richtig und vollständig sein,</li> <li>c. Informationen müssen bei Bedarf vorhanden sein,</li> <li>d. Informationsbearbeitungen müssen einer Person zugerechnet werden können,</li> <li>e. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.</li> </ul> <p>3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.</p> <p><b>§ 2. GAVI Sicherung der Verwaltungstätigkeit</b></p> <p>1 Das öffentliche Organ stellt durch organisatorische und technische Massnahmen sowie vertragliche Auflagen sicher, dass die staatliche Aufgabenerfüllung auch dann ohne wesentliche Beeinträchtigung gewährleistet ist, wenn ein privates Unternehmen, bei dem es Informatikdienstleistungen beinhaltet, Abmachungen nicht einhält oder die Geschäftstätigkeit einstellt.</p> <p>2 Privatrechtlich organisierte Unternehmen, an denen der Kanton Zürich allein oder zusammen mit anderen öffentlichen Institutionen eine Kapital- und Stimmenmehrheit hält, gelten nicht als private Unternehmen im Sinne dieser Bestimmung.</p>	<p><b>TRANSFERTS À L'ÉTRANGER</b></p> <p><b>§ 19. IDG Bekanntgabe von Informationen – Grenzüberschreitend</b></p> <p>An Empfängerinnen und Empfänger, die dem Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht unterstehen, gibt das öffentliche Organ Personendaten bekannt, wenn</p> <ul style="list-style-type: none"> <li>a. im Empfängerstaat ein angemessener Schutz für die Datenübermittlung gewährleistet ist,</li> <li>b. eine gesetzliche Grundlage dies erlaubt, um bestimmte interessender betroffenen Person oder überwiegende öffentliche Interessen zu schützen, oder</li> <li>c. vom öffentlichen Organ angemessene vertragliche Sicherheitsvorkehrungen getroffen werden.</li> </ul> <p><b>§ 22. IDV Grenzüberschreitende Bekanntgabe von Personendaten</b></p> <p>1 Die grenzüberschreitende Übermittlung von Personendaten gestützt auf §19 lit. a IDG ist zulässig, wenn die Rechtsordnung oder anerkannte Selbstregulierungsbestimmungen im Empfängerstaat einen angemessenen Schutz der übermittelten Daten gewährleisten. Das öffentliche Organ kann hierfür auf die Liste der oder des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemäss Art. 7 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz abstellen.</p> <p>2 Erfolgt die grenzüberschreitende Übermittlung von Personendaten gestützt auf §19 lit. c IDG, ist die oder der Beauftragte für den Datenschutz über die vereinbarten Sicherheitsvorkehrungen vorab zu informieren.</p> <p>3 Die grenzüberschreitende Übermittlung von Personendaten kann im Einzelfall auch gestützt auf die Einwilligung der betroffenen Person erfolgen.</p> <p><b>§ 3. GAVI Amtsgeheimnis und Datenschutz</b></p> <p>1 Das öffentliche Organ darf besondere Personendaten im Sinne des Gesetzes über die Information und den Datenschutz und solche, die im Interesse des Staates der Geheimhaltung unterliegen, privatrechtlich organisierte Unternehmen nur dann zur Bearbeitung zugänglich machen, wenn sie durch organisatorische und technische Massnahmen vor unbefugter Einsichtnahme geschützt sind. Es stellt sicher, dass solche Daten ausschliesslich von Mitarbeitenden des Unternehmens bearbeitet werden, die diesbezüglich seinem Kontroll- und Missionsrecht unterstellt und als Hilfspersonen an das Amtsgeheimnis sowie allfällige Berufs- oder Spezialgeheimnisse gebunden sind.</p> <p>2 Im Übrigen gelten die Bestimmungen des Gesetzes über die Information und den Datenschutz über das Bearbeiten von Daten im Auftrag.</p>	



Merci  
Danke  
Grazie  
Engraziel